Lecture Notes in Mathematics 1849

M. L. Brown

Heegner Modules and Elliptic Curves

Springer

Author

Martin L. Brown

Institut Fourier
BP 74
38402 Saint-Martin d'Hères
France
e-mail: Martin.Brown@ujf-grenoble.fr

Library of Congress Control Number: 2004107464

Mathematics Subject Classification (2000):
11F52, 11G05, 11G09, 11G15, 11G40, 11R58, 14F20, 14G10, 14H52, 14J27, 14K22

ISSN 0075-8434
ISBN 3-540-22290-1 Springer Berlin Heidelberg New York
DOI: 10.107/b98488

Springer is a part of Springer Science + Business Media
springeronline.com

Printed in Germany

Typesetting: Camera-ready TEX output by the authors

41/3142/du - 543210 - Printed on acid-free paper

Preface

In this text, we define the Heegner module of an elliptic curve over a global field. For global ground fields of positive characteristic, Drinfeld proved that certain elliptic curves are the images of Drinfeld modular curves. On these modular curves are points corresponding to Heegner points on classical modular curves. These points, called Drinfeld-Heegner points, correspond to generators of the Heegner module of the elliptic curve. Furthermore, for the case of a Weil elliptic curve over the rational field $\mathbb{Q}$, the Heegner module of the curve is generated by the corresponding Heegner points.

The cohomology of the Heegner module of an elliptic curve over a global field induces elements in the cohomology of the elliptic curve. As an application, we prove the Tate conjecture for a class of elliptic surfaces over finite fields. This case of the Tate conjecture is essentially equivalent to the conjecture of Birch and Swinnerton-Dyer for a corresponding class of elliptic curves over global fields and is also equivalent to the finiteness of the Tate-Shafarevich groups of these elliptic curves. This application is parallel to V.A. Kolyvagin's proof of the conjecture of Birch and Swinnerton-Dyer for a class of Weil elliptic curves over the field of rational numbers.

Paris, March 2004 *M.L. Brown*

Contents

1 Introduction 1
- 1.1 Statement of the Tate conjecture 2
- 1.2 The Drinfeld modular curve $X_0^{\mathrm{Drin}}(I)$ 3
- 1.3 Analogue for F of the Shimura-Taniyama-Weil conjecture 3
- 1.4 Drinfeld-Heegner points 4
- 1.5 Heegner sheaves 4
- 1.6 Hecke operators 4
- 1.7 Bruhat-Tits buildings with complex multiplication 5
- 1.8 Bruhat-Tits buildings with complex multiplication and Drinfeld-Heegner points 6
- 1.9 Classification of Bruhat-Tits buildings with complex multiplication 6
- 1.10 The Heegner module of a galois representation 7
- 1.11 Cohomology of the Heegner module 8
- 1.12 The Tate conjecture and the Heegner module 8
- 1.13 Statement of the main result on the Tate conjecture 9
- 1.14 Heegner points on the classical modular curve $X_0(N)/\mathbb{Q}$ 10
- 1.15 Prerequisites and guide 10

2 Preliminaries 13
- 2.1 Notation 13
- 2.2 Orders in quadratic field extensions 14
- 2.3 Ring class fields 18
- 2.4 The Drinfeld moduli schemes $\mathbf{Y}_0^{\mathrm{Drin}}(I), \mathbf{X}_0^{\mathrm{Drin}}(I)$, M_I^d 23
- 2.5 Complex multiplication of rank 2 Drinfeld modules 26

3 Bruhat-Tits trees with complex multiplication 31
- 3.1 The Bruhat-Tits building Δ for SL_2 of a discretely valued field 32
- 3.2 Lattices in quadratic extensions: elementary results 33
- 3.3 Lattices in quadratic extensions: discrete valuation rings 36
- 3.4 Proofs of the propositions of §3.3 38

3.5 Explicit formulae for the conductor $\mathrm{Exp}(\Lambda)$ 41
3.6 Bruhat-Tits trees with complex multiplication 45
3.7 The standard metric and Bruhat-Tits trees with complex multiplication 46
3.8 Classification of Bruhat-Tits trees with complex multiplication 57
3.9 Lattices in quadratic extensions: Dedekind domains 62
3.10 The global Bruhat-Tits net 65
3.11 Bruhat-Tits nets with complex multiplication 69

4 Heegner sheaves 75
4.1 Drinfeld-Heegner points, Heegner morphisms 75
4.2 Construction of Drinfeld-Heegner points 76
4.3 Notation for Drinfeld-Heegner points 78
4.4 Galois action on Drinfeld-Heegner points 79
4.5 Hecke operators on $\mathbf{X}_0^{\mathrm{Drin}}(I)$ and the Bruhat-Tits net $\Delta_A(\mathrm{SL}_2(F))$ 80
4.6 Drinfeld-Heegner points and Hecke operators 86
4.7 Elliptic curves and Drinfeld modular curves 96
4.8 Drinfeld-Heegner points and elliptic curves 97
4.9 Heegner sheaves 99

5 The Heegner module 105
5.1 Group rings of finite abelian groups 106
5.2 The group rings Δ_c of Picard groups 109
5.3 The Heegner module of a galois representation 111
5.4 Čech galois cohomology 121
5.5 Group rings and **Č**ech cohomology 144
5.6 Group cohomology; Kolyvagin elements 169
5.7 Basic properties of the Heegner module 195
5.8 Proofs of the propositions of §5.7 198
5.9 Faithful flatness of the Heegner module 207
5.10 Proofs of the results of §5.9 209
5.11 The Heegner module as a Heegner sheaf 221

6 Cohomology of the Heegner module 223
6.1 General notation 224
6.2 Exact sequences and preliminary lemmas 224
6.3 Cohomology of the Heegner module: vanishing cohomology . . . 232
6.4 The main lemma 232
6.5 Proof of lemma 6.4.3. 234
6.6 The main proposition 241
6.7 The submodule $J_{c,z,S}$ 245
6.8 The kernel of Ξ 273
6.9 Proofs 277

6.10 Galois invariants of the Heegner module: S is an infinitesimal trait . . . 294
6.11 Proof of theorem 6.10.7 . . . 298

7 Finiteness of Tate-Shafarevich groups . . . 329
7.1 Quasi-modules . . . 330
7.2 Igusa's theorem . . . 339
7.3 Consequences of Igusa's theorem . . . 341
7.4 Proof of proposition 7.3.6. . . . 352
7.5 Preliminaries . . . 357
7.6 Statement of the main result and historical remarks . . . 357
7.7 Tate-Shafarevich groups . . . 363
7.8 Proof that theorem 7.7.5 implies theorem 7.6.5 . . . 365
7.9 The Selmer group . . . 366
7.10 The set $\mathcal{P}$ of prime numbers . . . 367
7.11 Frobenius elements and the set $\mathcal{D}_{l^n}$ of divisors . . . 369
7.12 The Heegner module attached to E/F . . . 371
7.13 Galois invariants of the Heegner module and the map η . . . 372
7.14 The cohomology classes $\gamma(c), \delta(c)$ . . . 382
7.15 Tate-Poitou local duality . . . 402
7.16 Application of Tate-Poitou duality . . . 404
7.17 Equivariant Pontrjagin duality . . . 406
7.18 Proof of theorem 7.7.5 . . . 412
7.19 Comments and errata for [Br2] . . . 433

Appendix A. Rigid analytic modular forms . . . 435
A.1 Basic definitions . . . 435
A.2 The Tate algebra . . . 436
A.3 Affinoid spaces, rigid analytic spaces . . . 437
A.4 Etale cohomology of rigid analytic spaces . . . 440
A.5 The space Ω^d . . . 444
A.6 The moduli scheme M_I^d . . . 445
A.7 An analytic description of M_I^d . . . 448
A.8 Rigid analytic modular forms . . . 450
A.9 Analytic modular forms . . . 451
A.10 q-expansions at the cusps of $\overline{M}_I^2$ . . . 452
A.11 Eisenstein series . . . 454
A.12 Hecke operators . . . 456
A.13 Elliptic curves over F and modular forms . . . 458

Appendix B. Automorphic forms and elliptic curves over function fields . . . 461
B.1 The Bruhat-Tits building for PGL over a local field . . . 461
B.2 The building map on Ω^d . . . 464
B.3 Fibres of the building map on Ω^2 . . . 466

B.4 Structures of level H on Drinfeld modules; the moduli scheme M_H^d 468
B.5 Action of arithmetic subgroups of $\mathrm{GL}_2(F)$ on T 471
B.6 Cohomology of Ω^2 and harmonic cochains 479
B.7 Cohomology of the moduli space M_H^2 483
B.8 Harmonic cochains and the special representation of $\mathrm{GL}_2(F_\infty)$ 488
B.9 Automorphic forms and the main theorem 492
B.10 The Langlands correspondence $\pi \to \sigma(\pi)$ 495
B.11 Elliptic curves as images of Drinfeld modular curves 497
B.12 The Langlands conjecture for GL_n over function fields (according to Lafforgue) 504

References 507

Index 511

1

Introduction

The points of departure of this text are twofold: first the proof by Drinfeld in 1974 ([Dr1], see also Appendix B) of an important case of the Langlands conjecture for GL_2 over a global field of positive characteristic and second the proof by Kolyvagin [K] in 1989 of the Birch Swinnerton-Dyer conjecture for a class of Weil elliptic curves over the rational field $\mathbb{Q}$.

A consequence of Drinfeld's work is that an elliptic curve E over a global field F of positive characteristic with split multiplicative reduction at a place is an image of a Drinfeld modular curve (see Appendix B, §B.11). The analogues of Heegner points on elliptic curves over the rational field $\mathbb{Q}$ may be then constructed on the curve E; these points on E are called Drinfeld-Heegner points.

These Drinfeld-Heegner points satisfy relations given by the action of the Hecke operators on the Drinfeld modular curves. We may then define, by generators and these relations, a *Heegner module* attached to the elliptic curve E. The Drinfeld-Heegner points of E generate a subgroup of E which is a homomorphic image of the Heegner module; nevertheless, the Heegner module is an object distinct from E. The cohomology of the Heegner module may be computed to a large extent (see Chapter 6). As an application of the cohomology of the Heegner module, we may then prove under suitable hypotheses the Tate conjecture for the elliptic surface over a finite field corresponding to the elliptic curve E/F (see Chapter 7).

The final part of the proof of the Tate conjecture (see Chapter 7) is parallel to Kolyvagin's calculation with "Euler systems" (see [R]). In particular, the derived cohomology classes of Kolyvagin transposed to the present case of elliptic curves over function fields arise naturally as part of the cohomology of the Heegner module.

Chapter 7 of this text is the sequel to the paper [Br2], in which we considered the Tate conjecture for surfaces equipped with a rational pencil of elliptic curves; here we consider the general case of surfaces with an irrational

M.L. Brown: LNM 1849, pp. 1–11, 2004.

elliptic fibration. Furthermore, for the original case of a rational pencil of elliptic curves, we give much more complete results and eliminate some of the technical hypotheses of the main theorem 1.1 of the first paper [Br2].

In this chapter below, we summarise the main results of this text.

1.1 Statement of the Tate conjecture

Let

k be a finite field of characteristic p with $q = p^m$ elements;
$\bar{k}$ be an algebraic closure of k;
C/k be a smooth projective irreducible curve over k;
F be the function field of the curve C;
X/k be an elliptic surface over C; that is to say, X/k is a smooth projective irreducible surface, equipped with a morphism $f : X \to C$ with a section such that all fibres of f, except a finite number, are elliptic curves;
E/F be the generic fibre of $f : X \to C$, which is an elliptic curve E over F;
∞ be a closed point of C.

The zeta function $\zeta(X, s)$ of X is defined by the formula

$$\zeta(X, s) = \prod_{x \in X(\bar{k})} \frac{1}{1 - |\kappa(x)|^{-s}}.$$

By Grothendieck and Deligne, for every prime number $l \neq p$ the zeta function takes the form

$$\zeta(X, s) = \prod_{i=0}^{4} P_i(X, q^{-s})^{(-1)^{i+1}}$$

where we have

(i) $P_i(X, t) = \det(1 - t\Theta |\ H^i_{\text{ét}}(X \times_k \bar{k}, \mathbb{Q}_l))$

$$P_0(X, t) = 1 - t, \quad P_4(X, t) = 1 - q^2 t,$$

where Θ is the Frobenius automorphism of $X \times_k \bar{k}$ relative to k;

(ii) $P_i(X, t) \in \mathbb{Z}[t]$ is independent of the prime number l for all i;

(iii) the roots of $P_i(X, t)$ in $\mathbb{C}$ have absolute values equal to $q^{-i/2}$.

Let $\rho(X)$ be the rank of the Néron-Severi group $\mathrm{NS}(X)$ of X/k. The Tate conjecture for this particular case of a surface over a finite field can be stated in one of these three equivalent ways:

(a) If $l \neq p$, the cycle map

$$\mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{Q}_l \to H^2_{\text{ét}}(X \times_k \bar{k}, \mathbb{Q}_l(1))^{\mathrm{Gal}(\bar{k}/k)}$$

is an isomorphism.
(b) The multiplicity of q as an inverse root of $P_2(X,t)$ is equal to $\rho(X)$.
(c) The order of the pole of $\zeta(X,s)$ at $s=1$ is equal to $\rho(X)$.

[For more details see [Br2, Introduction], [T1], [T3].]

1.2 The Drinfeld modular curve $X_0^{\mathrm{Drin}}(I)$

Let A be the coordinate ring $\Gamma(C \setminus \{\infty\}, \mathcal{O}_c)$ of the affine curve $C \setminus \{\infty\}$. Let I be a non-zero ideal of A.

The curve $X_0^{\mathrm{Drin}}(I)$ is the coarse moduli scheme of Drinfeld modules of rank 2 for A equipped with an I-cyclic subgroup (Definition 2.4.2); this curve is compactified by a finite number of cusps which correspond to "degenerate" Drinfeld modules. The points of $X_0^{\mathrm{Drin}}(I)/F$ correspond to pairs (D, Z) where D is a Drinfeld module of rank 2 for A and Z is a finite closed sub-group scheme of D which is isomorphic to A/I, as an A-module-scheme.

This modular curve $X_0^{\mathrm{Drin}}(I)$ is an analogue for the global field F of the classical modular curve $X_0(N)$ which is the coarse moduli scheme of elliptic curves equipped with a cyclic subgroup of order N, where N is a positive integer.

[For more details see, §2.4.]

1.3 Analogue for F of the Shimura-Taniyama-Weil conjecture

Let E/F be an elliptic curve which admits "split Tate multiplicative reduction" at ∞. Let I be the non-zero ideal of the ring A which is the conductor, without the place at ∞, of the elliptic curve E.

Thanks to the work of Drinfeld on the Langlands conjecture for GL(2), there is a finite surjective morphism of curves

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

This result is the analogue for the global field F of the Shimura-Taniyama-Weil conjecture proved by Wiles [W] for semi-stable elliptic curves over $\mathbb{Q}$.

[For more details, see §4.7 and Appendix B.]

1.4 Drinfeld-Heegner points

Let K be a field which is an quadratic extension of F where the place ∞ remains inert; K is said to be an *imaginary quadratic extension* of F.

Let D be a Drinfeld module for A of rank 2 with complex multiplication by an order $\mathcal{O}$ of K; let Z be an I-cyclic subgroup of D. Then the pair (D, Z) represents a point on the modular curve $X_0^{\mathrm{Drin}}(I)$ (see §1.2).

If the quotient Drinfeld module D/Z has the same ring of endomorphisms $\mathcal{O}$ as D then the point (D, Z) on the modular curve $X_0^{\mathrm{Drin}}(I)$ is called a *Drinfeld-Heegner point* (see chapter 4).

If (D, Z) is a Drinfeld-Heegner point and $\psi : X_0^{\mathrm{Drin}}(I) \to E$ is a finite surjective morphism of curves, where E is an elliptic curve over F (see §1.3), then the point $\psi(D, Z)$ is called a *Drinfeld-Heegner point* of the elliptic curve E.

The Drinfeld-Heegner points (D, Z) and $\psi(D, Z)$ are rational over the ring class field $K[c]$, where c is the conductor of the order $\mathcal{O}$ of K relative to A (see §§2.2,2.3).

1.5 Heegner sheaves

Let E/F be an elliptic curve equipped with a finite surjective morphism of curves

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

where I is the conductor, without the place at ∞, of E (see §1.3).

Let F^{sep} be a separable closure of the field F. The set of Drinfeld-Heegner points of E generates a subgroup $\mathcal{H}$ of the abelian group $E(F^{\mathrm{sep}})$ of F^{sep}-rational points of E. The group $\mathcal{H}$ equipped with its action by the Galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ is then a sheaf of abelian groups for the étale topology of Spec F (see chapter 4) where for any étale morphism $U \to \mathrm{Spec}\ F$ we have

$$\Gamma(U, \mathcal{H}) = \left\{ f : U \to E \quad \middle| \quad \begin{array}{c} \text{the geometric points of} \\ \text{the image of } f \text{ are Drinfeld} - \text{Heegner} \end{array} \right\}.$$

Evidently $\mathcal{H}$ is a subsheaf of the étale sheaf defined by the elliptic curve E.

In the same way, the set of Drinfeld-Heegner points of $X_0^{\mathrm{Drin}}(I)$ defines a sheaf of sets for the étale topology on Spec F. Furthermore, a sheaf of abelian groups may be defined for the étale topology on the curve C and which is the subsheaf generated by the Drinfeld-Heegner points of the sheaf defined by the Néron model of E over C .

1.6 Hecke operators

Let z be a closed point of $C \setminus \{\infty\}$ let $\mathfrak{m}_z$ be the maximal ideal of the ring A defined by z. If z is not in the support of Spec A/I, the Hecke operator T_z is

defined on the curve $X_0^{\mathrm{Drin}}(I)$ by

$$T_z : (D, Z) \mapsto \sum_H (D/H, (Z+H)/H)$$

where H runs over the $\mathfrak{m}_z$-cyclic subgroups of D and the right hand side of this formula is a divisor on $X_0^{\mathrm{Drin}}(I)$.

[See §4.5 for more details.]

1.7 Bruhat-Tits buildings with complex multiplication

Let $\Delta(\mathrm{SL}_2(F))$ be the euclidean Bruhat-Tits building for SL_2 of the field F equipped with its discrete valuation associated to a closed point z. For this case of SL_2, the building $\Delta(\mathrm{SL}_2(F))$ is a *tree*.

Let $\mathcal{L}$ be the set of vertices of $\Delta(\mathrm{SL}_2(F))$. Then a *Bruhat-Tits tree with complex multiplication* is a couple $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ where Exp, called an *exponent function*, is a map of sets (see chapter 3)

$$\mathrm{Exp} : \mathcal{L} \to \mathbb{Z}.$$

We are principally concerned with Bruhat-Tits buildings with complex multiplication which arise in the following way. Let

M be a reduced 2-dimensional commutative F-algebra;
R be the discrete valuation ring of F associated to the closed point z;
π be a uniformising parameter of R;
S be the integral closure of R in M.

As M is a 2-dimensional vector space over F, the R-lattices contained in M correspond surjectively to the elements of $\mathcal{L}$. Two R-lattices Λ_1, Λ_2 in M correspond to the same point in $\mathcal{L}$ if and only if they are equivalent, that is, $\Lambda_1 = a\Lambda_2$ for some $a \in F^*$.

To each lattice equivalence class $[\Lambda] \in \mathcal{L}$, where $\Lambda \subset M$ is a lattice of M, is associated the ring of endomorphisms $\mathrm{End}_R^M(\Lambda)$ which is the subring of M preserving Λ:

$$\mathrm{End}_R^M(\Lambda) = \{m \in M \mid m\Lambda \subset \Lambda\}.$$

The ring $\mathrm{End}_R^M(\Lambda)$ is uniquely determined by its conductor ideal $[S : \mathrm{End}_R^M(\Lambda)]$, which is an ideal of R, and depends only on the lattice class of Λ. The conductor $[S : \mathrm{End}_R^M(\Lambda)]$ is of the form $\pi^{\mathrm{Exp}([\Lambda])}R$, where the exponent of the conductor $\mathrm{Exp}([\Lambda])$ is an integer; this defines a map

$$\mathrm{Exp} : \mathcal{L} \to \mathbb{Z}.$$

This pair $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ is a Bruhat-Tits building with complex multiplication. When the algebra M is not reduced, a Bruhat-Tits building with complex multiplication may also be defined (chapter 3).

This construction may be globalised to define a *Bruhat-Tits net with complex multiplication* for any excellent Dedekind domain R (see §§3.9, 3.10, 3.11).

1.8 Bruhat-Tits buildings with complex multiplication and Drinfeld-Heegner points

Let (D, Z) be a Drinfeld-Heegner point on $X_0^{\mathrm{Drin}}(I)$ relative to the imaginary quadratic field extension K of F (see §1.4). Let z be a closed point of $C \setminus \{\infty\}$ where z is not in the support of Spec A/I; let T_z be the Hecke operator at z. Then

$$T_z(D, Z)$$

is a divisor on $X_0^{\mathrm{Drin}}(I)$ whose irreducible components are also Drinfeld-Heegner points.

The Drinfeld module D, which has complex multiplication by an order of K, corresponds to an A-sublattice Λ of rank 2 of K, under the equivalence between Drinfeld modules of infinite characteristic and lattices. Hence D corresponds via Λ to a vertex v of the Bruhat-Tits building $\Delta(\mathrm{SL}_2(F))$ with respect to the discrete valuation on F corresponding to z. The irreducible components of $T_z(D, Z)$ then correspond to the neighbouring vertices of v in $\Delta(\mathrm{SL}_2(F))$. The exponents at z of the conductors of the endomorphism rings of these components of $T_z(D, Z)$ are then the values of an exponent function Exp on the corresponding vertices of $\Delta(\mathrm{SL}_2(F))$.

The endomorphism rings of the components of $T_z(D, Z)$ are in this way described by a Bruhat-Tits tree with complex multiplication $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ with respect to z (see §§3.6-3.8).

1.9 Classification of Bruhat-Tits buildings with complex multiplication

Let M, R, z be as in §1.7. Let $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ be the corresponding Bruhat-Tits tree with complex multiplication.

We prove that there are precisely 4 distinct forms of the Bruhat-Tits trees with complex multiplication $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$, that is to say, 4 distinct forms of the exponent functions Exp; there are 3 forms corresponding to the splitting of the place z in the quadratic extension of algebras M/F and there is a 4th form when M is not a reduced algebra.

We give a simple formula for the exponent functions Exp in terms of the standard metric on the euclidean building $\Delta(\mathrm{SL}_2(F))$ (see theorems 3.7.3, 3.7.5 and figures 1, 2, 3, and 4 of §3.8).

1.10 The Heegner module of a galois representation

Let

ρ be a finite dimensional continuous representation over a local field L of the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$, where F^{sep} denotes the separable closure of F;
K/F be an imaginary quadratic field extension;
R be a subring of L such that the character of ρ takes its values in R.

We construct a discrete galois R-module $\mathcal{H}(\rho)$ over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ called the *canonical Heegner module attached to ρ and K/F with coefficients in R.*

The Heegner module $\mathcal{H}(\rho)$ is defined by generators and relations over the ring R. The generators are the symbols $< b, c >$ where c runs over all effective divisors on Spec A and b runs over all divisor classes of $\mathrm{Pic}(O_c)$, the Picard group of the order O_c of K with conductor c. The relations are explicitly given in (5.3.5)-(5.3.8); they are derived from the action of the Hecke operators on Drinfeld-Heegner points.

The most important case of this construction of $\mathcal{H}(\rho)$ arises from elliptic curves. Suppose that E/F is an elliptic curve equipped with a finite surjective morphism of curves

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

For any prime number l different from the characteristic of F, the curve E provides a continuous l-adic representation

$$\sigma : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l)).$$

Let K/F be an imaginary quadratic extension field of F in which all primes dividing the conductor of E, except ∞, split completely. The character of this representation σ takes its values in $\mathbb{Z}$. The Heegner module $\mathcal{H}(\sigma)$ attached to σ and K/F is then an abelian group equipped with the structure of a discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module; it is also equipped with a galois-equivariant homomorphism (see examples 5.3.18)

$$f : \mathcal{H}(\sigma)^{(0)} \to E(F^{\mathrm{sep}})$$

where $\mathcal{H}(\sigma)^{(0)}$ is the direct summand of $\mathcal{H}(\sigma)$ generated by the symbols $< b, c >$ where c runs over all effective divisors on Spec A prime to a particular finite exceptional set of prime divisors. The image of this homomorphism is precisely the subgroup of $E(F^{\mathrm{sep}})$ generated by the Drinfeld-Heegner points; that is to say, the image $f(\mathcal{H}(\sigma)^{(0)})$ may be considered as a sheaf of abelian groups for the étale topology on Spec K and it coincides with the Heegner sheaf $\mathcal{H}$ of E, as in §1.5.

[See chapter 5 for more details.]

1.11 Cohomology of the Heegner module

As in the preceding section §1.10, let $\mathcal{H}(\rho)$ over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the Heegner module over R attached to ρ, K/F, and R.

The Heegner module $\mathcal{H}(\rho)$ is an *abelian representation* of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ in that the action of this galois group factors through an abelian quotient.

More precisely, let $K[c]$ be the ring class field of K over F with conductor c (§2.3). Then $\mathcal{H}(\rho)$ may be expressed as a direct limit

$$\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$$

where c runs over all effective divisors on Spec A and $\mathcal{H}_c$ is a $\mathrm{Gal}(K[c]/K)$-module and is an R-module of finite type. This direct limit (which under a simple hypothesis is a direct union; see corollary 5.9.4) defines a filtration on $\mathcal{H}(\rho)$ and gives this Heegner module the structure of a discrete module over the abelian galois group

$$\mathrm{Gal}\Big(\bigcup_c K[c]/K\Big).$$

For any R-algebra S and any prime divisor z in the support of c, we attempt to determine in Chapter 6 the galois cohomology groups

$$H^i(\mathrm{Gal}(K[c]/K[c-z]), \mathcal{H}_c \otimes_R S), \quad \text{for } i \geq 0.$$

This is the first step in the determination of the galois cohomology groups

$$H^i(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathcal{H}(\rho) \otimes_R S), \quad \text{for } i \geq 0.$$

The most precise results we obtain are for the case where S is an *infinitesimal trait* that is to say an artin local ring which is a quotient of a discrete valuation ring.

[See chapter 6 for more details.]

1.12 The Tate conjecture and the Heegner module

Let $\mathcal{E}/C$ be the Néron model of the elliptic curve E/F. Then $\mathcal{E}$ can be considered as a sheaf of abelian groups on C for the étale topology.

The *Tate-Shafarevich group of* E/F is defined by

$$Ш(E,F) = H^1_{\text{ét}}(C, \mathcal{E}).$$

As k is a perfect field, this says that $Ш(E,F)$ is the group of principal homogeneous of E/F which are everywhere locally trivial. Thanks to the work of Artin, Tate and Milne, the finiteness of the group $Ш(E,F)$ is equivalent to the Tate conjecture for the elliptic surface $\mathcal{E}/k$ of §1.1.

Suppose that E/F is an elliptic curve equipped with a finite surjective morphism of curves over F

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

For any prime number l different from the characteristic of F, we have a continuous l-adic representation

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l)).$$

Let K/F be an imaginary quadratic extension field of F in which all primes dividing the conductor of E, except ∞, split completely. As in §1.10, let $\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$ be the Heegner module attached to ρ and K/F and the ring of coefficients $\mathbb{Z}$; we have a morphism of sheaves for the étale topology over Spec K

$$f : \mathcal{H}(\rho)^{(0)} \to E.$$

The morphism of sheaves f provides homomorphisms of cohomology groups

$$\Big(\mathcal{H}_c \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}}\Big)^{\mathrm{Gal}(K[c]/K)} \to H^1_{\text{ét}}(\mathrm{Spec}\ K[c], E_n)^{\mathrm{Gal}(K[c]/K)}$$

for all integers $n \geq 1$ prime to the characteristic of F and all c prime to a finite exceptional set of divisors, where E_n is the n-torsion subgroup of E. This gives rise (see (7.14.5)) to the fundamental *Heegner homomorphism*, for all n prime to a finite exceptional set of prime numbers,

$$\Big(\mathcal{H}_c \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}}\Big)^{\mathrm{Gal}(K[c]/K)} \to H^1_{\text{ét}}(\mathrm{Spec}\ K, E).$$

The subgroups of $H^1_{\text{ét}}(\mathrm{Spec}\ K, E)$ coming from the calculation of the cohomology of the Heegner module $\mathcal{H}(\rho)$, by a fine analysis in Chapter 7, enables us to show, under suitable hypotheses, the finiteness of the Tate-Shafarevich group $Ш(E, F)$ and hence to prove the Tate conjecture for $\mathcal{E}/k$.

1.13 Statement of the main result on the Tate conjecture

In this section, let F be a global field of positive characteristic and with exact field of constants k; fix a place ∞ of F with residue field equal to k. Let E/F be an elliptic curve with an origin and with split multiplicative reduction at ∞. Then E/F is equipped with a map of F-schemes

$$\pi : X_0^{\mathrm{Drin}}(I) \to F$$

where I, which is an ideal of A, is the conductor of E without the component at ∞ (see §1.3). Let K be an imaginary quadratic extension field of F for

which every prime dividing the conductor of E/F, except ∞, splits completely in K/F. Let $< 0, I_1, 0, \pi >$ be a Drinfeld-Heegner point of $E(K[0])$ (for the notation, see (4.8.2)). Put

$$x_0 = \mathrm{Tr}_{K[0]/K} < 0, I_1, 0, \pi > \in E(K).$$

Let $\epsilon = \pm 1$ be the sign in the functional equation of the L-function of E/F.

1.13.1. Theorem. *Suppose that $K \neq F \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$ and that x_0 has infinite order in the group $E(K)$. Let $\mathcal{E}/k$ (resp. $\mathcal{E}'/k$) be a proper smooth model of the Néron model of the elliptic curve E/F (resp. $E \times_F K/K$). Then we have:*
(i) *$E(F)$ is a finite abelian group if $\epsilon = +1$, and is an abelian group of rank 1 if $\epsilon = -1$;*
(ii) *$E(K)$ is an abelian group of rank 1;*
(iii) *The Tate conjecture holds for the elliptic surfaces $\mathcal{E}/k$ and $\mathcal{E}'/k$ (see §1.1);*
(iv) *The Birch-Swinnerton-Dyer conjecture holds for the elliptic curves E/F and $E \times_F K/K$ (see* [Br2, Introduction]*);*
(v) *The Artin-Tate conjecture holds for the elliptic surfaces $\mathcal{E}/k$ and $\mathcal{E}'/k$ provided that* char.$(F) \neq 2$ *(see* [Br2, Introduction]*).*

1.13.2. Remark. In this extension of the main theorem 1.1 of [Br2], the hypotheses stated therein have been largely eliminated. It is probable that the hypothesis that $p \neq 2$ in part (v) of the above theorem 1.13.1 can be dispensed with completely.

1.14 Heegner points on the classical modular curve $X_0(N)/\mathbb{Q}$

In this paper, we apply the methods developped to the Tate conjecture for elliptic surfaces over finite fields. Nevertheless, the work below applies equally to classical Heegner points on elliptic curves over $\mathbb{Q}$ and in this way goes beyond prior work of Kolyvagin on the Birch-Swinnerton Dyer conjecture. In particular, the Bruhat-Tits trees with complex multiplication, global Bruhat-Tits nets, Heegner sheaves, and Heegner modules, defined in Chapters 3,4, and 5, and the cohomology of the Heegner module computed in Chapter 6, with minor modifications, also apply to elliptic curves over $\mathbb{Q}$.

1.15 Prerequisites and guide

Prerequisites for reading this text are scheme theory, class field theory, and a basic knowledge of Drinfeld modules and elliptic curves ([H), [N], [DH], [Si1], and [Si2] respectively). Group cohomology is used throughout but almost all

the basic definitions are given. Etale cohomology, except for §§5.4,5.5, is hardly used until the final chapter 7 (see [M2]).

Drinfeld's proof of a particular case of the Langlands conjecture for GL_2 is presented in Appendix B but only the statement of the result and its implications for elliptic curves over function fields are required to follow the main text (see §B.11 and notably theorem B.11.17). Rigid analytic modular forms and rigid analytic spaces are sketched in Appendix A; but this is inessential for understanding the main text.

The important results not covered in this text are the following:

(i) Igusa's determination of the Galois action on torsion points on elliptic curves over function fields [I].

(ii) The relation between the conjectures of Tate, Artin-Tate, for surfaces over finite fields and the Birch Swinnerton-Dyer conjecture for elliptic curves over function fields (see [T1], [T3], [M1]).

It is unnecessary to read the whole text to follow the proof of the Tate conjecture theorem 1.13.1. For this, it is sufficient to read the following:

(a) Examples 5.3.18(1) and the definition of the Heegner module in §§5.3.1-5.3.11.

(b) That part of section 5.6 on Kolyvagin elements notably proposition 5.6.12.

(c) Case (1) of the table 6.10.7 (z remains prime in K/F and is prime to c) on the galois invariants of the Heegner module.

(d) Chapter 7.

For a clear presentation of a special case of Kolyvagin's work on elliptic curves over $\mathbb{Q}$, see [GB2].

2

Preliminaries

This chapter contains preliminaries on orders in quadratic extension fields, ring class fields, complex multiplication of Drinfeld modules, and Drinfeld modular curves. Proofs in this chapter are usually omitted as the results of this chapter are essentially well known.

In this chapter and the chapters 3 and 4, we extend the results of Section 2 of the paper [Br2] to the general case of global fields of positive characteristic $p > 0$. In [Br2, §2], the ground field is assumed to be the rational function field $F = k(T)$ and in some instances the characteristic p is assumed to be different from 2. The results of [Br2, §2] generalise with few changes; nevertheless, some differences arise because the affine coordinate ring A (see §2.1 below) need no longer have class number 1. We shall give much more complete results than those of [Br2, §2] and indeed give complementary results for the case of rational function fields.

2.1 Notation

The following notation is fixed for the rest of this paper:

k is a finite field with $q = p^m$ elements;
θ is the Frobenius $x \mapsto x^p$;
C/k is an integral smooth 1-dimensional projective k-scheme, where k is the exact field of constants (a *curve*);
∞ is a closed point of C/k;
C_{aff} is the affine curve $C \setminus \{\infty\}$;
A is the coordinate ring $H^0(C_{\text{aff}}, \mathcal{O}_{C_{\text{aff}}})$ of the affine curve C_{aff};
F is the fraction field of A (that is, the function field of C/k);
$\kappa(z)$, where z is a closed point of C, is the residue field at z;
K/F is a quadratic extension field of F;
B is the integral closure of A in K.

M.L. Brown: LNM 1849, pp. 13–30, 2004.

2.2 Orders in quadratic field extensions

(2.2.1) We list below various elementary properties of orders in quadratic field extensions; these are easily verified and most proofs are omitted.

(2.2.2) One says that K/F is *imaginary* if the point ∞ is inert or ramified in the quadratic field extension K/F.

(2.2.3) The ring B is a finite A-module [ZS, Vol. 1, Ch. 5, §4, Th. 9] and is a Dedekind domain.

(2.2.4) An *order O in K* with respect to A is an A-subalgebra of B whose field of fractions is equal to K.

(2.2.5) The *conductor* of an order O is $[B : O]_A$, which is an ideal of A.

We then have that Spec $A/[B : O]_A$ is a zero dimensional closed subscheme of Spec A to which we may associate an effective divisor c on C_{aff}

$$c = \sum_{\mathfrak{p} \in \text{ Spec } A} \mathfrak{p}.\text{ord}_{\mathfrak{p}}[B : O]_A$$

which we also call the conductor of O. We have $c = 0$ if and only if $O = B$.

(2.2.6) There is a bijection (as in [Br2, §2.4]) between orders O_c of K with respect to A and effective k-rational divisors c on the affine curve C_{aff}, where c is the conductor of O_c. This is written

$$c \mapsto O_c = A + BI(c)$$

where $I(c)$ is the ideal of A cutting out the effective divisor c.

(2.2.7) For effective divisors c, c' on C_{aff} we have $c \geq c'$ if and only if $O_c \subset O_{c'}$. Let

$$f : \text{Spec } O_{c'} \to \text{Spec } A$$

be the structure map. If $c \geq c'$ then the map Spec $O_{c'} \to$ Spec O_c obtained from inclusion is finite and is an isomorphism outside the closed subscheme of Spec $O_{c'}$ given by

$$f^{-1}\{\mathfrak{p} \in \text{Spec } A |\ \text{ord}_{\mathfrak{p}}(c) > \text{ord}_{\mathfrak{p}}(c')\}.$$

(2.2.8) The units of the order O_c are given by

$$O_c^* = \begin{cases} A^*, & \text{if } c \neq 0; \\ B^*, & \text{if } c = 0. \end{cases}$$

(2.2.9) Let $\mathfrak{p}$ be a maximal ideal of A which is contained in the support of the effective divisor c on C_{aff}. Then there is a unique prime ideal of O_c lying over $\mathfrak{p}$. This prime ideal is equal to, in the notation of (2.2.6),

$$\mathfrak{p} + I(c)B.$$

(2.2.10) Let $\mathfrak{p}$ be a maximal ideal of A. Let c be an effective divisor on C_{aff} whose support contains $\mathfrak{p}$ that is to say

$$c = m.\mathfrak{p} + (\text{prime to } \mathfrak{p})$$

where $m \geq 1$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_i$ $(i \leq 2)$ be the prime ideals of B lying over $\mathfrak{p}$. Let $\mathfrak{p}_1 = \mathfrak{q}_1 \cap O_c$, which is the unique prime ideal of O_c lying over $\mathfrak{p}$. Let $B_{\mathfrak{p}}$ denote the semi-local ring

$$(B - \mathfrak{q}_1 - \ldots - \mathfrak{q}_i)^{-1}B = B \otimes_A A_{\mathfrak{p}}.$$

The quotient of unit groups of the localizations

$$B^*_{\mathfrak{p}}/O^*_{c,\mathfrak{p}_1}$$

is a finite group and the natural map $B \to B_{\mathfrak{p}}$ induces an isomorphism of finite multiplicative groups

$$B^*_{\mathfrak{p}}/O^*_{c,\mathfrak{p}_1} \cong (B/\mathfrak{p}^m B)^*/(A/\mathfrak{p}^m)^*.$$

Furthermore, if $\hat{B}_{\mathfrak{p}}$ and $\hat{O}_{c,\mathfrak{p}_1}$ are the corresponding completions of these semi-local rings with respect to their jacobson radicals then we have a natural isomorphism of quotients of multiplicative groups

$$\hat{B}^*_{\mathfrak{p}}/\hat{O}^*_{c,\mathfrak{p}_1} \cong B^*_{\mathfrak{p}}/O^*_{c,\mathfrak{p}_1}.$$

(2.2.11) Suppose now that $c \geq c'$ are effective divisors on C_{aff} where c is as in (2.2.10) above and

$$c' = m'.\mathfrak{p} + (\text{prime to } \mathfrak{p})$$

where $m \geq m' \geq 1$, so that $\mathfrak{p}$ is in the support of both c and c'.

Let $U(m, m', \mathfrak{p})$ denote the subgroup of "higher principal units" of $(B/\mathfrak{p}^m B)^*/(A/\mathfrak{p}^m)^*$ that is the group given as the kernel of the natural surjective homomorphism

$$U(m, m', \mathfrak{p}) = \ker\big\{(B/\mathfrak{p}^m B)^*/(A/\mathfrak{p}^m)^* \to (B/\mathfrak{p}^{m'} B)^*/(A/\mathfrak{p}^{m'})^*\big\}.$$

Let $\mathfrak{p}_1$ be the unique prime ideal of O_c which lies over $\mathfrak{p}$. Let $\mathfrak{p}'_1$ be the unique prime of $O_{c'}$ lying over $\mathfrak{p}$. The quotient of unit groups of the localizations

$$O^*_{c',\mathfrak{p}'_1}/O^*_{c,\mathfrak{p}_1}$$

is a finite abelian group; we have a natural isomorphism of groups obtained from (2.2.10)

$$O^*_{c',\mathfrak{p}'_1}/O^*_{c,\mathfrak{p}_1} \cong U(m, m', \mathfrak{p}).$$

Furthermore, if $\hat{O}_{c',\mathfrak{p}'_1}$ and $\hat{O}_{c,\mathfrak{p}_1}$ are the corresponding completions of these local rings with respect to their maximal ideals then we have a natural isomorphism of quotients of multiplicative groups

$$\hat{O}^*_{c',\mathfrak{p}'_1}/\hat{O}^*_{c,\mathfrak{p}_1} \cong O^*_{c',\mathfrak{p}'_1}/O^*_{c,\mathfrak{p}_1}.$$

(2.2.12) Let $c \geq c'$ be effective divisors on C_{aff}. The inclusion map $O_c \subset O_{c'}$ then gives rise to a surjective homomorphism of abelian groups, where $\text{Pic}(R)$ denotes the Picard group of a ring R,

$$t_{c,c'} : \text{Pic}(O_c) \to \text{Pic}(O_{c'}).$$

(2.2.13) In the case where $c' = 0$ and $c > 0$, the kernel $\ker(t_{c,0})$ of the homomorphism $t_{c,c'}$ of Picard groups of (2.2.12) is given, by

$$\ker(t_{c,0}) \cong \frac{(B/I(c)B)^*}{(A/I(c))^*}/(B^*/A^*)$$

where $I(c)$ is the ideal of A cutting out c.

[In order to prove this, for any effective divisors $c \geq c'$ on C_{aff} put $X = \text{Spec } O_{c'}$, $Y = \text{Spec } O_c$, and $j : X \to Y$ the map obtained from the inclusion $O_c \subset O_{c'}$. We then obtain an exact sequence of sheaves of abelian groups for the Zariski topology on X

$$0 \to j^{-1}\mathcal{O}^*_Y \to \mathcal{O}^*_X \to \mathcal{H} \to 0$$

where $j^{-1}\mathcal{O}^*_Y$ denotes the inverse image sheaf [H, p.65] and where $\mathcal{H}$ is a skyscraper sheaf with support contained in the set of the points of X where c and c' differ. The long exact sequence of cohomology then gives an exact sequence

$$0 \to O^*_c \to O^*_{c'} \to H^0(X, \mathcal{H}) \to H^1(X, j^{-1}\mathcal{O}^*_Y) \to H^1(X, \mathcal{O}^*_X) \to 0$$

where we evidently have $H^1(X, \mathcal{H}) = 0$. Furthermore we have

$$H^1(X, j^{-1}\mathcal{O}^*_Y) = \text{Pic}(O_c)$$

$$H^1(X, \mathcal{O}^*_X) = \text{Pic}(O_{c'}).$$

This gives the exact sequence of abelian groups

$$0 \to O_c^* \to O_{c'}^* \to H^0(X, \mathcal{H}) \to \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c'}) \to 0. \tag{2.2.14}$$

In the particular case where $c' = 0$, we have by (2.2.10)

$$H^0(X, \mathcal{H}) = \frac{(B/I(c)B)^*}{(A/I(c))^*}.$$

This with the exact sequence (2.2.14) gives the expression above for the kernel $\ker(t_{c,0})$ in the case where $c > c' = 0$.]

(2.2.15) In the case where $c > c' > 0$, for the kernel $\ker(t_{c,c'})$ of the surjective homomorphism

$$t_{c,c'} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c'})$$

we have an isomorphism

$$\ker(t_{c,c'}) \cong \frac{(B/I(d)B)^*}{(A/I(d))^*} \prod_{\mathfrak{p} \in \ \mathrm{Supp}\ (c')} U(m_{\mathfrak{p}}, m'_{\mathfrak{p}}, \mathfrak{p}).$$

The product is over all maximal ideals $\mathfrak{p}$ of A in the support of the divisor c'. Here the symbols are given by

$c = \sum_{\mathfrak{p}} m_{\mathfrak{p}}.\mathfrak{p}$;
$c' = \sum_{\mathfrak{p}} m'_{\mathfrak{p}}.\mathfrak{p}$;
$d = \sum_{\mathfrak{p} \notin \ \mathrm{Supp}\ (c')} m_{\mathfrak{p}}.\mathfrak{p}$ is the greatest effective divisor which is $\leq c$ and prime to c';
$I(d)$ is the ideal of A defining the effective divisor d.

[This formula follows immediately from (2.2.10), (2.2.11), (2.2.13) and the exact sequence (2.2.14): with the notation above and that of (2.2.13) we have the isomorphism

$$H^0(X, \mathcal{H}) \cong \frac{(B/I(d)B)^*}{(A/I(d))^*} \prod_{\mathfrak{p} \in \ \mathrm{Supp}\ (c')} U(m_{\mathfrak{p}}, m'_{\mathfrak{p}}, \mathfrak{p}).\ ]$$

2.3 Ring class fields

In this section we give some generalities on ring class field extensions associated to orders in imaginary quadratic extensions.

(2.3.1) Let

K/F be an imaginary quadratic field extension, with respect to ∞ (§2.2, (2.2.2));
B be the integral closure of A in K;
K^{ab} be the maximal abelian separable extension field of K;
J_K be the idèle group of K;
J_K/K^* be the idèle class group of K;
$[-, K^{\mathrm{ab}}/K] : J_K/K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ be the Artin reciprocity map.

The homomorphism $[-, K^{\mathrm{ab}}/K]$ is injective and its image consists of elements of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ whose restrictions to $\mathrm{Gal}(\bar{k}/k)$ are integral powers of the Frobenius automorphism, where $\bar{k}$ is the algebraic closure of k.

(2.3.2) Let

O_c be an order of K, relative to A, with conductor c (§2.2, (2.2.6));
A_v, for a place v distinct from ∞ of F, denote the localization of the ring A at the maximal ideal corresponding to v;
$\hat{A}_v$ be the completion of A_v with respect to the topology defined by the maximal ideal of A_v;
$\hat{O}_{c,v}$ be the completion of the semi-local ring $O_c \otimes_A A_v$ with respect to the topology defined by its jacobson radical, that is to say $\hat{O}_{c,v} = O_c \otimes_A \hat{A}_v$;
$G_c = K_\infty^* \prod_{v \neq \infty} \hat{O}_{c,v}^*$ be the subgroup of the idèle group J_K whose components are the units of $\hat{O}_{c,v}$ for all places $v \neq \infty$ of F, and K_∞^* for the component at $v = \infty$, and where in the product v runs over all places of F.

For a given place $v \neq \infty$ of F, that part $\hat{O}_{c,v}^*$ of the product for G_c is a subgroup of $(B \otimes_A A_v)^*$ which is the unit group of the product of the completions of B at all the places of K lying over v. Note that distinct places of K may give rise to the *same* restriction on O_c. Then K^*G_c/K^* is an open subgroup of finite index in the idèle class group J_K/K^*; hence via the reciprocity map K^*G_c/K^* corresponds to a finite abelian galois extension field $K[c]$ of K.

(2.3.3) The field extension $K[c]/K$ defined in (2.3.2) is called the *ring class field extension with conductor c.*

(2.3.4) The Artin reciprocity map induces an isomorphism

$$\mathrm{Pic}(O_c) \cong \mathrm{Gal}(K[c]/K).$$

If $\mathfrak{p}$ is a prime ideal of B which is unramified in $K[c]/K$, then this isomorphism associates the Frobenius element at $\mathfrak{p}$ of the abelian Galois group $\mathrm{Gal}(K[c]/K)$ to the Cartier divisor class $[\mathfrak{p} \cap O_c]$ in $\mathrm{Pic}(O_c)$ of the locally free O_c-module $\mathfrak{p} \cap O_c$ of rank 1.

(2.3.5) Let $c \geq c'$ be effective divisors on C_{aff}. Then by (2.3.4), the galois group $\mathrm{Gal}(K[c]/K[c'])$ is naturally isomorphic to the kernel

$$\ker(\mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c'})). \tag{2.3.6}$$

Let $I(c)$ be the ideal of A defining the conductor c. By (2.2.13) we then obtain that if $c \neq 0$ there is a natural isomorphism

$$\mathrm{Gal}(K[c]/K[0]) \cong \frac{(B/I(c)B)^*}{(A/I(c)))^*}/(B^*/A^*). \tag{2.3.7}$$

More explicitly, if $c \neq 0$ and

$$c = \sum_{\mathfrak{p}} m_{\mathfrak{p}}.\mathfrak{p}$$

then we have the natural group isomorphism

$$\mathrm{Gal}(K[c]/K[0]) \;\cong\; \Big\{ \prod_{\mathfrak{p} \in \mathrm{Supp}(c)} (B/\mathfrak{p}^{m_{\mathfrak{p}}}B)^*/(A/\mathfrak{p}^{m_{\mathfrak{p}}})^* \Big\}/(B^*/A^*). \tag{2.3.8}$$

(2.3.9) In general, if $c > c' > 0$ then by (2.2.15) and (2.3.5) we obtain a natural isomorphism

$$\mathrm{Gal}(K[c]/K[c']) \cong \frac{(B/I(d)B)^*}{(A/I(d))^*} \prod_{\mathfrak{p} \in \mathrm{Supp}\ (c')} U(m_{\mathfrak{p}}, m'_{\mathfrak{p}}, \mathfrak{p}). \tag{2.3.10}$$

The product here is over all maximal ideals $\mathfrak{p}$ of A in the support of the divisor c' and, as in (2.2.15), the divisor d is the greatest effective divisor $\leq c$ and prime to c' and

$$m_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}} c, \quad m'_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}} c'.$$

(2.3.11) The numerical order of the Galois group $\mathrm{Gal}(K[c]/K[c'])$ is given by these formulae. For any prime divisor z of C_{aff}, define an integer $(z, K/F)$ in

$\mathbb{Z}$ by the recipe

$$(z, K/F) = \begin{cases} -1, & \text{if } z \text{ is inert in } K/F \\ +1, & \text{if } z \text{ splits completely in } K/F \\ 0, & \text{if } z \text{ ramifies in } K/F. \end{cases}$$

If n is a positive integer then from (2.3.8) we have that $K[n.z]/K[0]$ is a field extension of degree

$$|\kappa(z)|^{n-1}(|\kappa(z)| - (z, K/F))/|B^*/A^*|.$$

The extension $K[z]/K[0]$ is cyclic if z is inert or splits completely in K/F, but need not be cyclic if z is ramified in K/F.

(2.3.12) Let z be a prime divisor in $\mathrm{Supp}(c)$ where $c \in \mathrm{Div}_+(A)$, $c \neq 0$.
(a) If $c - z \neq 0$ then the field extension $K[c]/K[c-z]$ has degree equal to

$$\begin{cases} |\kappa(z)| - (z, K/F), & \text{if } z \notin \mathrm{Supp}(c-z) \\ |\kappa(z)|, & \text{if } z \in \mathrm{Supp}(c-z). \end{cases}$$

(b) If $z \notin \mathrm{Supp}(c-z)$ and either z is inert or split completely in K/F then $\mathrm{Gal}(K[c]/K[c-z])$ is cyclic of order prime to the characteristic of F.

On the other hand, if either $z \in \mathrm{Supp}(c-z)$ or z is ramified in K/F then $\mathrm{Gal}(K[c]/K[c-z])$ is a direct sum of cyclic groups of prime order equal to the characteristic of the field F.
(c) The group $\mathrm{Gal}(K[c]/K[c-z])$ is *pure* that is to say a direct sum of cyclic groups of the same order.

[Part (c) follows from (b). The parts (a) and (b) follow from the explicit description of the group $G = \mathrm{Gal}(K[c]/K[c-z])$ given in (2.2.15) and (2.3.9) by considering the separate cases as we now check. Let $\mathfrak{p}$ be the prime ideal of the affine coordinate ring A corresponding to the point z.

Case 1. Assume that $z \notin \mathrm{Supp}(c-z)$.

Then we have an isomorphism

$$G \cong \begin{cases} (B/\mathfrak{p}B)^*/(A/\mathfrak{p})^* & \text{if } c - z \neq 0 \\ \dfrac{(B/\mathfrak{p}B)^*/(A/\mathfrak{p})^*}{B^*/A^*} & \text{if } c - z = 0. \end{cases}$$

(a) Suppose that $\mathfrak{p}$ is inert in the field extension K/F.

As $B/\mathfrak{p}B$ is a finite field its group $(B/\mathfrak{p}B)^*$ of non-zero elements is cyclic. Hence the group G is cyclic of order prime to the characteristic of F.

(b) Suppose that $\mathfrak{p}$ is split completely in the field extension K/F.

We have an isomorphism of rings

$$\frac{B}{\mathfrak{p}B} \cong \frac{A}{\mathfrak{p}} \times \frac{A}{\mathfrak{p}}.$$

Hence we have the isomorphism of groups

$$G \cong \begin{cases} (A/\mathfrak{p})^* & \text{if } c - z \neq 0 \\ \dfrac{(A/\mathfrak{p})^*}{B^*/A^*} & \text{if } c - z = 0. \end{cases}$$

Again $(A/\mathfrak{p})^*$ is a finite cyclic group as it is the group of units of a finite field; hence the group G is cyclic of order prime to the characteristic of F.

(c) Suppose that $\mathfrak{p}$ is ramified in the field extension K/F.

Let π be a local parameter of the infinitesimal trait $B/\mathfrak{p}B$ (definition 6.7.5). Then we have an isomorphism

$$(B/\mathfrak{p}B)^*/(A/\mathfrak{p})^* \cong (B/\pi^2 B)^*/(A/\mathfrak{p})^*.$$

As the residue field of $B/\mathfrak{p}B$ is isomorphic to $A/\mathfrak{p}$ we obtain an isomorphism of groups

$$(B/\mathfrak{p}B)^*/(A/\mathfrak{p})^* \cong (A/\mathfrak{p})^+$$

where $(A/\mathfrak{p})^+$ is the additive group if the field $A/\mathfrak{p}$. If the field extension K/F admits ramified primes such as $\mathfrak{p}$ then we have $B^* = A^*$ and hence G is isomorphic to the additive group of the field $A/\mathfrak{p}$ and hence is a direct sum of cyclic groups of order equal to the characteristic of F.

Case 2. Assume that $z \in \mathrm{Supp}(c - z)$.

Let $r \geq 1$ be the order of z in the divisor $c - z$. Then G is isomorphic to a kernel as follows

$$G \cong \ker\{(B/\mathfrak{p}^{r+1}B)^*/(A/\mathfrak{p}^{r+1})^* \to (B/\mathfrak{p}^r B)^*/(A/\mathfrak{p}^r)^*\}.$$

(a) Suppose that $\mathfrak{p}$ is inert in the field extension K/F.

As $\mathfrak{p}$ is inert in K/F the infinitesimal traits $B/\mathfrak{p}^{r+1}B$ (definition 6.7.5) and $A/\mathfrak{p}^{r+1}$ have the same local parameter π Hence G is isomorphic to the kernel of the natural homomorphism

$$G \cong \ker\{(B/\pi^{r+1}B)^*/(A/\pi^{r+1}A)^* \to (B/\pi^r B)^*/(A/\pi^r A)^*\}.$$

It follows that there is an isomorphism

$$G \cong (B/\pi B)^+/(A/\pi A)^+$$

where $(B/\pi B)^+$, $(A/\pi A)^+$ are the additive groups of the finite fields $B/\pi B$, $A/\pi A$. Hence G is a direct sum of cyclic groups of order equal to the characteristic of F.

(b) Suppose that $\mathfrak{p}$ is split completely in the field extension K/F.

Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the distinct prime ideals of B lying over $\mathfrak{p}$. Then we have isomorphisms

$$(B/\mathfrak{p}^{r+1}B)^*/(A/\mathfrak{p}^{r+1})^* \cong (B/\mathfrak{p}_1^{r+1})^* \times (B/\mathfrak{p}_2^{r+1})^*/(A/\mathfrak{p}^{r+1})^* \cong (A/\mathfrak{p}^{r+1})^*.$$

Hence we have a group isomorphism

$$G \cong \ker\{(A/\mathfrak{p}^{r+1})^* \to (A/\mathfrak{p}^r)^*\}.$$

As $r \geq 1$ it follows that we have an isomorphism $G \cong (A/\mathfrak{p})^+$; that is to say G is isomorphic to the additive group of the finite field $A/\mathfrak{p}$. Hence G is a direct sum of cyclic groups of order equal to the characteristic of F.

(c) Suppose that $\mathfrak{p}$ is ramified in the field extension K/F.

Let π be a local parameter of the infinitesimal trait $B/\mathfrak{p}B$ (definition 6.7.5). Then we have an isomorphism

$$(B/\mathfrak{p}^{r+1}B)^*/(A/\mathfrak{p}^{r+1})^* \cong (B/\pi^{2(r+1)}B)^*/(A/\mathfrak{p}^{r+1})^*.$$

Hence we have an isomorphism

$$G \cong \ker\{(B/\pi^{2(r+1)}B)^*/(A/\mathfrak{p}^{r+1})^* \to (B/\pi^{2r}B)^*/(A/\mathfrak{p}^r)^*\}.$$

As the residue field of $B/\mathfrak{p}B$ is isomorphic to $A/\mathfrak{p}$, we obtain an isomorphism $G \cong (A/\mathfrak{p})^+$ where $(A/\mathfrak{p})^+$ is the additive group if the field $A/\mathfrak{p}$. Hence G is a direct sum of cyclic groups of order equal to the characteristic of F.]

(2.3.13) Suppose that $c \in \mathrm{Div}_+(A)$ and z is a prime divisor of C_{aff}.

(a) The primes ramified in $K[c]/K$ are precisely the primes in the support of c.
(b) The extension $K[c]/K$ is split completely at the place of K lying above ∞.
(c) If $z \notin \mathrm{Supp}(c)$ then for any positive integer n, the galois extension $K[c+nz]/K[c]$ is totally ramified at all places of $K[c]$ above z.

[For the proof, assume that the prime divisor z of C_{aff} is not in the support of c. As in (2.3.2), let

$$G_{c+nz} = K_\infty^* \prod_{v \neq \infty} \hat{O}_{c+nz,v}^*$$

be the subgroup of the idèle group J_K which corresponds to the ring class field $K[c+nz]$ via the reciprocity map. Write C_K for the idèle class group J_K/K^*. Then we have a commutative diagram of abelian group homomorphisms

$$\begin{array}{ccccc} 0 \to \mathrm{Gal}(K[c+nz]/K[c]) & \to & \mathrm{Gal}(K[c+nz]/K) & \to & \mathrm{Gal}(K[c]/K) \to 0 \\ & & \uparrow & & \uparrow \\ & & C_K/K^*G_{c+nz}/K^* & \to & C_K/K^*G_c/K^* \end{array}$$

where the horizontal morphisms form an exact sequence and the vertical arrows are the reciprocity isomorphisms. Let w be a prime of K lying over the prime z of F. Let U denote the subgroup of C_K given by the idèles $(1, 1, \ldots, 1, a_w, 1, \ldots)$ where a_w is the w-component of the idèle and a_w is a unit in the completion of K at w (i.e. a_w is a unit of the corresponding discrete valuation ring). By the above diagram, (2.3.8), and (2.3.10), the image of U in $\mathrm{Gal}(K[c+nz]/K)$ is precisely the subgroup $\mathrm{Gal}(K[c+nz]/K[c])$. It follows that the inertia group of w in $\mathrm{Gal}(K[c+nz]/K)$ is equal to $\mathrm{Gal}(K[c+nz]/K[c])$. Therefore the primes of K above z are unramified in the extension $K[c]/K$ and the primes above z in $K[c]$ are totally ramified in the field extension $K[c+nz]/K[c]$. This proves (c); parts (a) and (b) are obvious by class field theory.]

2.4 The Drinfeld moduli schemes $\mathbf{Y}_0^{\mathrm{Drin}}(I), \mathbf{X}_0^{\mathrm{Drin}}(I)$, M_I^d

We give a few brief remarks on the basic geometric properties of the Drinfeld moduli schemes $\mathbf{Y}_0^{\mathrm{Drin}}(I)$, $\mathbf{X}_0^{\mathrm{Drin}}(I)$, and M_I^d. For some further details on these moduli schemes as well as the moduli scheme M_H^d, see appendices A and B. For properties of the generic fibres of these moduli schemes, which are curves over global fields of positive characteristic, see [Ge].

(2.4.1) Let I be a non-zero ideal of A. Let S be a locally noetherian A-scheme and D/S a Drinfeld module of rank 2 for A. We may assume that D is a standard Drinfeld module given by the pair $(G_{\mathcal{L}}, \phi)$, where $\mathcal{L}$ is a line bundle $\mathcal{L}$ on S, where $G_{\mathcal{L}}$ is the additive S-group scheme $\mathbf{Spec}_{O_S} \bigoplus_{n=0}^{\infty} \mathcal{L}^{\otimes n}$, and where $\phi : A \to \mathrm{End}(G_{\mathcal{L}})$ is a k-algebra homomorphism.

2.4.2. Definition. An *I-cyclic subgroup Z of D/S* is a finite flat subgroup scheme Z/S of $G_{\mathcal{L}}/S$ and a homomorphism of A-modules

$$\psi : A/I \to G_{\mathcal{L}}(S)$$

such that there is an equality of relative Cartier divisors of $G_{\mathcal{L}}/S$

$$\sum_{m \in A/I} \psi(m) = Z.$$

2.4.3. Remark. For the case where $A = \mathbb{F}_q[T]$, an I-cyclic subgroup of D/S was defined in [Br2, Definition 2.6.1]. The above definition is an immediate generalisation of this case.

This method of defining supplementary structures on moduli problems, by equality of Cartier divisors, is due to Drinfeld. It equally applies to moduli of elliptic curves (see [KM]); by this means some technical difficulties that formerly arose in the theory of moduli of elliptic curves are avoided.

(2.4.4) Let $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ denote the coarse moduli scheme of rank 2 Drinfeld modules equipped with a cyclic I-structure; that is to say, $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ is a coarse moduli scheme for the functor on the category $A - \mathcal{S}ch$ of locally noetherian A-schemes given by

$$A - \mathcal{S}ch \to \mathcal{S}ets$$
$$S \mapsto \left\{ \begin{array}{c} S - \text{isomorphism classes of pairs } (D, Z) \text{ where} \\ D/S \text{ is a Drinfeld module of rank 2 and } Z/S \text{ is an} \\ I - \text{cyclic subgroup of } D \end{array} \right\}$$

(2.4.5) If L is an algebraically closed field then the L-valued points of $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ are represented by pairs (D, Z) where D/L is a Drinfeld module of rank 2 for A and Z/L is an I-cyclic subgroup of D.

(2.4.6) For any integer $d \geq 0$, let M_I^d denote the coarse moduli scheme of Drinfeld modules for A of rank d equipped with a full level I-structure.

If Spec A/I contains at least two elements then M_I^d is a fine moduli scheme for Drinfeld modules of rank d equipped with a full level I-structure [Dr, Prop. 5.3]. In this case, M_I^d is a smooth k-scheme and the map $M_I^d \to$ Spec A is smooth over Spec A outside of the closed subscheme Spec A/I (see [Dr, Cor. to Prop. 5.4]).

(2.4.7) The k-scheme $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ is normal and 2-dimensional. Furthermore, $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ is an A-scheme of finite type. Provided that Spec A/I has at least 2 elements, then $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ may be obtained as the quotient by a finite group of the fine moduli scheme M_I^2.

Let $F[0]$ be the Hilbert classs field of F, that is to say $F[0]$ is the maximal unramified abelian extension of F which is split completely at ∞. We write $Y_0^{\mathrm{Drin}}(I)/F$ for the generic fibre of the A-scheme $\mathbf{Y}_0^{\mathrm{Drin}}(I)/A$. Then the exact field of constants of $Y_0^{\mathrm{Drin}}(I)/F$ is $F[0]$ (see [GR, §8.3]).

As the generic fibre of $\mathbf{Y}_0^{\mathrm{Drin}}(I)/A$ is a smooth curve defined over the field $F[0]$ we have that the normal surface $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ is fibred over Spec $A[0]$, where $A[0]$ is the integral closure of A in the Hilbert class field $F[0]$ of F. Furthermore, $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ as a k-scheme has only a finite number of isolated singular points. These singular points only occur at points corresponding to the supersingular Drinfeld modules of finite characteristic dividing I. By blowing up

these singular points we obtain a smooth surface which is the minimal smooth desingularisation of $\mathbf{Y}_0^{\mathrm{Drin}}(I)$.

(2.4.8) The A-scheme $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ may be compactified to a scheme $\mathbf{X}_0^{\mathrm{Drin}}(I)/A$ by adding the cusps to the surface $\mathbf{Y}_0^{\mathrm{Drin}}(I)$. The generic fibre of $\mathbf{X}_0^{\mathrm{Drin}}(I)/A$ is a smooth curve defined over $F[0]$ and written $X_0^{\mathrm{Drin}}(I)/F[0]$.

Write $J(I)/F[0]$ for the jacobian of the smooth curve $X_0^{\mathrm{Drin}}(I)/F[0]$.

2.4.9. Theorem. *The abelian variety $J(I)/F[0]$ has good reduction at all places of $F[0]$ prime to I and ∞. The cusps of $X_0^{\mathrm{Drin}}(I)/F[0]$ generate a torsion subgroup of $J(I)(\overline{F})$, where $\overline{F}$ is the algebraic closure of F.*

Proof. That $J(I)/F[0]$ has good reduction at all places prime to Supp I and ∞ follows from the modular interpretation of the reduction of the scheme $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ at such places. That the cusps generate a torsion subgroup is a consequence of [G, Chapter VI, Corollary 5.12]. □

(2.4.10) Let

F_∞ be the completion at ∞ of F;
$\overline{F}_\infty$ be the algebraic closure of F_∞;
$\hat{\overline{F}}_\infty$ be the completion at a place above ∞ of $\overline{F}_\infty$;
$\Omega = \hat{\overline{F}}_\infty - F_\infty$ be the Drinfeld "upper half-plane".

The group $\mathrm{GL}(2, A)$, of invertible 2×2-matrices with coefficients in A, acts on Ω via homographic transformations; that is to say, if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, A)$ and $\omega \in \Omega$, then we have

$$g\omega = \frac{a\omega + b}{c\omega + d}.$$

Let Γ be a discrete subgroup of $\mathrm{GL}(2, A)$. Then the quotient space $\Gamma\backslash\Omega$ may be equipped with the sructure of a rigid analytic space over F_∞ (see [Dr], [GR]).

Let $\Gamma_0(I)$ be the congruence (discrete) subgroup of $\mathrm{GL}(2, A)$ given by

$$\Gamma_0(I) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, A) \mid c \equiv 0 \text{ (modulo } I)\}.$$

Fix an embedding $\sigma : F[0] \hookrightarrow \hat{\overline{F}}_\infty$. Then the set $Y_0^{\mathrm{Drin}}(I)(\hat{\overline{F}}_\infty)$ of $\hat{\overline{F}}_\infty$-valued points of the curve $Y_0^{\mathrm{Drin}}(I)/F[0]$ is also a rigid analytic space over F_∞ and

there is an isomorphism of rigid analytic spaces

$$Y_0^{\mathrm{Drin}}(I)(\widehat{\overline{F}}_\infty) \cong \Gamma_0(I)\backslash\Omega.$$

[For more details on Drinfeld moduli schemes as rigid analytic spaces, see appendices A and B.]

2.5 Complex multiplication of rank 2 Drinfeld modules

(2.5.1) For any non-zero ideal I of A such that Spec A/I contains at least two elements, let M_I^1 be the fine moduli scheme of rank 1 Drinfeld modules for A with a full level I-structure (see (2.4.6)). Let

$$M^1 = \lim_{\leftarrow} M_I^1$$

where I runs over all ideals of A such that Spec A/I contains at least two elements.

(2.5.2) Let J_F^f be the idèle group of F without the component at ∞; that is to say, the idèle group of F is $J_F = F_\infty^* \times J_F^f$. The group F^* is a subgroup of J_F^f and we write J_F^f/F^* for the quotient group i.e. the idèle class group without the component at ∞.

(2.5.3) The group J_F^f/F^* acts on M^1 as follows. Let S be a locally noetherian A-scheme; let D/S be a Drinfeld module of rank 1 for A equipped with a homomorphism of A-modules

$$\psi : F/A \to D(S)$$

such that for any non-zero ideal I of A the restriction of ψ to I^{-1}/A is a full level I-structure on D.

As the A-module F/A is torsion and the annihilator of every element is a finite group, the action of A on F/A extends to a module action of the profinite completion $\hat{A}$ of A on F/A. Let $a \in \hat{A}$ be a non-zero element; the kernel P of a on F/A is finite. The divisor $H \subset D$ which is equal to

$$H = \sum_{b \in P} \psi(b)$$

is an A-invariant subgroup scheme of D; hence the quotient D/H is a rank 1 Drinfeld module for A. Define the map $\psi_1 : F/A \to (D/H)(S)$ so that the following diagram is commutative

$$\begin{array}{ccc} & \overset{\psi}{} & \\ F/A & \to & D(S) \\ a\downarrow & & \downarrow \\ F/A & \to & (D/H)(S) \\ & \underset{\psi_1}{} & \end{array}$$

Then the restriction of ψ_1 to I^{-1}/A, for any non-zero ideal I, is a full level I-structure of D/H. This defines an action on the left by the multiplicative monoid $\hat{A} - \{0\}$ on the pairs (D, ψ) and hence an action of $\hat{A} - \{0\}$ on M^1. The non-zero elements of A contained in $\hat{A}$ act trivially on M^1. Hence we obtain an action of the quotient $\hat{A} - \{0\}/A - \{0\}$ of multiplicative monoids on M^1; this quotient of monoids is a group isomorphic to J_F^f/F^* and this defines the action of J_F^f/F^* on M^1.

2.5.4. Main Theorem of Complex Multiplication. (Drinfeld [Dr, §8]). *The scheme M^1 is the spectrum of the ring of ∞-integers of the maximal abelian extension of F which is split completely at ∞. Furthermore, the action of J_F^f/F^* on M^1 coincides with the galois action of* $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ *on M^1 via the reciprocity map $J_F/F^* \to \mathrm{Gal}(F^{\mathrm{sep}}/F)$.* □

(2.5.5) Let D be a Drinfeld module of rank 2 for A of infinite characteristic and defined over a field L. Let $\mathrm{End}(D)$ denote the A-algebra of endomorphisms of D.

The Drinfeld module D is said to have complex multiplication if $\mathrm{End}(D)$ is commutative and

$$\dim_F \mathrm{End}(D) \otimes_A F = 2.$$

In this event, $K = \mathrm{End}(D) \otimes_A F$ is an imaginary quadratic field extension of F and $\mathrm{End}(D)$ is an order O_c of K relative to A of conductor c, say.

By the main theorem of complex multiplication of Drinfeld modules, D can be defined over the ring class field $K[c]$ of K. There are precisely $[K[c] : K]$ isomorphism classes of Drinfeld modules of rank 2 with complex multiplication by O_c and they are permuted transitively by the Galois group $\mathrm{Gal}(K[c]/K)$.

(2.5.6) A finite group G is called *generalised dihedral* if there are subgroups H, C_2 of G such that H is an abelian normal subgroup, C_2 is a cyclic subgroup of order 2, and G is the semi-direct product of H and C_2, that is to say there is a short exact exact sequence of finite groups

$$0 \quad \to \quad H \quad \to \quad G \quad \stackrel{f}{\to} \quad C_2 \quad \to \quad 0$$

where the restriction of the homomorphism f to the subgroup C_2 is the identity.

Assume that G is generalised dihedral with the corresponding abelian subgroups H, C_2 as in the previous definition. Then the elements of C_2 act via conjugation on H. Let H^{C_2} be the subgroup of H which is invariant under the action of C_2. Let σ be the non-trivial element of the subgroup C_2. Then there is a norm homomorphism

$$N_{C_2} : H \to H^{C_2}, \quad h \mapsto h\sigma h\sigma^{-1}.$$

The composition law on the group G is then completely determined by the two abelian groups H, C_2, the homomorphism $N_{C_2} : H \to H$, and the relation

$$h\sigma = N_{C_2}(h)\sigma h^{-1} \quad \text{for all } h \in H.$$

2.5.7. Proposition. (i) *The finite group* $\mathrm{Gal}(K[c]/F)$ *is generalised dihedral. There is a short exact sequence of groups where* $\mathrm{Gal}(K[c]/K)$ *is an abelian normal subgroup and* $\mathrm{Gal}(K/F)$ *is a cyclic subgroup of order 2 of* $\mathrm{Gal}(K[c]/F)$ *and the restriction of* f *to* $\mathrm{Gal}(K/F)$ *is the identity*

$$0 \to \mathrm{Gal}(K[c]/K) \to \mathrm{Gal}(K[c]/F) \xrightarrow{f} \mathrm{Gal}(K/F) \to 0.$$

(ii) *The group* $\mathrm{Pic}(A)$ *is naturally isomorphic to a subgroup of* $\mathrm{Gal}(K[c]/K)^{\mathrm{Gal}(K/F)}$ *and the norm homomorphism* $N_{K/F} : \mathrm{Gal}(K[c]/F) \to \mathrm{Gal}(K[c]/F)^{\mathrm{Gal}(K/F)}$ *factors as*

$$\mathrm{Gal}(K[c]/K) \to \mathrm{Pic}(A) \hookrightarrow \mathrm{Gal}(K[c]/K)^{\mathrm{Gal}(K/F)}.$$

Proof. Let $F[0]$ be the maximal unramified abelian extension of F which is split completely at ∞. Then $F[0]$ is a subfield of $K[c]$, as the join $F[0].K$ of the fields $F[0]$ and K in the separable closure of K is an abelian unramified extension of K which is split completely at the prime of K above ∞. The reciprocity maps give a commutative diagram

$$\begin{array}{ccc} & \overset{\cong}{\to} & \\ \mathrm{Pic}(A) & \to & \mathrm{Gal}(F[0]/F) \\ N_{K/F} \uparrow & & \uparrow \\ \mathrm{Pic}(O_c) & \to & \mathrm{Gal}(K[c]/K) \\ & \underset{\cong}{\to} & \end{array}$$

where the horizontal maps are the reciprocity isomorphisms. The vertical homomorphism $\mathrm{Pic}(O_c) \to \mathrm{Pic}(A)$ is the norm $N_{K/F}$ and the homomorphism $\mathrm{Gal}(K[c]/K) \to \mathrm{Gal}(F[0]/F)$ is the restriction of the galois group $\mathrm{Gal}(K[c]/K)$ to the subfield $F[0]$ of $K[c]$.

The restriction of the galois group $\mathrm{Gal}(K_\infty/F_\infty)$ to $K[c]$ gives a homomorphism

$$\mathrm{Gal}(K_\infty/F_\infty) \to \mathrm{Gal}(K[c]/F)$$

whose image is a subgroup C_2 of $\mathrm{Gal}(K[c]/F)$ order 2.

The restriction homomorphism $\mathrm{Gal}(K[c]/F) \to \mathrm{Gal}(K/F)$ gives rise to the exact sequence of galois groups

$$0 \to \mathrm{Gal}(K[c]/K) \to \mathrm{Gal}(K[c]/F) \to \mathrm{Gal}(K/F) \to 0.$$

In particular, $\mathrm{Gal}(K[c]/K)$ is an abelian normal subgroup of $\mathrm{Gal}(K[c]/F)$ and we have that $\mathrm{Gal}(K[c]/F)$ is a semi-direct product of the subgroups C_2 and $\mathrm{Gal}(K[c]/K)$. This proves that $\mathrm{Gal}(K[c]/F)$ is a generalised dihedral group and proves part (i).

Let $\mathrm{Ca}(O_c)$ be the group of Cartier divisors on Spec O_c. Then we have a short exact sequence of abelian groups

$$0 \to K^* \to \mathrm{Ca}(O_c) \to \mathrm{Pic}(O_c) \to 0.$$

The group $\mathrm{Gal}(K/F)$ acts on the component groups of this exact sequence; taking invariants, we obtain the commutative diagram whose rows are short exact sequences, as $H^1(\mathrm{Gal}(K/F), K^*) = 0$,

$$\begin{array}{ccccccccc} 0 & \to & F^* & \to & (\mathrm{Ca}(O_c))^{\mathrm{Gal}(K/F)} & \to & (\mathrm{Pic}(O_c))^{\mathrm{Gal}(K/F)} & \to & 0 \\ & & \cong\uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & F^* & \to & \mathrm{Ca}(A) & \to & \mathrm{Pic}(A) & \to & 0 \end{array}$$

The canonical isomorphisms

$$\mathrm{Ca}(B) \cong \mathrm{Div}(B), \quad \mathrm{Ca}(A) \cong \mathrm{Div}(A)$$

where $\mathrm{Div}(B)$ is the group of Weil divisors on the normal scheme Spec B, then shows that the natural homomorphism

$$\mathrm{Ca}(A) \to \mathrm{Ca}(B)$$

is injective. Taking $c = 0$ in the previous diagram, it follows that the homomorphism

$$\mathrm{Pic}(A) \to (\mathrm{Pic}(B))^{\mathrm{Gal}(K/F)}$$

is an injection. As this injection factors through the homomorphism

$$(\mathrm{Pic}(O_c))^{\mathrm{Gal}(K/F)} \to (\mathrm{Pic}(B))^{\mathrm{Gal}(K/F)}$$

it follows that the homomorphism

$$\mathrm{Pic}(A) \to (\mathrm{Pic}(O_c))^{\mathrm{Gal}(K/F)}$$

is injective.

The above diagram with $c = 0$ provides the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \to & F^* & \to & \mathrm{Div}(A) & \to & \mathrm{Pic}(A) & \to & 0 \\ & & \cong\downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & F^* & \to & \mathrm{Div}(B)^{\mathrm{Gal}(K/F)} & \to & \mathrm{Pic}(B)^{\mathrm{Gal}(K/F)} & \to & 0 \\ & & N_{K/F}\uparrow & & N_{K/F}\uparrow & & N_{K/F}\uparrow & & \\ 0 & \to & K^* & \to & \mathrm{Div}(B) & \to & \mathrm{Pic}(B) & \to & 0 \end{array}$$

A diagram chase shows that the subgroup $N_{K/F}(\mathrm{Pic}(B))$ is contained in the image of $\mathrm{Pic}(A)$ in $\mathrm{Pic}(B)$.

Suppose now that $c \geq 0$ is any divisor of $\mathrm{Div}_+(A)$. We have the exact sequence of abelian groups, from (2.3.8),

$$0 \to I \to \mathrm{Pic}(O_c) \to \mathrm{Pic}(B) \to 0$$

where the kernel I is the subgroup

$$I \cong \Big\{ \prod_{\mathfrak{p} \in \mathrm{Supp}(c)} (B/\mathfrak{p}^{m_\mathfrak{p}} B)^* / (A/\mathfrak{p}^{m_\mathfrak{p}})^* \Big\} / (B^*/A^*).$$

It follows that the norm $N_{K/F} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_c)$ lies in the commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & I & \to & \mathrm{Pic}(O_c) & \to & \mathrm{Pic}(B) & \to & 0 \\ & & & & N_{K/F} \downarrow & & N_{K/F} \downarrow & & \\ & & & & N_{K/F}(\mathrm{Pic}(O_c)) & \overset{\cong}{\to} & N_{K/F}(\mathrm{Pic}(B)) & & \end{array}$$

It follows from this and that the subgroup $N_{K/F}(\mathrm{Pic}(B))$ is contained in the image of $\mathrm{Pic}(A)$ in $\mathrm{Pic}(B)$, that we have $N_{K/F}(\mathrm{Pic}(O_c))$ is contained in the subgroup $\mathrm{Pic}(A)$ of $\mathrm{Pic}(O_c)$. This proves (ii).

The composition law of the group $\mathrm{Gal}(K[c]/F)$ may be written as follows. Let σ be the non-trivial element of order 2 of the subgroup C_2 of $\mathrm{Gal}(K[c]/F)$. Let $h \in \mathrm{Gal}(K[c]/K)$. Then we have $\sigma h \sigma^{-1} \in \mathrm{Gal}(K[c]/K)$ and

$$h \sigma h \sigma^{-1} = N_{K/F}(h) \in \mathrm{Pic}(A). \qquad \square$$

2.5.8. Remark. A different proof of this proposition for the rational function field case is given in [Br1, Prop. 2.5.6].

3

Bruhat-Tits trees with complex multiplication

Let

E be a global field;
$\mathcal{S}$ be a non-empty set of places of E containing all the archimedean places, if any;
E' be a quadratic extension field of E;
R be the ring of $\mathcal{S}$-integers of E;
Λ be an R-sublattice of rank 2 of E';
$\mathrm{End}_R^{E'}(\Lambda) = \{m \in E' |\ m\Lambda \subseteq \Lambda\}$ be the subring of E' of elements which are R-endomorphisms of Λ.

The principal problem of this chapter is to determine this ring of endomorphisms $\mathrm{End}_R^{E'}(\Lambda)$ of the lattice Λ.

For the case where R is a discrete valuation ring, we introduce in §3.6 "Bruhat-Tits trees with complex multiplication" which describe precisely the ring of endomorphisms $\mathrm{End}_R^{E'}(\Lambda)$. We show that for the case of rank 2 lattices over discrete valuation rings only 3 types of Bruhat-Tits trees with complex multiplication arise; these are represented diagrammatically in the figures 1, 2, and 3 of §3.8. A 4th type also occurs for the case of non-reduced quadratic algebras (figure 4 of §3.8).

For the general case of rings of $\mathcal{S}$-integers of global fields, we define a "Bruhat-Tits net" in §3.10 which is essentially a union of all the local Bruhat-Tits trees; a Bruhat-Tits net resembles pictorially a spider's web.

The results of this chapter are applied in the next to the action of the Hecke operators on Drinfeld-Heegner points. The results here apply equally to the action of Hecke operators on classical modular curves.

M.L. Brown: LNM 1849, pp. 31–74, 2004.

3.1 The Bruhat-Tits building Δ for SL_2 of a discretely valued field

We shall describe the *Bruhat-Tits building* $\Delta(\mathrm{SL}_2(L))$ of the group $\mathrm{SL}_2(L)$ relative to the discrete valuation v of a field L. For more details see [Bro2, Chap. 5, §8] and Appendix B, §B.1.

(3.1.1) Let

R be a discrete valuation ring;
L be the fraction field of R;
$\pi \in R$ be a local parameter of R;
v be the corresponding discrete valuation on L normalised so that $v(\pi) = 1$.

(3.1.2) Let V be a 2-dimensional vector space over L. A *lattice* in V is a finitely generated R-submodule of V which generates V as a vector space over L. Evidently, a lattice is then a free R-module of rank 2.

(3.1.3) We may define these relations between lattices of V:

(1) Two lattices Λ, Λ' of V are *equivalent* if there is $a \in L^*$ such that

$$a\Lambda = \Lambda'.$$

Equivalence of lattices is an equivalence relation. For a lattice Λ in V we write $[\Lambda]$ for the corresponding lattice class.

(2) Two lattice classes $[\Lambda], [\Lambda']$ of V are *incident* if they admit representative lattices Λ, Λ' such that

$$\pi\Lambda \subset \Lambda' \subset \Lambda.$$

The relation of incidence is symmetric and reflexive amongst the lattice classes.

(3.1.4) The group $\mathrm{GL}_2(L)$ acts in a natural way on the set of lattice classes of V. This permutation action is transitive and the stabilizer of a given lattice class is the product of the subgroup of homotheties of $\mathrm{GL}_2(L)$ with the group of automorphisms of the lattice.

(3.1.5) Fix a lattice class $[\Lambda_0]$ of V. For any lattice class $[\Lambda]$ of V there is (by (3.1.4)) an element $g \in \mathrm{GL}_2(L)$, uniquely determined up to multiplication by a homothety and an automorphism of Λ_0, such that $g[\Lambda] = [\Lambda_0]$. Let $\det(g) \in L^*$ be the determinant of g; the parity of the integer $v(\det(g))$,

which is the valuation of $\det(g)$, is independent of the choice of g and depends only on $[\Lambda]$ and $[\Lambda_0]$.

The *type* of the lattice class $[\Lambda]$ is defined to be the parity of the integer $v(\det(g))$.

(3.1.6) The set $\mathcal{L}$ of lattice classes of V with the relation of incidence is a *plane incidence geometry*.

A *flag* in the plane incidence geometry $\mathcal{L}$ is a set of pairwise incident elements; the *flag complex* associated to $\mathcal{L}$ is a simplicial complex Δ which has $\mathcal{L}$ as a vertex set and the finite flags as simplices. The *type* of a vertex of the simplicial complex Δ is then the type of a lattice class as described in (3.1.5).

The *Bruhat-Tits building* $\Delta(\mathrm{SL}_2(L))$ is then the flag complex Δ equipped with the labelling of vertices given by their type. Indeed, Δ is a *Euclidean building* as its apartments are Euclidean Coxeter complexes [Bro2, Chap. VI,§2].

(3.1.7) The underlying simplicial complex of the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$ of $\mathrm{SL}_2(L)$ is a *tree*.

Fix a lattice $\Lambda = Re_1 \oplus Re_2$ in V; then a fundamental apartment Σ of $\Delta(\mathrm{SL}_2(L))$ is an (infinite) line in the tree Δ with vertices $[R\pi^a e_1 \oplus R\pi^b e_2]$ where the exponents $a, b \in \mathbb{Z}$ run through all positive and negative integers. All other apartments of $\Delta(\mathrm{SL}_2(L))$ are of the form $g\Sigma$ where $g \in \mathrm{GL}_2(L)$.

(3.1.8) The *standard metric* d on the Euclidean building $\Delta(\mathrm{SL}_2(L))$ is defined as follows. Given any two points x, y of $\Delta(\mathrm{SL}_2(L))$ there is an apartment E containing x and y and which is a Euclidean space with metric d_E; put

$$d(x, y) = d_E(x, y).$$

It is readily checked that this is independent of the choice of apartment E. This defines the metric d on $\Delta(\mathrm{SL}_2(L))$ up to multiplication by a real scalar. For more details, see [Bro2, Chap VI,§3].

It is convenient to normalise the standard metric d by setting the distance between any two adjacent vertices of the tree $\Delta(\mathrm{SL}_2(L))$ to be 1.

3.2 Lattices in quadratic extensions: elementary results

We give some preliminary results on rank 2 lattices over an excellent discrete valuation ring. The straightforward proofs here are omitted.

(3.2.1) Let

R be an excellent discrete valuation ring;
L be the field of fractions of R;
π be a local parameter of R;
v be the discrete valuation on L normalised so that $v(\pi) = 1$;
V be a 2-dimensional vector space over L with basis e_1, e_2;
Λ_0 be the R-sublattice of V given by

$$\Lambda_0 = Re_1 \oplus Re_2.$$

(3.2.2) For a sublattice Λ_1 of Λ_0, the *invariants* $\mathrm{inv}(\Lambda)$ of Λ_1, relative to Λ_0, are a pair of non-negative integers (n_1, n_2) where $0 \leq n_1 \leq n_2$, and where there is an isomorphism of R-modules

$$\frac{\Lambda_0}{\Lambda_1} \cong \frac{R}{(\pi^{n_1})} \oplus \frac{R}{(\pi^{n_2})}.$$

If Λ is an R-lattice of V, the *invariants* $\mathrm{inv}(\Lambda)$ of Λ relative to Λ_0 are then defined to be the sequence of invariants of $a\Lambda$ relative to Λ_0 minus $v(a)$ where a is any element of L^* such that $a\Lambda \subset \Lambda_0$; that is to say

$$\mathrm{inv}(\Lambda) = (n_1, n_2) \in \mathbb{Z}^2$$

where $(n_1 + v(a), n_2 + v(a))$ are the invariants of $a\Lambda$ relative to Λ_0. It is easily checked that the sequence $\mathrm{inv}(\Lambda)$ is uniquely determined by the lattice Λ and is independent of the choice of the element $a \in L^*$.

(3.2.3) The *index* $[\Lambda_0 : \Lambda]$ is the fractionary ideal of R given by

$$[\Lambda_0 : \Lambda] = (\pi^{n_1+n_2})R$$

where $\mathrm{inv}(\Lambda) = (n_1, n_2)$. As Λ and Λ_0 are isomorphic R-modules, there is an invertible linear map $l : V \to V$ such that $l(\Lambda_0) = \Lambda$; the index is then also given by the formula

$$[\Lambda_0 : \Lambda] = \det(l)R.$$

(3.2.4) Let Λ be an R-sublattice of V. Then Λ has a basis over R of the form $ae_1 + be_2, de_2$ where $a, b, d \in L$, $a \neq 0$, $d \neq 0$. We have $\Lambda \subset \Lambda_0$ if and only if a, b and d all belong to R.

We have these formulae for the index and invariants of Λ

$$[\Lambda_0 : \Lambda] = adR$$

$$\mathrm{inv}(\Lambda) = \begin{cases} (v(b), v(ad/b)), & \text{if } |a| < |b| > |d| \\ (v(a), v(d)) \text{ or } (v(d), v(a)), & \text{otherwise.} \end{cases}$$

(3.2.5) Let Λ, Λ' be sublattices of Λ_0 with bases over R of the form ae_1+be_2, de_2 and $a'e_1 + b'e_2, d'e_2$ respectively. Then we have $\Lambda \supset \Lambda'$ if and only if

$$a \text{ divides } a'$$

$$d \text{ divides } d'$$

$$b' \equiv \frac{a'}{a} b \text{ (modulo } d).$$

The index $[\Lambda : \Lambda']$ is given by

$$[\Lambda : \Lambda'] = \frac{a'd'}{ad} R.$$

(3.2.6) Let Λ and Λ' be the two lattices of (3.2.5). Then we have $\Lambda = \Lambda'$ if and only if there are units $\epsilon_1, \epsilon_2 \in R^*$ such that

$$a = \epsilon_1 a'$$

$$d = \epsilon_2 d'$$

$$b' \equiv \frac{a'}{a} b \text{ (modulo } d).$$

(3.2.7) Let Λ be the lattice of (3.2.5). The distinct sublattices of Λ of index πR are those with a basis over R either given by

$$\pi a e_1 + \pi b e_2, d e_2$$

or given by

$$a e_1 + (b + rd) e_2, \pi d e_2$$

where $r \in R$ runs through representatives of the residue field $R/\pi R$ of R. In particular, the set of such lattices bijects with the elements of the projective line $\mathbb{P}_1(R/\pi R)$.

[This follows from the properties (3.2.4) and (3.2.6).]

3.3 Lattices in quadratic extensions: discrete valuation rings

Let R, v, π, L be as in the preceding section §3.2. Let

M/L be a finite dimensional commutative L-algebra;
S be the integral closure of R in M;
Λ be an R-lattice in M;
$\mathrm{End}_R^M(\Lambda)$ be the endomorphism ring of the lattice Λ with respect to M, that is to say $\mathrm{End}_R^M(\Lambda)$ is the subring of M given by $\{x \in M |\, x\Lambda \subset \Lambda\}$.

All the propositions of this section are proved in the next section §3.4.

3.3.1. Proposition. *Assume that the algebra M is a 2-dimensional L-vector space. Then we have:*
(i) *The algebra M is L-isomorphic to one of these algebras*
  (a) *a field;*
  (b) *the direct product $L \times L$, where L is embedded diagonally in the product;*
  (c) *the non-reduced algebra $L[\epsilon]/(\epsilon^2)$.*
(ii) *The algebra M is equipped with a multiplicative norm*

$$N_{M/L} : M \to L.$$

(iii) *For any lattice Λ of M, the ring $\mathrm{End}_R^M(\Lambda)$ is a lattice in M and is a subring of S.*

3.3.2. Proposition. *Assume that the algebra M is a 2-dimensional L-vector space. Let S be the integral closure of R in M.*
(a) *If M is a field then S is a discrete valuation ring and is a free R-module of rank 2 with a basis $1, \tau$ for some $\tau \in S$.*
(b) *If M is L-isomorphic to $L \times L$ then S is R-isomorphic to $R \times R$.*
(c) *If M is L-isomorphic to $L[\epsilon]/(\epsilon^2)$ then S is isomorphic to the R-algebra $R \oplus L\epsilon$.*

3.3.3. Definitions. (i) For any non-empty subset $\mathcal{E}$ of L we put

$$v(\mathcal{E}) = \inf_{e\in\mathcal{E}} v(e).$$

(ii) Let Λ be an R-lattice in the 2-dimensional algebra M. The endomorphism ring $\mathrm{End}_R^M(\Lambda)$ is an R-lattice contained in the integral closure S (proposition 3.3.1(iii)).

If M is reduced, then S is an R-lattice (proposition 3.3.2) and the *conductor* of $\mathrm{End}_R^M(\Lambda)$ is defined to be

$$[S : \mathrm{End}_R^M(\Lambda)].$$

If M is not reduced we may fix an R-lattice Λ_0 of M and then the conductor of $\mathrm{End}_R^M(\Lambda)$ is defined to be

$$[\Lambda_0 : \mathrm{End}_R^M(\Lambda)].$$

The conductor of Λ, in all cases, is a fractionary ideal of R of the form $\pi^\alpha R$. The integer $\alpha \in \mathbb{Z}$ is the *exponent* $\mathrm{Exp}(\Lambda)$ *of the conductor* of Λ. That is to say, we have

$$\mathrm{Exp}(\Lambda) = v([\Lambda_0 : \mathrm{End}_R^M(\Lambda)])$$

where $\Lambda_0 = S$ if M is reduced.

3.3.4. Proposition. *Assume that M is a reduced 2-dimensional L-algebra. For an R-lattice Λ in M, we have*

$$\mathrm{Exp}(\Lambda) = \max(\mathrm{inv}(\Lambda) - v(\Lambda \cap L), v([S : \Lambda]) - v(N_{M/L}(\Lambda)).$$

3.3.5. Remarks. (i) To explain the notation of this last proposition, $\mathrm{inv}(\Lambda) - v(\Lambda \cap L)$ is the set of two integers $\lambda - v(\Lambda \cap L)$ where λ runs over the integer invariants of Λ; the maximum in the formula for $\mathrm{Exp}(\Lambda)$ in the proposition 3.3.4 is then the maximum of a set of 3 integers.

(ii) This last proposition 3.3.4 and its proof are similar to [K, §1, Proposition 2], which considered the case of endomorphism rings of rank 2 lattices over $\mathbb{Z}$.

(iii) The subring $\mathrm{End}_R^M(\Lambda)$ of M is uniquely determined by the integer $\mathrm{Exp}(\Lambda)$ (relative to Λ_0 if M is not reduced). That is to say, the ring of endomomorphisms of a lattice Λ is determined up to isomorphism by one integer $\mathrm{Exp}(\Lambda)$.

[This may be seen directly; it also follows from the proof of proposition 3.3.4 given in §3.4.]

(iv) The next result follows immediately from the definition of $\mathrm{Exp}(\Lambda)$ (defined relative to some fixed lattice Λ_0 if M is not reduced).

3.3.6. Proposition. *If M is 2-dimensional over L, then* $\mathrm{Exp}(\Lambda)$ *depends only on the equivalence class* $[\Lambda]$ *of the lattice* Λ *and hence* Exp *is induced from a map* $\mathcal{L} \to \mathbb{Z}$ *where* $\mathcal{L}$ *is the set of vertices of the Bruhat-Tits building* $\Delta(\mathrm{SL}_2(L))$ *with respect to the discrete valuation* v *(cf. §3.1).* □

3.4 Proofs of the propositions of §3.3

In this section, we prove Propositions 3.3.1, 3.3.2, and 3.3.4.

Proof of proposition 3.3.1. (i) As M is a commutative artin ring, we have that M is a direct product of local L-algebras. As M is a 2-dimensional L-algebra we conclude that M falls into one of these three distinct possibilites:

(a') M is a quadratic field extension of L;
(b') M is a direct product $M \cong L \times L$ of two copies of L where the structure map $L \to L \times L$ is the diagonal;
(c') M is a local non-reduced L-algebra.

The cases (a') and (b') correspond with the cases (a) and (b) of the proposition. Suppose that the algebra M is of type (c') above i.e. M is a local non-reduced L-algebra. Let N be the nil-radical of M. Then N is a proper ideal of M and is a sub-L-vector space of M. Hence we have

$$\dim_L N = 1.$$

Therefore the quotient algebra M/N is L-isomorphic to L. Let $\epsilon \in N$ be a basis of the vector space N. Then we have $N^2 \subseteq N$; the case where $N^2 = N$ is excluded by Nakayama's lemma. Therefore we have $N^2 = 0$ and hence $\epsilon^2 = 0$. We obtain then that M is isomorphic to $L[\epsilon]/(\epsilon^2)$; that is, M is of type (c) of the proposition. This is the required result.

(ii) The norm $N_{M/L} : M \to L$ is defined as follows: if $x \in M$ then $N_{M/L}(x)$ is the determinant of the L-linear map on M defined by multiplication by x.

(iii) As Λ is a free R-module of rank 2, we have that $\mathrm{End}_R^M(\Lambda)$ is isomorphic to an R-submodule of the free R-module $M_2(R)$ of 2×2 matrices with coefficients in R. Hence $\mathrm{End}_R^M(\Lambda)$ is a finitely generated R-module. Evidently, $\mathrm{End}_R^M(\Lambda)$ generates M as an L-vector space; hence $\mathrm{End}_R^M(\Lambda)$ is a lattice in M. □

Proof of proposition 3.3.2. In the case (c), where M is isomorphic to $L[\epsilon]/(\epsilon^2)$, it is evident that ϵ is an element integral over R and hence that the integral closure S of R is equal to $R \oplus L\epsilon$. This proves the result in this case.

If M is an étale L-algebra then S is a finite R-module; hence as R is a discrete valuation ring we obtain that S is a free R-module of rank 2. This proves the result in this case.

The remaining case to consider is where M/L is reduced and is not étale and hence M lies in possibility (a); that is to say, M is a purely inseparable quadratic extension field of L. As R is an excellent ring (see (3.2.1)), the ring S, which is the integral closure of R in M, is a finite R-module. As S is a torsion free R-module and M is 2-dimensional over L it follows that S is a finite free R-module of rank 2. It then follows (see (3.2.4)) that the elements $1, \tau$ form a basis of S over R for some element τ of S. □

Proof of proposition 3.3.4. The norm $N_{M/L} : M \to L$ (cf. Proposition 3.3.1(ii)) is given by $x.x^\sigma$ where $\sigma : M \to M$ is an involution if M/L is étale and σ is the identity if not.

We fix a basis $1, \tau$ for the free module S over R of rank 2 (see Proposition 3.3.2). Let Λ be an R-lattice contained in M. Then Λ is a free R-module of rank 2 and, by (3.2.4), has a basis

$$a\tau + b, d \tag{3.4.1}$$

where $a, b, d \in L$ and $a \neq 0$, $d \neq 0$.

Let I be the ideal of R given by

$$I = \{c \in R \mid c\tau\Lambda \subseteq \Lambda\}. \tag{3.4.2}$$

Then we have

$$\mathrm{End}_R^M(\Lambda) = R \oplus \tau I \tag{3.4.3}$$

and

$$\mathrm{Exp}(\Lambda) = v(I).$$

Let $c \in R$. We have

$$c\tau d \in \Lambda$$

if and only if there are $\alpha, \beta \in R$ such that

$$c\tau d = \alpha(a\tau + b) + \beta d;$$

this occurs if and only if a divides cd and there is $\beta \in R$ such that

$$(\frac{cd}{a})b + \beta d = 0.$$

Hence we have $c\tau d \in \Lambda$ if and only if a divides cd and a divides cb.

Furthermore, we have

$$c\tau(a\tau + b) \in \Lambda$$

if and only if there are $\gamma, \delta \in R$ such that

$$c\tau(a\tau + b) = \gamma(a\tau + b) + \delta d. \tag{3.4.4}$$

Write $\mathrm{Tr}_{M/L}(\tau)$ for the trace $\tau + \tau^\sigma$ of τ. As τ satisfies its own characteristic equation, we have

$$\tau^2 = \tau \mathrm{Tr}_{M/L}(\tau) - N_{M/L}(\tau).$$

Hence equation (3.4.4) becomes

$$c(a\mathrm{Tr}_{M/L}(\tau) + b)\tau - caN_{M/L}(\tau) = \gamma a\tau + (\gamma b + \delta d).$$

Hence $\gamma, \delta \in R$ exist satisfying (3.4.4) if and only if

$$\gamma = c\mathrm{Tr}_{M/L}(\tau) + \frac{cb}{a}$$

and

$$\delta d = -\gamma b - caN_{M/L}(\tau) = -\frac{c}{a}\big[b^2 + ba\mathrm{Tr}_{M/L}(\tau) + a^2 N_{M/L}(\tau)\big]$$

$$= -\frac{c}{a} N_{M/L}(a\tau + b).$$

Hence $\gamma, \delta \in R$ exist satisfying (3.4.4) if and only if ad divides $cN_{M/L}(a\tau + b)$ and a divides cb.

In summary, we have shown that $c \in R$ belongs to I if and only if these three conditions are fulfilled:

a divides cd
a divides cb
ad divides $cN_{M/L}(a\tau + b)$.

We therefore have that the exponent $\mathrm{Exp}(\Lambda)$ of the conductor is given by the expression

$$\mathrm{Exp}(\Lambda) = \max(0, v(a/d), v(a/b), v(ad/N_{M/L}(a\tau + b)). \tag{3.4.5}$$

By (3.2.4), the (unordered) invariants of Λ are

$$\mathrm{inv}(\Lambda) = \begin{cases} v(b), v(ad/b), & \text{if } |a| < |b| > |d| \\ v(a), v(d), & \text{otherwise.} \end{cases} \tag{3.4.6}$$

Any element λ of Λ is of the form

$$\lambda = \mu(a\tau + b) + \nu d$$

where $\mu, \nu \in R$. We then have, where $\mathrm{Tr}_{M/L}$ denotes the trace from M to L,

$$N_{M/L}(\lambda) = \mu^2 N_{M/L}(a\tau + b) + \mu\nu d\mathrm{Tr}_{M/L}(a\tau + b) + \nu^2 d^2.$$

As $\mathrm{Tr}_{M/L}(\tau) \in R$ we obtain that

$$v(d\mathrm{Tr}_{M/L}(a\tau + b)) \geq \min(v(ad), v(bd)).$$

We then obtain, as both d^2 and $N_{M/L}(a\tau + b)$ are elements of $N_{M/L}(\Lambda)$,

$$\min(v(N_{M/L}(a\tau + b)), v(d^2)) \geq v(N_{M/L}(\Lambda))$$

$$\geq \min(v(N_{M/L}(a\tau + b)), v(ad), v(bd), v(d^2)).$$

Hence we have

$$\min(v(N_{M/L}(\Lambda)), v(ad), v(bd)) = \min(v(N_{M/L}(a\tau + b)), v(ad), v(bd), v(d^2)).$$

From (3.4.5) and as $[S : \Lambda] = adR$, we obtain,

$$\max(0, v(a/b), v([S : \Lambda]) - v(N_{M/L}(\Lambda))) =$$

$$\max(0, v(a/d), v(a/b), v(ad/N_{M/L}(a\tau + b))) = \mathrm{Exp}(\Lambda). \tag{3.4.7}$$

We then have that the exponent $\mathrm{Exp}(\Lambda)$ is given by

$$\mathrm{Exp}(\Lambda) = \max(0, v(a/d), v(a/b), v([S : \Lambda]) - v(N_{M/L}(\Lambda))). \tag{3.4.8}$$

By (3.4.6) we easily obtain, as $\Lambda \cap L = dR$,

$$\max(\mathrm{inv}(\Lambda) - v(\Lambda \cap L)) = \max(0, v(a/d), v(a/b)). \tag{3.4.9}$$

For in the case where $|a| < |b| > |d|$ we have that $\max(\mathrm{inv}(\Lambda) - v(\Lambda \cap L))$ takes the value $v(a/b)$ and otherwise it takes the value $\max(v(a/d), 0)$. We then obtain from (3.4.8) and (3.4.9) that the exponent $\mathrm{Exp}(\Lambda)$ is given by

$$\mathrm{Exp}(\Lambda) = \max(\mathrm{inv}(\Lambda) - v(\Lambda \cap L), v([S : \Lambda]) - v(N_{M/L}(\Lambda))$$

which is the formula of the proposition. □

3.5 Explicit formulae for the conductor $\mathrm{Exp}(\Lambda)$

Let R, v, π, L, M, S be as in the preceding sections §§3.2,3.3.

The next proposition is an explicit formula for the valuation of the norm $N_{M/L}(\Lambda)$ of an R-lattice Λ of M when R is an excellent henselian discrete valuation ring. As a corollary, we obtain explicit formulae for the exponent $\mathrm{Exp}(\Lambda)$.

3.5.1. Proposition. *Assume that M is a reduced 2-dimensional L-algebra and R is an excellent henselian discrete valuation ring. There is a basis $1, \tau$ of S over R such that for any R-lattice Λ of M with R-basis $a\tau + b, d$, where $a, b, d \in L$, we have:*
(i) $v(N_{M/L}(\Lambda)) = 2\min(v(a), v(b), v(d))$ *if v is inert and unramified in M/L;*
(ii) $v(N_{M/L}(\Lambda)) = \min(2v(a) + 1, 2v(b), 2v(d))$ *if v is ramified in M/L;*
(iii) $v(N_{M/L}(\Lambda)) = \min(v(a+b), v(d)) + \min(v(b), v(d))$ *if v splits completely in M/L.*

From proposition 3.3.3 and the formulae (3.2.4) (or more directly from the formula (3.4.8)), we obtain the next corollary.

3.5.2. Corollary. *Under the hypotheses of proposition 3.5.1, we have*
$\mathrm{Exp}(\Lambda) = \max\big(0, v(a/d), v(a/b), v(d/a), v(ad/b^2)\big)$ *if v is inert and unramified in M/L;*
$\mathrm{Exp}(\Lambda) = \max\big(0, v(a/d), v(a/b), v(d/a) - 1, v(ad/b^2)\big)$ *if v is ramified in M/L;*
$\mathrm{Exp}(\Lambda) = \max\big(0, v(a/d), v(a/b), v(ad/b(a+b))\big)$ *if v splits completely in M/L.*
□

Proof of proposition 3.5.1. An element λ of Λ is of the form

$$\lambda = \alpha(a\tau + b) + \beta d, \text{ where } \alpha, \beta \in R.$$

The norm of λ takes the form

$$N_{M/L}(\lambda) = \alpha^2 a^2 N_{M/L}(\tau) + \alpha a(\alpha b + \beta d)\mathrm{Tr}_{M/L}(\tau) + (\alpha b + \beta d)^2 \tag{3.5.3}$$

where $\mathrm{Tr}_{M/L}$ denotes the trace from M to L. We obtain that

$$v(N_{M/L}(\lambda)) \geq \tag{3.5.4}$$

$$\min(2v(\alpha a) + v(N_{M/L}(\tau)), v(\alpha a(\alpha a + \beta d)) + v(\mathrm{Tr}_{M/L}(\tau)), 2v(\alpha b + \beta d)).$$

We have the evident inequality

$$v(\alpha a(\alpha b + \beta d)) \geq 2\min(v(\alpha a), v(\alpha b + \beta d));$$

hence we obtain from (3.5.4) as $v(\mathrm{Tr}_{M/L}(\tau)) \geq 0$

$$v(N_{M/L}(\lambda)) \geq \min(2v(\alpha a) + v(N_{M/L}(\tau)), 2v(\alpha a) + v(\mathrm{Tr}_{M/L}(\tau)), 2v(\alpha b + \beta d)).$$

As $v(\alpha) \geq 0$ and $v(\beta) \geq 0$, we obtain

$$v(N_{M/L}(\Lambda)) \geq \min(2v(a) + v(N_{M/L}(\tau)), 2v(a) + v(\mathrm{Tr}_{M/L}(\tau)), 2v(b), 2v(d)). \tag{3.5.5}$$

(i) Assume v is inert and unramified in M/L. Take $\tau \in S$ such that the images of $1, \tau$ form a basis of the residue field of the discrete valuation ring S over the residue field of R. We then have

$$v(N_{M/L}(\tau)) = 0,\ v(\mathrm{Tr}_{M/L}(\tau)) \geq 0. \tag{3.5.6}$$

By (3.5.5) we obtain

$$v(N_{M/L}(\Lambda)) \geq 2\min(v(a), v(b), v(d)). \tag{3.5.7}$$

On the other hand, we have $d \in \Lambda$ and

$$v(N_{M/L}(d)) = 2v(d); \tag{3.5.8}$$

furthermore we have $a\tau + b \in \Lambda$ and from (3.5.4) and (3.5.6) we obtain

$$v(N_{M/L}(a\tau + b)) \geq \min(2v(a), 2v(b)). \tag{3.5.9}$$

If $v(a) \neq v(b)$ then $a\tau$ and b have different valuations and in this case we have

$$v(N_{M/L}(a\tau + b)) = \min(2v(a), 2v(b)). \tag{3.5.10}$$

Suppose that $v(a) = v(b)$; if $v(N_{M/L}(a\tau + b)) > 2v(a)$ then the image of $\tau + (b/a)$ in the residue field of S would be zero; but this contradicts that $1, \tau$ form a basis of the residue field of S over the residue field of R. Hence we have in this case $v(N_{M/L}(a\tau + b)) = 2v(a)$ and equality again holds in (3.5.9). We have therefore shown that equality holds in (3.5.7); that is to say, we have

$$v(N_{M/L}(\Lambda)) = 2\min(v(a), v(b), v(d)).$$

(ii) As v is ramified in M/L, we have that M is a field, S is a discrete valuation ring, and S/R totally ramified with ramification index 2. We may take $\tau \in S$ to be a local parameter for the discrete valuation ring S and then $1, \tau$ is a basis of S as an R-module by Nakayama's lemma. Denote by v^* the extension of the valuation v to M such that v and v^* coincide on L; we then have $v^*(\tau) = 1/2$. We have

$$v(N_{M/L}(\tau)) = v(\pi) = 1$$
$$v(\mathrm{Tr}_{M/L}(\tau)) \geq v(\pi) = 1.$$

From (3.5.5) we obtain

$$v(N_{M/L}(\Lambda)) \geq \min(2v(a) + 1, 2v(b), 2v(d)). \tag{3.5.11}$$

We have $d \in \Lambda$ and hence we obtain

$$v(N_{M/L}(\Lambda)) \leq v(N_{M/L}(d)) = 2v(d).$$

Furthermore, $a\tau$ and b have distinct valuations, as $v^*(\tau)$ does not lie in the value group of v on L. Hence we have

$$v(N_{M/L}(\Lambda)) \leq v(N_{M/L}(a\tau+b)) = 2\min(v^*(a\tau), v(b)) = \min(2v(a)+1, 2v(b)).$$

We obtain finally that equality holds in (3.5.11) that is to say we have

$$v(N_{M/L}(\Lambda)) = \min(2v(a) + 1, 2v(b), 2v(d)).$$

(iii) Suppose that the valuation v is split completely in M/L, that is to say the valuation v has two inequivalent extensions to M. By proposition 3.3.1, we have that M is either isomorphic to $L \times L$ or is a quadratic field extension of L which must be separable as v splits. Hence S is a semi-local ring which is a free R-module of rank 2.

Let κ be the residue field of R. Then $S \otimes_R \kappa$ is a 2-dimensional commutative algebra over κ; hence $S \otimes_R \kappa$ is one of the 3 possibilities given by proposition 3.3.1. If $S \otimes_R \kappa$ were a field then S would be a discrete valuation ring and hence v would not split in M which is a contradiction. If $S \otimes_R \kappa$ were not reduced then again S would be a discrete valuation ring and hence v would not split in M which is a contradiction. Hence the only possibility is that $S \otimes_R \kappa$ is equal to $\kappa \times \kappa$; in particular $S \otimes_R \kappa$ is an étale κ-algebra. Hence for all prime ideals $\mathfrak{p}$ of R, the $\kappa(\mathfrak{p})$-algebra $S \otimes_R \kappa(\mathfrak{p})$ is étale; hence as S is R-flat, we have that S is an étale R-algebra. As R is henselian, S is a direct product of local R-algebras; as S is a free R-module of rank 2 we obtain an isomorphism of R-algebras

$$f : S \cong R \times R.$$

Hence M is L-isomorphic to the algebra $L \times L$.

We may select $\tau \in S$ such that $f(\tau) = (1, 0)$. Then $1, \tau$ is a basis of S over R. Furthermore, the non-trivial element of $\mathrm{Gal}(M/L)$ is induced by the exchange of the two factors in $R \times R$. Hence we have for $\lambda \in \Lambda$, where $\lambda = \alpha(a\tau + b) + \beta d$ and $\alpha, \beta \in R$,

$$\lambda = (\alpha(a + b) + \beta d, \alpha b + \beta d).$$

Hence we have

$$N_{M/L}(\lambda) = (\alpha(a + b) + \beta d)(\alpha b + \beta d)$$

and we obtain

$$v(N_{M/L}(\lambda)) = v(\alpha(a + b) + \beta d) + v(\alpha b + \beta d)$$

$$\geq \min(v(a + b), v(d)) + \min(v(b), v(d)).$$

As this latter term is independent of λ, we have

$$v(N_{M/L}(\Lambda)) \geq \min(v(a + b), v(d)) + \min(v(b), v(d)). \tag{3.5.12}$$

If $A, B \in L$ then it is immediately checked that for a suitable choice of α, β equal to 0 or 1 in L we have the simultaneous equalities

$$v(\alpha A + \beta) = \min(v(A), 0)$$

and

$$v(\alpha B + \beta) = \min(v(B), 0).$$

Putting $A = (a+b)/d$ and $B = b/d$ we obtain that for some choice of $\alpha, \beta = 0, 1$ we have, where $\lambda = \alpha(a\tau + b) + \beta d$,

$$v(N_{M/L}(\lambda)) = \min(v(a+b), v(d)) + \min(v(b), v(d)).$$

Hence we have equality in (3.5.12), as required. □

3.6 Bruhat-Tits trees with complex multiplication

(3.6.1) Let R, v, π, L be as in §3.2. Let

$\Delta(\mathrm{SL}_2(L))$ be the Bruhat-Tits building of $\mathrm{SL}_2(L)$ with respect to the discrete valuation v (see §3.1);
$\mathcal{L}$ denote the set of vertices of the Bruhat-Tits tree $\Delta(\mathrm{SL}_2(L))$.

(3.6.2) Let M be a 2-dimensional commutative L-algebra. Fix an R-lattice Λ_0 of M; if M is reduced we take Λ_0 to be the integral closure of R in M (proposition 3.3.2).

A *Bruhat-Tits building with complex multiplication by* M is a triple

$$(\Delta(\mathrm{SL}_2(L)), \mathrm{Exp}_{M,\Lambda_0}, M)$$

where $\mathrm{Exp}_{M,\Lambda_0}$ is the map

$$\mathrm{Exp}_{M,\Lambda_0} : \mathcal{L} \to \mathbb{Z}.$$

defined as follows. Let $x \in \mathcal{L}$. Select an R-lattice Λ of M whose equivalance class $[\Lambda]$ is equal to x. Then the ring of endomorphisms $\mathrm{End}_R^M(\Lambda)$ is the subring of M preserving Λ (see §3.3)

$$\mathrm{End}_R^M(\Lambda) = \{m \in M \mid m\Lambda \subset \Lambda\}.$$

The integer $\mathrm{Exp}_{M,\Lambda_0}(x)$ is defined to be the exponent of the conductor of the R-lattice $\mathrm{End}_R^M(\Lambda)$ relative to the lattice Λ_0 (see Definition 3.3.3 and proposition 3.3.1(iii)).

The abelian group M^* acts, as a subgroup of $\mathrm{GL}_2(L)$, on the vertices of $\Delta(\mathrm{SL}_2(L))$ and preserves the function $\mathrm{Exp}_{M,\Lambda_0}$; hence M^* is a group of automorphisms of the triple $(\Delta(\mathrm{SL}_2(L)), \mathrm{Exp}_{M,\Lambda_0}, M)$.

(3.6.3) The pair

$$(\Delta(\mathrm{SL}_2(L)), f)$$

where f is a map of sets

$$f : \mathcal{L} \to \mathbb{Z}$$

is a *Bruhat-Tits tree with complex multiplication* if for some 2-dimensional commutative L-algebra M the triple $(\Delta(\mathrm{SL}_2(L)), f, M)$ is a Bruhat-Tits building with complex multiplication by M, that is to say $f = \mathrm{Exp}_{M,\Lambda_0}$ for a suitable R-lattice Λ_0 as in (3.6.1).

3.7 The standard metric and Bruhat-Tits trees with complex multiplication

In this section we give a formula for the exponent function on a Bruhat-Tits tree with complex multiplication in terms of the standard metric on the building (theorems 3.7.3 and 3.7.5).

(3.7.1) Let R, v, π, L be as in §3.2. Let

d be the standard metric on the Euclidean Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$, with respect to v, normalised so the distance between adjacent vertices is 1 (see §3.1 or [Bro2, Ch. VI,§3]).
M be a 2-dimensional commutative L-algebra;
S be the integral closure of R in M;
$(\Delta(\mathrm{SL}_2(L)), \mathrm{Exp}_{M,\Lambda_0}, M)$ be a Bruhat-Tits tree with complex multiplication by M where $\Lambda_0 = S$ if M is reduced (see (3.6.2)).

3.7.2. Definition. Let N be an R-subalgebra of M. Then an ideal of the ring N which is also an R-lattice of M is called a *lattice ideal of* N.

[If M is a field and $N = S$, the integral closure of R in M, then every non-zero ideal of N is a lattice ideal, as S is a discrete valuation ring (proposition 3.3.2). But if M is not a field then S always has non-zero ideals which are not lattice ideals (by proposition 3.3.2).]

3.7.3. Theorem. *If M is a reduced algebra then for any R-lattice Λ of M we have*

$$\mathrm{Exp}(\Lambda) = d([\Lambda], [I])$$

where I is the unique lattice ideal of S, up to multiplication by an element of L^*, for which the distance $d([\Lambda], [I])$ is minimum.

(3.7.4) Suppose that M is not reduced. Then M is L-isomorphic to $L[\epsilon]/(\epsilon^2)$ (see proposition 3.3.1). We fix the lattice Λ_0 to be the R-subalgebra $R \oplus \epsilon R$ of the integral closure $S = R \oplus \epsilon L$ of R; Λ_0 then depends only on the choice of ϵ. We take exponents of conductors with respect to Λ_0.

The lattice ideals of Λ_0 are not necessarily of exponent 0; for example the lattice ideal of Λ_0

$$I = \pi^n R \oplus \epsilon R, \quad \text{where } n \geq 1,$$

has ring of endomorphisms $\mathrm{End}_R^M(I) = R \oplus \pi^{-n}\epsilon R$ and has exponent $\mathrm{Exp}_{M,\Lambda_0}(I) = -n$.

3.7.5. Theorem. *Suppose that M is not reduced. For any R-lattice Λ of M we have*

$$|\mathrm{Exp}(\Lambda)| = \min_I d([\Lambda], [I]).$$

where the minimum runs over all lattice ideals I of Λ_0 such that $\mathrm{Exp}(I) = 0$.

One possible proof of these results is obtained by passing to the henselisation of R and directly checking the many diverse cases using the explicit formulae of corollary 3.5.2. In this section, we prove these theorems 3.7.3 and 3.7.5 by a different method.

Let $\kappa = R/(\pi)$ be the residue field of the discrete valuation ring R. Recall that $\mathrm{End}_R^M(\Lambda)$ denotes the subring of M formed of endomorphisms of the lattice Λ whereas $\mathrm{End}_\kappa(\Lambda \otimes_R \kappa)$ denotes the ring of κ-vector space endomorphisms of $\Lambda \otimes_R \kappa$. The reduction homomorphism of R-modules $\Lambda \to \Lambda \otimes_R \kappa$ induces a homomorphism of R-algebras

$$f_\Lambda : \mathrm{End}_R^M(\Lambda) \to \mathrm{End}_\kappa(\Lambda \otimes_R \kappa).$$

.

3.7.6. Lemma. *We have an isomorphism of R-algebras*

$$f_\Lambda(\mathrm{End}_R^M(\Lambda)) \cong \mathrm{End}_R^M(\Lambda) \otimes_R \kappa.$$

Proof of lemma 3.7.6. On the one hand, it is clear that $\pi\mathrm{End}_R^M(\Lambda)$ lies in the kernel of f_Λ. On the other hand if $u \in \ker(f_\Lambda)$ then we have

$$u(\Lambda) \subset \pi\Lambda.$$

Hence $\pi^{-1}u$ is an element of the L-algebra M; therefore multiplication by $\pi^{-1}u$ defines an R-linear map of M such that

$$(\pi^{-1}u)(\Lambda) \subset \Lambda.$$

Hence we have $\pi^{-1}u \in \mathrm{End}_R^M(\Lambda)$ and therefore we obtain $u \in \pi\mathrm{End}_R^M(\Lambda)$. This gives the isomorphism of R-algebras

$$f_\Lambda(\mathrm{End}_R^M(\Lambda)) \cong \mathrm{End}_R^M(\Lambda)/\pi\mathrm{End}_R^M(\Lambda)$$

as required. □

3.7.7. Lemma. *Assume either that M is reduced and $\mathrm{Exp}(\Lambda) \geq 1$ or that M is not reduced. Let κ be the residue field of R. We have an isomorphism of R-algebras*

$$\mathrm{End}_R^M(\Lambda) \otimes_R \frac{R}{(\pi^2)} \cong \frac{R}{(\pi^2)}\frac{[\epsilon]}{(\epsilon^2 - \pi\mu\epsilon)}$$

where

$$\mu = \begin{cases} 1, & \text{if } \kappa \text{ has characteristic } 2,\ S/R \text{ is étale, and } \mathrm{Exp}(\Lambda) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Proof of lemma 3.7.7. Suppose that M is reduced. The algebra S is a free R-module of rank 2 hence we may select an R-basis of S of the form $1, s$ where $s \in S \setminus R$.

Suppose that M is not reduced. Then we may choose $s \in M$ such that $s^2 = 0$ and we have equalities of R-algebras $M = L[s]$ and $S = R \oplus \epsilon L$ (see proposition 3.3.1). We may fix the R-lattice $\Lambda_0 = R \oplus sR$.

In both cases where M is or is not reduced, we obtain an equality of R-algebras

$$\mathrm{End}_R^M(\Lambda) = R \oplus s\pi^n R.$$

where

$$n = \mathrm{Exp}(\Lambda).$$

The exponent $\mathrm{Exp}(\Lambda)$ here is relative to Λ_0 if M is not reduced and is relative to S if M is reduced.

Suppose first either that $n \geq 2$ or that M is not reduced. We have

$$(s\pi^n)^2 = \begin{cases} \pi^2(\pi^n s)(\pi^{n-2}s) \in \pi^2\mathrm{End}_R^M(\Lambda), & \text{if } n \geq 2 \\ 0, & \text{if } M \text{ is not reduced.} \end{cases}$$

Hence putting $\epsilon = s\pi^n$ (modulo π^2) we have $\epsilon^2 = 0$ (modulo π^2). We obtain the isomorphism of R-algebras

$$\mathrm{End}_R^M(\Lambda) \otimes_R \frac{R}{(\pi^2)} \cong \frac{R}{(\pi^2)}\frac{[\epsilon]}{(\epsilon^2)}. \tag{3.7.8}$$

This proves the lemma in these cases, as S/R is étale only if M is reduced.

Suppose now that $n = 1$ and M is reduced. As s is integral over R, we have that s satisfies an equation of the form

$$s^2 = as + b, \quad \text{where } a, b \in R.$$

We obtain

$$(\pi s)^2 = a\pi^2 s + \pi^2 b.$$

As $\pi^2 b \in \pi^2 R$ we obtain the isomorphism of R-algebras, putting $\zeta = \pi s$,

$$\text{End}_R^M(\Lambda) \otimes_R \frac{R}{(\pi^2)} \cong \frac{R}{(\pi^2)}\frac{[\zeta]}{(\zeta^2 - a\pi\zeta)} \tag{3.7.9}$$

Case 1. Assume the characteristic of κ is not equal to 2. Then the change of variable

$$\epsilon = \zeta - \frac{a\pi}{2}$$

shows that $\epsilon^2 \in \pi^2 R$ and the isomorphism (3.7.9) reduces to the isomorphism (3.7.8).

Case 2. Assume that the characteristic of κ is equal to 2 and that S is not étale over R. Then a is divisible by π. Again the isomorphism (3.7.9) reduces to the isomorphism (3.7.8).

Case 3. Assume that κ has characteristic 2 and S is étale over R; we have that a is not divisible by π and hence that $a \in R^*$. The change of variable $\epsilon = a^{-1}\zeta$ then reduces the isomorphism (3.7.9) to the form

$$\text{End}_R^M(\Lambda) \otimes_R \frac{R}{(\pi^2)} \cong \frac{R}{(\pi^2)}\frac{[\epsilon]}{(\epsilon^2 - \pi\epsilon)}.$$

This algebra contains a nilpotent element ϵ of order 4 and hence it is not R-isomorphic to $R[\epsilon]/(\pi^2, \epsilon^2)$. This proves the lemma.□

3.7.10. Definition. The *star* $\text{st}(x)$ of a vertex x of the Bruhat-Tits tree $\Delta(\text{SL}_2(L))$ is the set of adjacent vertices to x, distinct from x, in $\Delta(\text{SL}_2(L))$. That is to say, the star $\text{st}(x)$ is the set of vertices of $\Delta(\text{SL}_2(L))$ whose distance from x is exactly 1, with respect to the normalised standard metric.

Let Λ be an R-lattice of M corresponding to the vertex x of $\Delta(\text{SL}_2(L))$. Then $\Lambda \otimes_R \kappa$ is a 2-dimensional vector space over κ. Let $\mathbb{P}_1(\Lambda \otimes_R \kappa)$ be the set of κ-rational points of the projective line over κ; that is to say $\mathbb{P}_1(\Lambda \otimes_R \kappa)$ may be identified with the set of 1-dimensional κ-subspaces of $\Lambda \otimes_R \kappa$.

3.7.11. Definition. The *star map* is a bijection of sets

$$\psi_x : \mathrm{st}(x) \to \mathbb{P}_1(\Lambda \otimes_R \kappa)$$

defined as follows. Let $x' \in \mathrm{st}(x)$ be an adjacent vertex to x in $\Delta(\mathrm{SL}_2(L))$. Select a representative R-lattice Λ' of the class x' such that

$$\pi\Lambda \subset \Lambda' \subset \Lambda.$$

The correspondence

$$x' = [\Lambda'] \mapsto \Lambda'/\pi\Lambda \subset \Lambda \otimes_R \kappa$$

defines the bijection ψ_x.

3.7.12. Lemma. *Let Λ and Λ' be R-lattices of M such that $[\Lambda]$ and $[\Lambda']$ are adjacent distinct vertices of the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$.*
(i) *We have*

$$|\mathrm{Exp}(\Lambda) - \mathrm{Exp}(\Lambda')| \leq 1. \tag{3.7.13}$$

(ii) *We have*

$$\mathrm{Exp}(\Lambda') \leq \mathrm{Exp}(\Lambda)$$

if and only if the endomorphisms in $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ have a common 1-dimensional eigenspace U on $\Lambda \otimes_R \kappa$ and $\psi_{[\Lambda]}([\Lambda']) = U$.
(iii) *Assume either that $\mathrm{Exp}(\Lambda) \geq 1$ and M is reduced or that M is not reduced. Then we have*

$$|\mathrm{Exp}(\Lambda) - \mathrm{Exp}(\Lambda')| = 1.$$

Proof of lemma 3.7.12. We may assume that Λ and Λ' verify $\pi\Lambda \subset \Lambda' \subset \Lambda$.
(i) For any $u \in \mathrm{End}_R^M(\Lambda)$ we have

$$(\pi u)(\Lambda') \subseteq \pi\Lambda \subset \Lambda'.$$

This shows that $\pi u \in \mathrm{End}_R^M(\Lambda')$ and hence that we have

$$\pi\mathrm{End}_R^M(\Lambda) \subseteq \mathrm{End}_R^M(\Lambda').$$

We obtain the inequality for the exponents of the conductors

$$\mathrm{Exp}(\Lambda') \leq \mathrm{Exp}(\Lambda) + 1.$$

By the symmetry between Λ and Λ' we then obtain the inequality (3.7.13).
(ii) Suppose now that

$$\mathrm{Exp}(\Lambda') \leq \mathrm{Exp}(\Lambda).$$

Then $\mathrm{End}_R^M(\Lambda)$ is a subring of $\mathrm{End}_R^M(\Lambda')$. But $\psi_{[\Lambda]}(\Lambda')$ corresponds to a 1-dimensional subspace of $\Lambda \otimes_R \kappa$ namely $\Lambda'/\pi\Lambda$, and hence this subspace is preserved by the elements of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$; as it is 1-dimensional, this subspace $\Lambda'/\pi\Lambda$ is therefore a common eigenspace of all elements of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$.

Conversely, suppose that the endomorphisms in $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ have a common 1-dimensional eigenspace $U \subset \Lambda \otimes_R \kappa$. Then U corresponds to a unique R-lattice Λ' such that $\pi\Lambda \subset \Lambda' \subset \Lambda$. As U is preserved by the elements of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$, for every element $u \in \mathrm{End}_R^M(\Lambda)$ we have

$$u(\Lambda') \subseteq \Lambda'.$$

That is to say the elements of $\mathrm{End}_R^M(\Lambda)$ preserve Λ'. Hence the endomorphism ring $\mathrm{End}_R^M(\Lambda)$ is a subring of $\mathrm{End}_R^M(\Lambda')$; we have in consequence the inequality of exponents

$$\mathrm{Exp}(\Lambda') \leq \mathrm{Exp}(\Lambda).$$

(iii) Assume either that $\mathrm{Exp}(\Lambda) \geq 1$ and M is reduced or that M is not reduced. By lemma 3.7.7 we have that the R-algebra $\mathrm{End}_R^M(\Lambda)$ takes the form

$$\mathrm{End}_R^M(\Lambda) = R \oplus R\eta \tag{3.7.14}$$

where η satisfies a relation of the form

$$\eta^2 \equiv \mu\pi\eta \text{ (modulo } \pi^2) \text{ where } \mu = 0 \text{ or } 1.$$

According to lemma 3.7.7 we may take μ to be zero unless κ has characteristic 2, $\mathrm{Exp}(\Lambda) = 1$, and S/R is étale in which case we take μ to be 1.

Assume that

$$\mathrm{Exp}(\Lambda) = \mathrm{Exp}(\Lambda'). \tag{3.7.15}$$

We then have that the R-algebra $\mathrm{End}_R^M(\Lambda)$ is isomorphic to $\mathrm{End}_R^M(\Lambda')$. As the endomorphism $\eta \otimes_R \kappa$ is non-zero and nilpotent on $\Lambda \otimes_R \kappa$, it has a unique 1-dimensional eigenspace namely its kernel. Therefore by part (ii) above, the 1-dimensional κ-vector space $\Lambda'/\pi\Lambda$ lies in the kernel of the endomorphism $\eta \otimes_R \kappa$ on $\Lambda \otimes_R \kappa$. Hence we have $\eta\Lambda' \subset \pi\Lambda$; as π is not a zero divisor of M we have $\pi^{-1}\eta \in M$ and also

$$(\pi^{-1}\eta)\Lambda' \subset \Lambda.$$

Hence we have, as $\eta^2 \equiv \mu\pi\eta$ (modulo π^2),

$$\eta^2\Lambda' \subset \pi\eta\Lambda' + \pi^2\Lambda'$$

and therefore, as $\eta\Lambda' \subset \pi\Lambda$,

$$\eta((\pi^{-1}\eta)\Lambda') = \pi^{-1}(\eta^2\Lambda') \subset \pi^{-1}(\pi\eta\Lambda' + \pi^2\Lambda') = \eta\Lambda' + \pi\Lambda' \subset \pi\Lambda.$$

This shows that $(\pi^{-1}\eta)\Lambda' \bmod \pi\Lambda$ lies in the kernel $\Lambda'/\pi\Lambda$ of $\eta\otimes\kappa$ on $\Lambda\otimes_R\kappa$. That is to say we have

$$(\pi^{-1}\eta)\Lambda' \subset \Lambda'.$$

Hence the lattice Λ' is stable under the endomorphism $\pi^{-1}\eta$, an endomorphism which does not lie in $\mathrm{End}_R^M(\Lambda)$ by (3.7.14). But this contradicts the hypothesis (3.7.15), which asserts that the endomorphism rings of Λ and Λ' are equal; hence this assumption (3.7.15) is false.

By part (i), we have that $\mathrm{Exp}(\Lambda)$ and $\mathrm{Exp}(\Lambda')$ differ by at most 1. As we have shown that $\mathrm{Exp}(\Lambda) \neq \mathrm{Exp}(\Lambda')$, the only remaining possibility is $|\mathrm{Exp}(\Lambda) - \mathrm{Exp}(\Lambda')| = 1$, as required.□

3.7.16. Lemma. (i) *Suppose either that M is reduced and* $\mathrm{Exp}(\Lambda) \geq 1$ *or that M is not reduced. Then all vertices but one of the star* $\mathrm{st}([\Lambda])$ *have exponent* $\mathrm{Exp}(\Lambda)+1$*; the exceptional vertex in* $\mathrm{st}([\Lambda])$ *has exponent* $\mathrm{Exp}(\Lambda)-1$.
(ii) *Suppose that* $\mathrm{Exp}(\Lambda) \geq 0$. *There is a unique chain $\mathcal{C}$ of distinct vertices in* $\Delta(\mathrm{SL}_2(L))$

$$\mathcal{C}: \ [\Lambda_1],\ [\Lambda_2],\ \ldots,\ [\Lambda_n] \tag{3.7.17}$$

where $\Lambda = \Lambda_1, \Lambda_2, \ldots, \Lambda_n$ are R-lattices of M, such that $[\Lambda_i], [\Lambda_{i+1}]$ are adjacent, for all i, $\mathrm{Exp}(\Lambda_{i+1}) = \mathrm{Exp}(\Lambda_i) - 1$, *for all i, and* $\mathrm{Exp}(\Lambda_n) = 0$.

Proof. (i) By lemmas 3.7.6 and 3.7.7, we have isomorphisms of κ-algebras

$$f_\Lambda(\mathrm{End}_R^M(\Lambda)) \cong \mathrm{End}_R^M(\Lambda) \otimes_R \frac{R}{(\pi)} \cong \kappa[\epsilon]/(\epsilon^2).$$

Hence the elements of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ have a unique 1-dimensional common eigenspace on $\Lambda\otimes_R\kappa$ namely the kernel of ϵ. By lemma 3.7.12(ii), there is a unique lattice Λ' such that $\pi\Lambda \subset \Lambda' \subset \Lambda$ for which

$$\mathrm{Exp}(\Lambda') \leq \mathrm{Exp}(\Lambda).$$

By lemma 3.7.12(iii) this lattice has exponent equal to $\mathrm{Exp}(\Lambda) - 1$. For all other lattices $\Lambda'' \neq \Lambda'$ verifying $\pi\Lambda \subset \Lambda'' \subset \Lambda$ we then obtain from lemma 3.7.12(ii) and (iii)

$$\mathrm{Exp}(\Lambda'') = \mathrm{Exp}(\Lambda) + 1.$$

As the lattices Λ'' verifying $\pi\Lambda \subset \Lambda'' \subset \Lambda$ correspond to the elements of $\mathrm{st}([\Lambda])$ this proves the statement above.
(ii) We construct the chain $\mathcal{C}$ by induction. We put $\Lambda = \Lambda_1$. Suppose the sequence (3.7.17) has been constructed up to $[\Lambda_i]$ where $i \geq 1$. If $\mathrm{Exp}(\Lambda_i) > 0$, by part (i) we may find a unique vertex x of $\mathrm{st}([\Lambda_i])$ for which any R-lattice Λ_{i+1} of M in the class x satisfies

$$\mathrm{Exp}(\Lambda_{i+1}) = \mathrm{Exp}(\Lambda_i) - 1.$$

This constructs the sequence (3.7.17) up to $[\Lambda_{i+1}]$. If, on the other hand, $\mathrm{Exp}(\Lambda_i) = 0$ then the sequence (3.7.17) stops with $[\Lambda_i]$.

Clearly, this sequence $\mathcal{C}$ of (3.7.17) of vertices is finite, is uniquely determined by the initial vertex $[\Lambda]$, and terminates with a vertex $[\Lambda_n]$ where $\mathrm{Exp}(\Lambda_n) = 0$ and Λ_n is a lattice ideal of Λ_0, as required. □

We now come to the proofs of the main results of this section, theorems 3.7.3 and 3.7.5.

Proof of theorem 3.7.3. We now assume that the algebra M is reduced. Let Λ be an R-lattice in M. The proof is in several steps.

Step 1. Let $\mathcal{C}: [\Lambda_1], [\Lambda_2], \ldots, [\Lambda_n]$ *be the chain associated to* $\Lambda = \Lambda_1$*, as in lemma 3.7.16. Then we have* $\mathrm{Exp}(\Lambda) = d([\Lambda], [\Lambda_n]) = n - 1$.

As $\mathrm{Exp}(\Lambda_{i+1}) = \mathrm{Exp}(\Lambda_i) - 1$, for all $i = 1, \ldots, n-1$, we obtain

$$\mathrm{Exp}(\Lambda) = \mathrm{Exp}(\Lambda_n) + n - 1 = n - 1. \tag{3.7.18}$$

As the chain $\mathcal{C}$ consists of distinct adjacent vertices, without repetition, of $\Delta(\mathrm{SL}_2(L))$ we have that $\mathcal{C}$ forms the set of vertices of a shortest path joining $[\Lambda]$ and $[\Lambda_n]$ in the Bruhat-Tits tree $\Delta(\mathrm{SL}_2(L))$; that is, we have demonstrated the equality

$$\mathrm{Exp}(\Lambda) = d([\Lambda], [\Lambda_n]).$$

Step 2. Suppose that I *is a lattice ideal of* S*. Then we have* $d([\Lambda], [\Lambda_n]) \leq d([\Lambda], [I])$ *with equality if and only if* $[I] = [\Lambda_n]$.

The distance $d([\Lambda], [I])$ is measured by constructing a sequence $\mathcal{V}$ of distinct vertices

$$\mathcal{V}: \ u_1 = [\Lambda], u_2, \ldots, u_m = [I] \tag{3.7.19}$$

of the tree $\Delta(\mathrm{SL}_2(L))$ such that $u_{i+1} \in \mathrm{st}(u_i)$ for all i; we then have

$$d([\Lambda], [I]) = m - 1.$$

In this sequence $\mathcal{V}$, we have, by lemma 3.7.12(i) and Step 1,

$$\mathrm{Exp}(u_1) = n - 1, \ \mathrm{Exp}(u_m) = 0, \ |\mathrm{Exp}(u_i) - \mathrm{Exp}(u_{i+1})| \leq 1 \text{ for all } i.$$

We must then have $m \geq n$ and equality holds if and only if

$$\mathrm{Exp}(u_{i+1}) = \mathrm{Exp}(u_i) - 1 \ \text{ for all } i.$$

But then we have $m = n$ if and only if u_{i+1} is the unique exceptional vertex of $\mathrm{st}(u_i)$ for all i; that is to say $m = n$ if and only if the sequence $\mathcal{V}$ coincides

with the chain $\mathcal{C}$ of lemma 3.7.16. We have therefore shown

$$d([\Lambda],[\Lambda_n]) \leq d([\Lambda],[I])$$

where equality holds if and only if $[I] = [\Lambda]$.

Step 3. We have $\mathrm{Exp}(\Lambda) = \min_I d([\Lambda],[I])$ *where the minimum runs over all lattice ideals* I *of* S *and the minimum is attained by a lattice ideal* I *whose class* $[I]$ *is uniquely determined by* $[\Lambda]$.

This follows from Steps 1 and 2. □

Proof of theorem 3.7.5. The proof here is similar to that of theorem 3.7.3 and is also in several steps. We assume that the algebra M is not reduced. Let Λ be an R-lattice in M.

Step 1. If $\mathrm{Exp}(\Lambda) < 0$ *then there is at least one chain* $\mathcal{C}$ *of distinct vertices in* $\Delta(\mathrm{SL}_2(L))$

$$\mathcal{C}: \ [\Lambda_1],\ [\Lambda_2],\ \ldots,\ [\Lambda_n] \tag{3.7.20}$$

where $\Lambda = \Lambda_1, \Lambda_2, \ldots, \Lambda_n$ *are* R*-lattices of* M*, such that* $[\Lambda_i], [\Lambda_{i+1}]$ *are adjacent, for all* i*,* $\mathrm{Exp}(\Lambda_{i+1}) = \mathrm{Exp}(\Lambda_i) + 1$*, for all* i*, and* $\mathrm{Exp}(\Lambda_n) = 0$.

The argument here is similar to that of the proof of lemma 3.7.16. We put $\Lambda_1 = \Lambda$ where $\mathrm{Exp}(\Lambda) < 0$. Assume the sequence (3.7.20) has been constructed from $[\Lambda_1]$ up to $[\Lambda_i]$. The vertices adjacent to $[\Lambda_i]$ are in bijection with the points of the projective line over the residue field of R; in particular, at least three vertices are adjacent to $[\Lambda_i]$. Hence by lemma 3.7.16 we may find at least one vertex x of $\mathrm{st}([\Lambda_i])$ for which any R-lattice Λ_{i+1} of M in the class x satisfies

$$\mathrm{Exp}(\Lambda_{i+1}) = \mathrm{Exp}(\Lambda_i) + 1.$$

This constructs the sequence (3.7.20) from $[\Lambda_1]$ up to $[\Lambda_{i+1}]$ provided that $\mathrm{Exp}(\Lambda_i) < 0$. If, on the other hand, $\mathrm{Exp}(\Lambda_i) = 0$ then the sequence (3.7.20) terminates with $[\Lambda_i]$ and then the class $[\Lambda_i]$ is that of a lattice ideal of Λ_0 of exponent 0.

Step 2. Let $\mathcal{C}: \ [\Lambda_1],\ [\Lambda_2],\ \ldots,\ [\Lambda_n]$ *be a chain associated to* $\Lambda = \Lambda_1$*, as in lemma 3.7.16 and Step 1. Then we have* $|\mathrm{Exp}(\Lambda)| = d([\Lambda],[\Lambda_n]) = n - 1$.

As $\mathrm{Exp}(\Lambda_{i+1}) = \mathrm{Exp}(\Lambda_i) \pm 1$, for all $i = 1, \ldots, n-1$ and where the signs are here either all positive or all negative, we obtain

$$|\mathrm{Exp}(\Lambda)| = n - 1 \pm \mathrm{Exp}(\Lambda_n) = n - 1.$$

As the chain $\mathcal{C}$ consists of distinct adjacent vertices, without repetition, of $\Delta(\mathrm{SL}_2(L))$ we have that $\mathcal{C}$ forms the set of vertices of a shortest path joining $[\Lambda]$ and $[\Lambda_n]$ in the Bruhat-Tits tree $\Delta(\mathrm{SL}_2(L))$; that is, we have demonstrated

the equality

$$|\mathrm{Exp}(\Lambda)| = d([\Lambda], [\Lambda_n]).$$

Step 3. Suppose that I is a lattice ideal of Λ_0 of exponent 0. Then we have $d([\Lambda], [\Lambda_n]) \leq d([\Lambda], [I])$.

The proof is similar to the proof of step 2 of the proof of theorem 3.7.3. The distance $d([\Lambda], [I])$ is measured by constructing a sequence $\mathcal{V}$ of distinct vertices

$$\mathcal{V}: \ u_1 = [\Lambda], u_2, \ldots, u_m = [I]$$

of the tree $\Delta(\mathrm{SL}_2(L))$ such that $u_{i+1} \in \mathrm{st}(u_i)$ for all i; we then have

$$d([\Lambda], [I]) = m - 1.$$

In this sequence $\mathcal{V}$, we have, by lemma 3.7.12(i) and Step 2,

$$|\mathrm{Exp}(u_1)| = n - 1, \ \mathrm{Exp}(u_m) = 0, \ |\mathrm{Exp}(u_i) - \mathrm{Exp}(u_{i+1})| \leq 1 \text{ for all } i.$$

We must then have $m \geq n$ and equality holds if and only if

$$\mathrm{Exp}(u_{i+1}) = \mathrm{Exp}(u_i) \pm 1 \ \text{ for all } i$$

and where the signs here are either all positive or all negative. We have therefore shown

$$d([\Lambda], [\Lambda_n]) \leq d([\Lambda], [I]).$$

Step 4. We have $|\mathrm{Exp}(\Lambda)| = \min_I d([\Lambda], [I])$ where the minimum runs over all lattice ideals I of Λ_0 of exponent 0.

This follows from Steps 2 and 3. □

3.7.21. Remark. (Maximal orders in the indefinite quaternion algebra $M_2(L)$). For this remark suppose that L is a non-archimedean local field. Let R be the ring of valuation integers of L and let π be a local parameter of R. Let $M_2(L)$ be the non-commutative L-algebra of 2×2 matrices over L. Let V be a 2-dimensional L-vector space on which $M_2(L)$ acts with its usual action. In particular, if V is a 2-dimensional commutative L-algebra, then V may be considered a subalgebra of the 4-dimensional algebra $M_2(L)$.

We have in this chapter considered the *commutative* R-subalgebras of $M_2(L)$ of rank 2 over R.

The *non-commutative* orders of the quaternion algebra $M_2(L)$ have the following properties (see [V] pp.37-41 for proofs and more details).

An order of $\mathrm{End}(V)$ is said to be *maximal* if it is not strictly contained in another order.

(1) The maximal orders of $\mathrm{End}(V)$ are the rings $\mathrm{End}(\Lambda)$ where Λ runs over the R-lattices of rank 2 of V.

(2) If Θ is an (rank 4) R-lattice of $\mathrm{End}(V)$ then there are 2 orders associated to Λ

$$O_l(\Theta) = \{h \in M_2(L) \mid h\Lambda \subseteq \Lambda\}$$
$$O_r(\Theta) = \{h \in M_2(L) \mid \Theta h \subseteq \Theta\}.$$

A lattice Θ is said to be *normal* if the orders $O_l(\Theta)$ and $O_r(\Theta)$ are maximal.

(3) The normal lattices of rank 4 of $\mathrm{End}(V)$ are the lattices $\mathrm{End}(\Lambda, \Lambda')$ where Λ, Λ' are rank 2 R-lattices of V.

(4) The maximal orders of $M_2(L)$ are conjugate to $M_2(R)$.

(5) Let $O = \mathrm{End}(\Lambda)$, $O' = \mathrm{End}(\Lambda')$ be two maximal orders of $\mathrm{End}(V)$ where Λ, Λ' are rank 2 R-lattices of V. We may assume that $\Lambda \subseteq \Lambda'$; then there are bases (f_1, f_2) and $(f_1\pi^a, f_2\pi^b)$ of Λ, Λ', respectively, over R where $a, b \in \mathbb{N}$. The integer $|a - b|$ depends only on the orders O, O'. The *distance* between the orders O, O' is defined to be $d(O, O') = |a - b|$.

For example, we have

$$d(M_2(R), \begin{pmatrix} R & \pi^{-n}R \\ \pi^n R & R \end{pmatrix}) = n.$$

(6) An *Eichler order of level* π^n is defined to be the intersection of 2 maximal orders of $\mathrm{End}(V)$ of distance n.

(7) Let O be an order of $M_2(L)$. Then the following properties are equivalent:
(a) there is a unique pair of maximal orders O_1, O_2 such that $O = O_1 \cap O_2$;
(b) O is a Eichler order;
(c) there is an integer $n \in \mathbb{N}$ such that O is conjugate to $\begin{pmatrix} R & R \\ \pi^n R & R \end{pmatrix}$;
(d) O contains a subring isomorphic to $\begin{pmatrix} R & 0 \\ 0 & R \end{pmatrix}$.

(8) Let O be a maximal order of $\mathrm{End}(V)$. The maximal orders situated at a distance n from O are the extremities of paths without a return of origin O and length n.

(9) The maximal orders of $\mathrm{End}(V)$ form a tree where two orders are joined by a line of the tree if and only if their distance apart is equal to 1.

3.8 Classification of Bruhat-Tits trees with complex multiplication

We retain the notation and hypotheses of (3.7.1).

There are precisely 4 distinct types of Bruhat-Tits trees $(\Delta(\mathrm{SL}_2(L)), \mathrm{Exp})$ with complex multiplication by the algebra M. They correspond to the decomposition of the valuation v in the extension of algebras M/L (see Figures 1, 2, 3 and 4).

(3.8.1) If M is reduced, v is inert and unramified in M/L, then (Figure 1)

$$\mathrm{Exp}(\Lambda) = d([\Lambda], [S]).$$

[For if v is inert in the extension M/L then M is a field and π is a local parameter of the discrete valuation ring S. Hence all lattice ideals of S are equivalent as R-lattices. Therefore only one vertex, namely $[S]$, of $\Delta(\mathrm{SL}_2(L))$ has exponent equal to 0; all other vertices have exponent ≥ 1. The formula of (3.8.1) above now immediately follows from theorem 3.7.3. See Figure 1.]

(3.8.2) Assume that M is reduced and v is split completely in M/L. Then S is a semi-local ring. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the 2 maximal ideals of S lying over the maximal ideal of R. Then $\mathfrak{p}_1, \mathfrak{p}_2$ are lattice ideals of S. Let $[n]$, where $n \in \mathbb{Z}$, denote the lattice equivalence class given by

$$[n] = \begin{cases} [\mathfrak{p}_1^n], & \text{if } n \geq 0, \\ [\mathfrak{p}_2^{-n}], & \text{if } n \leq 0, \end{cases}$$

where $\mathfrak{p}_i^n = S$ if $n = 0$. Any lattice ideal of S is equivalent as an R-lattice to $[n]$ for some $n \in \mathbb{Z}$.

We have (Figure 2)

$$\mathrm{Exp}(\Lambda) = \min_{n \in \mathbb{Z}} d([\Lambda], [n]).$$

[The vertices $[n]$, $n \in \mathbb{Z}$, are distinct in the building $\Delta(\mathrm{SL}_2(L))$. Furthermore, $[n]$ and $[n+1]$ are adjacent vertices for all $n \in \mathbb{Z}$ as we have

$$\pi\mathfrak{p}_i^n \subset \mathfrak{p}_i^{n+1} \subset \mathfrak{p}_i^n, \text{ for } i = 1 \text{ or } 2, \text{ and for all } n \in \mathbb{N}.$$

We have evidently $\mathrm{Exp}([n]) = 0$ for all $n \in \mathbb{Z}$. As $\mathfrak{p}_1\mathfrak{p}_2 = \pi S$, it follows that any lattice ideal of S is then equivalent as an R-lattice to either $\mathfrak{p}_1^{n_1}$ or $\mathfrak{p}_2^{n_2}$. The semi-local ring S is a principal ideal ring, as its localisations at the maximal ideals are discrete valuation rings. Hence the ideals $\mathfrak{p}_i^n$ are principal for all $n \geq 0$ and all i. The formula above follows directly from theorem 3.7.3.]

(3.8.3) Suppose M is reduced and that v is ramified in M/L. Then S is a discrete valuation ring. Let $\mathfrak{m}$ be the maximal ideal of S. The vertices $[S]$ and $[\mathfrak{m}]$ are adjacent and distinct in $\Delta(\mathrm{SL}_2(L))$; every lattice ideal of S is equivalent to either $[S]$ or $[\mathfrak{m}]$.

We have (Figure 3)

$$\mathrm{Exp}(\Lambda) = \min\big[d([\Lambda],[S]), d([\Lambda],[\mathfrak{m}])\big].$$

[As v is ramified in M/L we have that M is a field; hence S is a discrete valuation ring contained in M. As

$$\pi S \subset \mathfrak{m} \subset S,$$

the vertices $[S]$ and $[\mathfrak{m}]$ are adjacent and distinct in $\Delta(\mathrm{SL}_2(L))$. We have $\mathfrak{m}^2 = \pi S$. Hence the lattice ideals of S are equivalent as R-lattices either to S or to $\mathfrak{m}$. The formula stated above then follows directly from theorem 3.7.3. We may then construct Figure 3.]

(3.8.4) Suppose M is not reduced. Then for some non-zero element $\epsilon \in M$ we have $M = L[\epsilon]$ where $\epsilon^2 = 0$; furthermore, we have $S = R \oplus L\epsilon$. Fix a lattice $\Lambda_0 = R \oplus R\epsilon$ which is a subring of S.

We have (Figure 4)

$$|\mathrm{Exp}(\Lambda)| = \min_I d([\Lambda],[I])$$

where the minimum runs over all lattice ideals I of Λ_0 of exponent 0.

[This follows directly from theorem 3.7.5.]

(3.8.5) *Alternative arguments.* Instead of using theorems 3.7.3 and 3.7.5, one may use directly lemma 3.7.12 or corollary 3.5.2 to construct at least part of the Figures 1,2,3 and 4. For example:

(1) Assume that M is reduced and v is inert and unramified in M/L. By lemma 3.7.6 we have that the κ-algebra $f_S(\mathrm{End}_R^M(S))$ is isomorphic to the residue field $S/\pi S$ of the discrete valuation ring S. As the extension of residue fields $\kappa \subset S/\pi S$ is non-trivial, there is an element ϵ of $f_S(\mathrm{End}_R^M(S))$ whose characteristic polynomial over κ has no roots rational over κ; hence ϵ has no κ-rational eigenspaces on $S \otimes_R \kappa$. It follows from lemma 3.7.12(ii) that if Λ is a sublattice of S such that $[\Lambda]$ and $[S]$ are adjacent distinct vertices in the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$ then we have

$$\mathrm{Exp}(\Lambda) > \mathrm{Exp}(S) = 0.$$

Again by lemma 3.7.12(i), for such a lattice Λ we obtain that

$$\mathrm{Exp}(\Lambda) = 1.$$

This is equivalent to saying that the vertices in the star $\mathrm{st}([S])$ in $\Delta(\mathrm{SL}_2(L))$ have exponent of conductor equal to 1. See Figure 1.

(2) Assume that M is reduced and v is split completely in M/L. Let Λ be a lattice of S in the class $[n]$; then $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ consists of the diagonal elements of $\mathrm{End}_\kappa(\Lambda \otimes_R \kappa)$ hence there are 2 common 1-dimensional eigenspaces of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$. By lemma 3.7.12(ii), the star $\mathrm{st}([n])$ has precisely 2 vertices of exponent equal to 0 namely $[n-1]$ and $[n+1]$; all other vertices of $\mathrm{st}([n])$ have exponent equal to 1.

If Λ is a lattice of S of exponent ≥ 1, then the image $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ is isomorphic to $\kappa[\epsilon]/(\epsilon^2)$ (lemmas 3.7.6 and 3.7.7); hence there is one common 1-dimensional eigenspace of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ on $\Lambda \otimes_R \kappa$. Hence (lemma 3.7.12) the vertices of $\mathrm{st}([\Lambda])$ all have exponent equal to $\mathrm{Exp}(\Lambda) + 1$ except for one vertex which has exponent $\mathrm{Exp}(\Lambda) - 1$. See Figure 2.

(3) Assume that M is reduced and v is ramified in M/L. By lemma 3.7.6 we have that the κ-algebra $f_S(\mathrm{End}_R^M(S))$ is isomorphic to the non-reduced ring $S/\pi S \cong \kappa[\epsilon]/(\epsilon^2)$. Hence the elements of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ have one common eigenspace on $\Lambda \otimes_R \kappa$, therefore (lemma 3.7.12) the star $\mathrm{st}([\Lambda])$ has precisely one vertex of exponent 0; all other vertices have exponent 1.

If Λ is a lattice of S of exponent ≥ 1, then the image $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ is isomorphic to $\kappa[\epsilon]/(\epsilon^2)$ (by lemmas 3.7.6 and 3.7.7); hence, in the same way as in case (2) above, we conclude that the vertices of $\mathrm{st}([\Lambda])$ all have exponent equal to $\mathrm{Exp}(\Lambda) + 1$ except for one vertex which has exponent $\mathrm{Exp}(\Lambda) - 1$. See Figure 3.

(4) Assume that M is not reduced. If Λ is a lattice of M, then the image $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ is isomorphic to $\kappa[\epsilon]/(\epsilon^2)$ (lemmas 3.7.6 and 3.7.7); hence there is one common 1-dimensional eigenspace of $f_\Lambda(\mathrm{End}_R^M(\Lambda))$ on $\Lambda \otimes_R \kappa$. Hence (lemma 3.7.12) the vertices of $\mathrm{st}([\Lambda])$ all have exponent equal to $\mathrm{Exp}(\Lambda) + 1$ except for precisely one vertex which has exponent $\mathrm{Exp}(\Lambda) - 1$. See Figure 4.

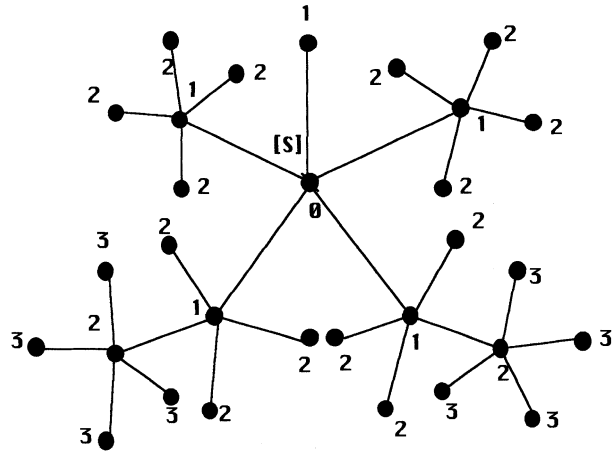

Fig. 1. The Bruhat-Tits building $\Delta(\mathrm{SL}(2,R))$ with CM: v is inert and M is reduced

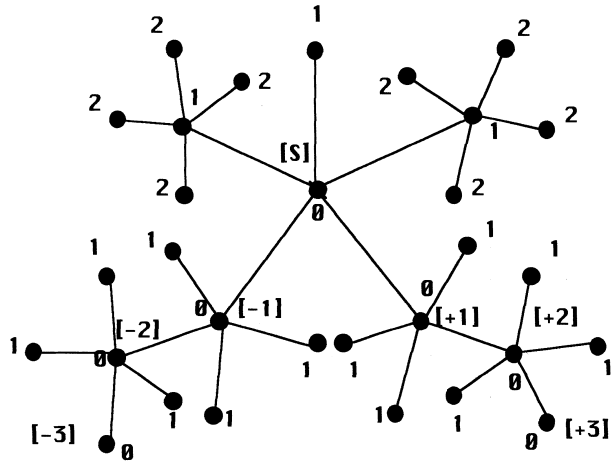

Fig. 2. The Bruhat-Tits building $\Delta(\mathrm{SL}(2,R))$ with CM: v is split completely and M is reduced

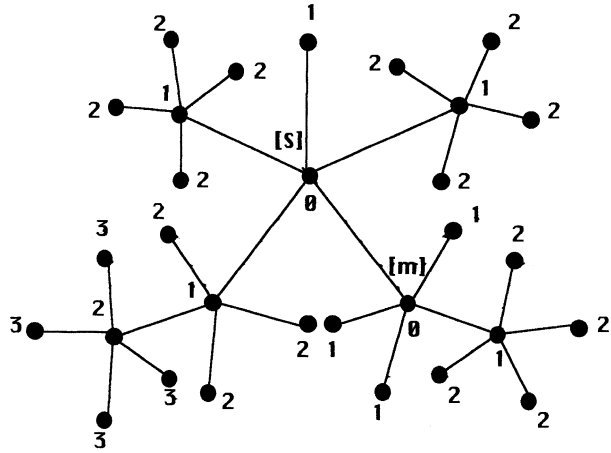

Fig. 3. The Bruhat-Tits building $\Delta(\mathrm{SL}(2,R))$ with CM: v is ramified and M is reduced

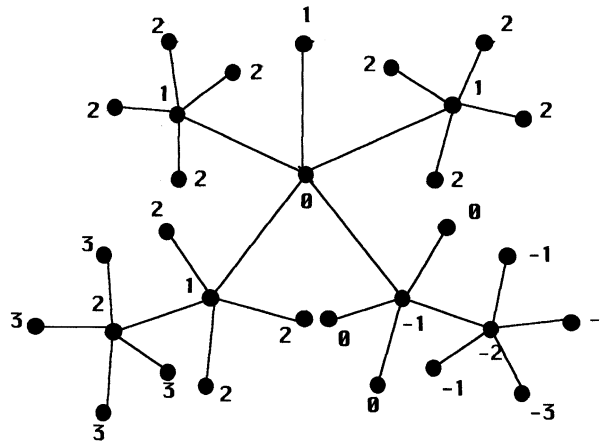

Fig. 4. The Bruhat-Tits building $\Delta(\mathrm{SL}(2,R))$ with CM: M is not reduced

3.9 Lattices in quadratic extensions: Dedekind domains

We extend some of the results on lattices over excellent discrete valuation rings of the first part of this chapter to lattices over excellent Dedekind domains.

(3.9.1) Let

R be an excellent Dedekind domain;
L be the field of fractions of R;
$\mathfrak{p}$ be a maximal ideal of R;
$R_\mathfrak{p}$ be the localisation of R at $\mathfrak{p}$;
$v_\mathfrak{p}$ be the discrete valuation on L associated to $\mathfrak{p}$ and normalised so that $v(\pi) = 1$ where $\pi \in R_\mathfrak{p}$ is a local parameter with respect to $\mathfrak{p}$;
M/L be a 2-dimensional reduced commutative L-algebra (M is a field or is L-isomorphic to $L \times L$ by proposition 3.3.1);
S be the integral closure of R in M.

(3.9.2) An *R-lattice Λ in M* is a finitely generated R-submodule of M which generates M as a vector space over L. For example, S is an R-lattice in M as R is excellent.

For any R-lattice Λ in M, let $\mathrm{End}_R^M(\Lambda)$ be the endomorphism ring of the lattice Λ with respect to M, that is to say:

$$\mathrm{End}_R^M(\Lambda) = \{x \in M |\ x\Lambda \subseteq \Lambda\}.$$

(3.9.3) Let $\Lambda_1, \Lambda_2, \Lambda_3$ be R-lattices in M. The local index $[\Lambda_1 R_\mathfrak{p} : \Lambda_2 R_\mathfrak{p}]$, which is a fractionary ideal of the discrete valuation ring $R_\mathfrak{p}$, has been defined in (3.2.3) for all maximal ideals $\mathfrak{p}$ of R.

Let $[\Lambda_1 : \Lambda_2]$ be the module index of Λ_2 in Λ_1. This is the fractionary ideal of R which is uniquely determined by the condition (see [CF, Chapter 1, §3, p.10]):

$$[\Lambda_1 : \Lambda_2]R_\mathfrak{p} = [\Lambda_1 R_\mathfrak{p} : \Lambda_2 R_\mathfrak{p}] \text{ for all maximal ideals } \mathfrak{p} \text{ of } R.$$

Note that $\Lambda_1 R_\mathfrak{p} = \Lambda_2 R_\mathfrak{p}$ for all but finitely many prime ideals $\mathfrak{p}$ of R so that $[\Lambda_1 : \Lambda_2]$ is well defined. These properties are easily shown:

$$[\Lambda_1 : \Lambda_2] = [\Lambda_2 : \Lambda_1]^{-1};$$
$$[\Lambda_1 : \Lambda_2][\Lambda_2 : \Lambda_3] = [\Lambda_1 : \Lambda_3];$$
$$[\Lambda_1 : \Lambda_2] \text{ is an ideal of } R \text{ if } \Lambda_1 \supseteq \Lambda_2;$$
$$[\Lambda_1 : \Lambda_2] = R \text{ and } \Lambda_1 \supseteq \Lambda_2 \text{ imply that } \Lambda_1 = \Lambda_2.$$

(3.9.4) An *order* O in M, with respect to R, is an R-subalgebra of S such that O generates M as an L-vector space. The *conductor* of O is the ideal of R given by $[S : O]$ (this generalises (2.2.6)).

(3.9.5) For any R-lattice Λ of M, the ring $\mathrm{End}_R^M(\Lambda)$ is an order of S, with respect to R.

[For the proof, it is clear that $R \subseteq \mathrm{End}_R^M(\Lambda)$ so that $\mathrm{End}_R^M(\Lambda)$ is an R-subalgebra of M. As S and Λ are R-lattices of M there are non-zero elements $b_1, b_2 \in R - \{0\}$ such that $b_1 S \subseteq \Lambda \subseteq b_2^{-1} S$. Hence we have the inclusion

$$b_1 b_2 S \subseteq \mathrm{End}_R^M(\Lambda).$$

Let $\lambda_1, \ldots, \lambda_r$ be finite set of generators of Λ as an R-module. Then an element $u \in \mathrm{End}_R^M(\Lambda)$ is represented with respect to this set of generators by a matrix $[a_{ij}]$ of order $r \times r$ with coefficients in R:

$$u(\lambda_i) = \sum_j a_{ij} \lambda_j, \text{ for all } i.$$

It follows that u satisfies a monic polynomial equation with coefficients in R, namely the equation $\det([a_{ij}] - XI_r) = 0$; hence the element u of M is integral over R. As S is the integral closure of R in M, this shows that $\mathrm{End}_R^M(\Lambda) \subseteq S$. The inclusions of R-modules $b_1 b_2 S \subseteq \mathrm{End}_R^M(\Lambda) \subseteq S$ prove that $\mathrm{End}_R^M(\Lambda)$ is an R-lattice of M and an order of S.]

(3.9.6) Let Λ be an R-lattice in M. The *conductor of* Λ is the conductor of the order $\mathrm{End}_R^M(\Lambda)$ relative to S, that is to say

$$\mathrm{cond}(\Lambda) = [S : \mathrm{End}_R^M(\Lambda)].$$

This conductor $\mathrm{cond}(\Lambda)$ is a non-zero ideal of R of the form

$$\mathrm{cond}(\Lambda) = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{Exp}_\mathfrak{p}(\Lambda)}$$

where the product runs over all non-zero prime ideals $\mathfrak{p}$ of the Dedekind domain R and where the integers $\mathrm{Exp}_\mathfrak{p}(\Lambda)$ are non-negative and are zero for

all but finitely many prime ideals $\mathfrak{p}$. This integer $\mathrm{Exp}_{\mathfrak{p}}(\Lambda) \in \mathbb{N}$ is the *local exponent of the conductor of* Λ *at* $\mathfrak{p}$.

(3.9.7) Let Λ be an R-lattice contained in M and $\mathfrak{p}$ be a maximal ideal of R. Let $R_{\mathfrak{p}}$ be the localisation of R at $\mathfrak{p}$. Then $\Lambda \otimes_R R_{\mathfrak{p}}$ is an $R_{\mathfrak{p}}$-lattice contained in M and hence the exponent of the conductor $\mathrm{Exp}(\Lambda \otimes_R R_{\mathfrak{p}})$ with respect to the discrete valuation ring $R_{\mathfrak{p}}$ is defined as in §3.3. We have

$$\mathrm{Exp}_{\mathfrak{p}}(\Lambda) = \mathrm{Exp}(\Lambda \otimes_R R_{\mathfrak{p}}).$$

[We have the equality of endomorphism rings, as subrings of M,

$$\mathrm{End}_R^M(\Lambda) \otimes_R R_{\mathfrak{p}} = \mathrm{End}_{R_{\mathfrak{p}}}^M(\Lambda \otimes_R R_{\mathfrak{p}})$$

obtained by localization at $\mathfrak{p}$. Furthermore, $SR_{\mathfrak{p}}$ is the integral closure of $R_{\mathfrak{p}}$ in M. This implies an equality of conductor ideals

$$[S : \mathrm{End}_R^M(\Lambda)] \otimes_R R_{\mathfrak{p}} = [SR_{\mathfrak{p}} : \mathrm{End}_{R_{\mathfrak{p}}}^M(\Lambda \otimes_R R_{\mathfrak{p}})].$$

The equality of exponents of conductors results from this.]

(3.9.8) Let $\hat{R}_{\mathfrak{p}}$ be the completion of the local ring $R_{\mathfrak{p}}$ for a maximal ideal $\mathfrak{p}$ of R. Let $\hat{L}_{\mathfrak{p}}$ be the fraction field of the discrete valuation ring $\hat{R}_{\mathfrak{p}}$. Let $\mathbb{A}_R$ be the adèle ring of the Dedekind domain R. That is to say, $\mathbb{A}_R$ is the restricted topological product of the $\hat{L}_{\mathfrak{p}}$ for all maximal ideals $\mathfrak{p}$ of R with respect to the subrings $\hat{R}_{\mathfrak{p}}$. Let $\hat{O}_R$ be the subring of $\mathbb{A}_R$ of adèles $(a_{\mathfrak{p}})_{\mathfrak{p}}$ such that $a_{\mathfrak{p}} \in \hat{R}_{\mathfrak{p}}$ for all $\mathfrak{p}$.

Fix an R-sublattice Λ_0 of M. Let Λ be an R-lattice of M. Then there is an element $f \in \mathrm{GL}_2(\mathbb{A}_R)$ such that there is an equality of submodules of $M \otimes_R \hat{O}_R$

$$f(\Lambda_0) \otimes_R \hat{O}_R = \Lambda \otimes_R \hat{O}_R.$$

Furthermore, another element $g \in \mathrm{GL}_2(\mathbb{A}_R)$ satisfies the condition $g(\Lambda_0) \otimes_R \hat{O}_R = \Lambda \otimes_R \hat{O}_R$ if and only if f, g lie in the same coset of $\mathrm{GL}_2(\hat{O}_R)$ in $\mathrm{GL}_2(\mathbb{A}_R)$. This then defines a bijection of sets

$$\left\{ R - \text{sublattices of } M \right\} \longrightarrow \mathrm{GL}_2(\mathbb{A}_R)/\mathrm{GL}_2(\hat{O}_R), \quad \Lambda \mapsto f\mathrm{GL}_2(\hat{O}_R).$$

[To show that this map is a bijection, we construct an inverse map. Let $f = (f_{\mathfrak{p}})_{\mathfrak{p}} \in \mathrm{GL}_2(\mathbb{A}_R)$. Then for each $\mathfrak{p}$ we have a homomorphism of R-modules

$$f_{\mathfrak{p}} : M \to M \otimes_R \hat{L}_{\mathfrak{p}}.$$

Hence for each maximal ideal $\mathfrak{p}$ of M we obtain an $\hat{R}_{\mathfrak{p}}$-lattice of rank 2 of $M \otimes_R \hat{R}_{\mathfrak{p}}$ given by $f_{\mathfrak{p}}(\Lambda_0) \otimes_R \hat{R}_{\mathfrak{p}}$. We put

$$\Lambda(\mathfrak{p}) = M \cap (f_{\mathfrak{p}}(\Lambda_0) \otimes_R \hat{R}_{\mathfrak{p}})$$

where this makes sense if we identify M with its image in $M \otimes_R \hat{L}_\mathfrak{p}$ under the map $m \mapsto m \otimes_R 1$. Clearly, $\Lambda(\mathfrak{p})$ is an $R_\mathfrak{p}$-lattice in M which satisfies $\Lambda(\mathfrak{p})\hat{R}_\mathfrak{p} = f_\mathfrak{p}(\Lambda_0) \otimes_R \hat{R}_\mathfrak{p}$ for all $\mathfrak{p}$ and

$$\Lambda(\mathfrak{p}) = \Lambda_0 R_\mathfrak{p} \quad \text{for all except finitely many } \mathfrak{p}.$$

We then put

$$\Lambda = \bigcap_\mathfrak{p} \Lambda(\mathfrak{p}).$$

Then Λ is an R-submodule of M which generates M as an L-vector space. That Λ is a noetherian R-module follows from the modules $\Lambda(\mathfrak{p})$ being noetherian $R_\mathfrak{p}$-modules and that $\Lambda(\mathfrak{p}) = \Lambda_0 R_\mathfrak{p}$ for all except finitely many $\mathfrak{p}$ and that $\Lambda = \bigcap_\mathfrak{p} \Lambda(\mathfrak{p})$. Hence Λ is an R-lattice of M. As $\Lambda R_\mathfrak{p} = \Lambda(\mathfrak{p})$ for all $\mathfrak{p}$ it follows that Λ is an R-submodule of M whose image in $\mathrm{GL}_2(\mathbb{A}_R)/\mathrm{GL}_2(\hat{O}_R)$ is the coset $f\mathrm{GL}_2(\hat{O}_R)$.]

(3.9.9) The group of fractionary ideals of the Dedekind domain R acts naturally on the sublattices of M: if I is a fractionary ideal of R and Λ is an R-sublattice of M then $I\Lambda$ is also a sublattice of M. We have the equality of endomorphism rings

$$\mathrm{End}_R^M(\Lambda) = \mathrm{End}_R^M(I\Lambda)$$

and equality of conductors

$$\mathrm{cond}(\Lambda) = \mathrm{cond}(I\Lambda).$$

3.10 The global Bruhat-Tits net

We retain the notation and hypotheses (3.9.1) of the preceding section; in particular, R is an excellent Dedekind domain and M/L is a 2-dimensional reduced commutative L-algebra (M is a field or is L-isomorphic to $L \times L$ by proposition 3.3.1).

(3.10.1) Let Λ, Λ' be R-lattices of M and $\mathfrak{p}$ be a maximal ideal of the excellent Dedekind domain R. Then Λ' is a $\mathfrak{p}$-*lower modification of* Λ if $\Lambda' \subset \Lambda$ and there is an isomorphism of R-modules

$$\Lambda/\Lambda' \cong R/\mathfrak{p}.$$

Similarly, Λ' is a $\mathfrak{p}$-*upper modification of* Λ if $\Lambda' \supset \Lambda$ and there is an isomorphism of R-modules $\Lambda'/\Lambda \cong R/\mathfrak{p}$. The lattice Λ' is a $\mathfrak{p}$-*modification of* Λ if it is either a $\mathfrak{p}$-upper or a $\mathfrak{p}$-lower modification of Λ.

(3.10.2) Exactly as for discrete valuation rings (§3.1), we define these relations between R-lattices of M:

(1) Two R-lattices Λ, Λ' of L are *equivalent* if there is $a \in M^*$ such that

$$a\Lambda = \Lambda'.$$

Equivalence of R-lattices is an equivalence relation. For an R-lattice Λ in M we write $[\Lambda]$ for the corresponding lattice class.

(2) Let $\mathfrak{p}$ be a maximal ideal of R. Two R-lattice classes $[\Lambda], [\Lambda']$ of M are $\mathfrak{p}$-*incident* if either they are equal or they admit representatives Λ, Λ' such that Λ' is a $\mathfrak{p}$-modification of Λ. The relation of $\mathfrak{p}$-incidence is symmetric and reflexive amongst the lattice classes for every maximal ideal $\mathfrak{p}$ of R.

(3.10.3) Equivalent definitions of $\mathfrak{p}$-incidence are: the R-lattice classes $[\Lambda], [\Lambda']$ of M are $\mathfrak{p}$-incident if either they are equal or they admit representatives Λ, Λ' such that

$$\Lambda R_{\mathfrak{q}} = \Lambda' R_{\mathfrak{q}} \text{ for all } \mathfrak{q} \neq \mathfrak{p}$$

and either

$$\mathfrak{p}\Lambda R_{\mathfrak{p}} \subset \Lambda' R_{\mathfrak{p}} \subset \Lambda R_{\mathfrak{p}},\ \mathfrak{p}\Lambda R_{\mathfrak{p}} \neq \Lambda' R_{\mathfrak{p}},$$

or

$$\mathfrak{p}\Lambda' R_{\mathfrak{p}} \subset \Lambda R_{\mathfrak{p}} \subset \Lambda' R_{\mathfrak{p}},\ \Lambda R_{\mathfrak{p}} \neq \mathfrak{p}\Lambda' R_{\mathfrak{p}}.$$

Alternatively, the R-lattice classes $[\Lambda], [\Lambda']$ of M are $\mathfrak{p}$-incident if and only if they admit representative lattices Λ, Λ' such that (see (3.9.3))

$$[\Lambda : \Lambda'] = \mathfrak{p}^m \text{ where the integer } m \text{ satisfies } -1 \leq m \leq 1 \text{ and}$$

$$\text{either } \Lambda \supseteq \Lambda' \text{ or } \Lambda \subseteq \Lambda'.$$

(3.10.4) Two R-lattice classes $[\Lambda], [\Lambda']$ of M are $\mathfrak{p}$-incident and $\mathfrak{q}$-incident where $\mathfrak{p}, \mathfrak{q}$ are two distinct maximal ideals of R if and only if $[\Lambda] = [\Lambda']$.

[For the proof, if $[\Lambda] = [\Lambda']$ then evidently the lattice classes $[\Lambda], [\Lambda']$ are $\mathfrak{p}$-incident for all maximal ideals $\mathfrak{p}$ of R. Conversely, assume that $[\Lambda], [\Lambda']$ are both $\mathfrak{p}$-incident and $\mathfrak{q}$-incident where $\mathfrak{p}, \mathfrak{q}$ are distinct maximal ideals of R. We may select representative lattices Λ, Λ' in M of these classes and an element $a \in L^*$ such that $[\Lambda : \Lambda'] = \mathfrak{p}^m$, where $|m| \leq 1$, and $[\Lambda : a\Lambda'] = \mathfrak{q}^n$, where $|n| \leq 1$. But we have $[\Lambda : a\Lambda'] = (a^2R)[\Lambda : \Lambda'] = (a^2R)\mathfrak{p}^m$. Hence we have the equality of fractionary ideals $\mathfrak{q}^n\mathfrak{p}^{-m} = (a^2R)$. This implies that both m and n are even integers and hence that $n = m = 0$; this shows that $[\Lambda] = [\Lambda']$, as required.]

(3.10.5) The group $\mathrm{GL}_2(L)$ acts on a basis of M over L; hence $\mathrm{GL}_2(L)$ acts as a permutation group on the set of R-lattice classes of M and also on the set of equivalence classes of R-lattices of M.

The group of fractionary ideals of R acts on the R-lattices of M via $\Lambda \mapsto I\Lambda$ for any fractionary ideal I (see (3.9.9)). Hence the group of fractionary ideals of R acts as a permutation group on the equivalence classes of R-lattice classes of M. This action factors through the Picard group $\mathrm{Pic}(R)$ and we obtain a permutation action of $\mathrm{Pic}(R)$ on the lattice classes which is noted as

$$[\Lambda] \mapsto [\Lambda] \otimes_R \mathcal{I}$$

where $\mathcal{I}$ is any locally free R-module of rank 1.

The action of $\mathrm{Pic}(R)$ on the lattice classes preserves the relation of $\mathfrak{p}$-incidence for any maximal ideal $\mathfrak{p}$.

(3.10.6) The R-lattice classes $[\Lambda], [\Lambda']$ of M are *locally* $\mathfrak{p}$*-incident* if either they are equal or for every prime ideal $\mathfrak{q}$ they admit representatives $\Lambda(\mathfrak{q}), \Lambda'(\mathfrak{q})$ such that

$$\Lambda(\mathfrak{q})R_{\mathfrak{q}} = \Lambda'(\mathfrak{q})R_{\mathfrak{q}} \text{ for all } \mathfrak{q} \neq \mathfrak{p}$$

and either

$$\mathfrak{p}\Lambda(\mathfrak{p})R_{\mathfrak{p}} \subset \Lambda'(\mathfrak{p})R_{\mathfrak{p}} \subset \Lambda(\mathfrak{p})R_{\mathfrak{p}},\ \mathfrak{p}\Lambda(\mathfrak{p})R_{\mathfrak{p}} \neq \Lambda'(\mathfrak{p})R_{\mathfrak{p}},$$

or

$$\mathfrak{p}\Lambda'(\mathfrak{p})R_{\mathfrak{p}} \subset \Lambda(\mathfrak{p})R_{\mathfrak{p}} \subset \Lambda'(\mathfrak{p})R_{\mathfrak{p}},\ \Lambda(\mathfrak{p})R_{\mathfrak{p}} \neq \mathfrak{p}\Lambda'(\mathfrak{p})R_{\mathfrak{p}}.$$

(Compare (3.10.3)). Then we have that $[\Lambda], [\Lambda']$ are locally $\mathfrak{p}$-incident if and only if for some locally free R-module $\mathcal{I}$ of rank 1 the R-lattices $[\Lambda], [\Lambda'] \otimes_R \mathcal{I}$ are $\mathfrak{p}$-incident.

[For we have elements $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in L^*$ such that $a_{\mathfrak{p}}\Lambda = \Lambda(\mathfrak{p})$ and $b_{\mathfrak{p}}\Lambda' = \Lambda'(\mathfrak{p})$ for all maximal ideals $\mathfrak{p}$. The elements $a_{\mathfrak{p}}b_{\mathfrak{p}}^{-1}$ then generate a fractionary ideal I of R such that the lattices $[I\Lambda]$ and $[\Lambda']$ are $\mathfrak{p}$-incident.]

(3.10.7) Let $\mathcal{L}$ be the set of lattice classes of M. A $\mathfrak{p}$*-flag* of $\mathcal{L}$ is a set of pairwise $\mathfrak{p}$-incident distinct elements of $\mathcal{L}$.

Let Δ_R be the flag complex associated to $\mathcal{L}$; this is a simplicial complex Δ_R with $\mathcal{L}$ as a vertex set and the finite $\mathfrak{p}$-flags as simplices for all maximal ideals $\mathfrak{p}$ of R. Each simplex corresponds to a $\mathfrak{p}$-flag for a unique maximal ideal $\mathfrak{p}$ of R (by (3.10.4)) except for the 0-simplices. Hence each simplex of dimension ≥ 1 is labelled by one maximal ideal of R; each 0-simplex is labelled by all the maximal ideals.

The simplicial complex Δ_R has only 0-simplices and 1-simplices and no higher dimensional simplices. Let $\mathrm{Sim}_1(\Delta_R)$ be the set of 1-simplices of Δ_R.

As each 1-simplex s is a $\mathfrak{p}$-flag for some unique $\mathfrak{p}$ we obtain a labelling map

$$\begin{aligned} \mathrm{Sim}_1(\Delta_R) &\to \mathrm{Max}(R) \\ s &\mapsto \mathfrak{p} \end{aligned}$$

where $\mathrm{Max}(R)$ is the set of maximal ideals of R.

(3.10.8) The *global Bruhat-Tits net* $\Delta_R(\mathrm{SL}_2(L))$ *with respect to* R is the simplicial complex Δ_R equipped with the labelling of the 1-simplices

$$\mathrm{Sim}_1(\Delta_R) \to \mathrm{Max}(R).$$

The Picard group $\mathrm{Pic}(R)$ acts as a group of automorphisms of the simplicial complex Δ_R and preserves the labelling map of 1-simplices. Hence $\mathrm{Pic}(R)$ acts as a group of automorphisms of the global Bruhat-Tits net $\Delta_R(\mathrm{SL}_2(L))$.

(3.10.9) Let $[\Lambda] \in \mathcal{L}$ be a lattice class. Let $C(\mathfrak{p}, [\Lambda])$, the $\mathfrak{p}$-*connected component of* $[\Lambda]$, be the set of points of the simplicial complex $\Delta_R(\mathrm{SL}_2(L))$ which are connected to the vertex $[\Lambda]$ by an arc consisting of $\mathfrak{p}$-labelled 1-simplices.

The following properties of $C(\mathfrak{p}, [\Lambda])$ are immediate consequences of the definition and elementary results on modules over Dedekind domains:

(a) The complex $C(\mathfrak{p}, [\Lambda])$ is the maximal connected subcomplex of $\Delta_R(\mathrm{SL}_2(L))$ containing $[\Lambda]$ whose 1-simplices are contained in the fibre of the map $\mathrm{Sim}_1(\Delta_R) \to \mathrm{Max}(R)$ over $\mathfrak{p}$.

(b) As a simplicial complex, $C(\mathfrak{p}, [\Lambda])$ is simplicially isomorphic to the Bruhat-Tits tree $\Delta(\mathrm{SL}_2(L))$ relative to the discrete valuation $v_\mathfrak{p}$ of L.

(c) For a fixed maximal ideal $\mathfrak{p}$, the components $C(\mathfrak{p}, [\Lambda])$ are disjoint or equal, as $[\Lambda]$ runs through all elements of $\mathcal{L}$.

(d) Two lattice classes $[\Lambda], [\Lambda']$ of $\mathcal{L}$ lie in the same component $C(\mathfrak{p}, [\Lambda])$ if and only if they admit representive lattices Λ, Λ' of M such that there is a sequence of R-lattices $\Lambda_1, \Lambda_2, \ldots, \Lambda_n$ of M where Λ_i and Λ_{i+1} are $\mathfrak{p}$-incident, for all i, and $\Lambda = \Lambda_1$, $\Lambda' = \Lambda_n$.

(e) For each maximal ideal $\mathfrak{p}$, let $d_\mathfrak{p}$ denote the standard metric on the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$, with respect to the discrete valuation $v_\mathfrak{p}$, normalised so that the distance between adjacent vertices is equal to 1 (see §3.1). Then $d_\mathfrak{p}$ induces a metric, also noted $d_\mathfrak{p}$, on each $\mathfrak{p}$-connected component $C(\mathfrak{p}, [\Lambda])$ of $\Delta_R(\mathrm{SL}_2(L))$.

(f) If $[\Lambda], [\Lambda']$ of $\mathcal{L}$ lie in the same component $C(\mathfrak{p}, [\Lambda])$ then there is $a \in L^*$ such that

$$[\Lambda : a\Lambda'] = \mathfrak{p}^m \quad \text{where} \quad |m| \leq d_{\mathfrak{p}}([\Lambda], [\Lambda']).$$

[This follows from (d) and (e).]

(g) If $\mathfrak{p}$ and $\mathfrak{q}$ are distinct maximal ideals of R, and $[\Lambda], [\Lambda'] \in \mathcal{L}$, then $C(\mathfrak{p}, [\Lambda])$ and $C(\mathfrak{q}, [\Lambda'])$ are either disjoint or intersect in precisely one vertex of $\Delta_R(\mathrm{SL}_2(L))$.
[To prove this, by localising R we may reduce to the case where R is a semi-local Dedekind domain with precisely two maximal ideals $\mathfrak{p}, \mathfrak{q}$. Hence R is a unique factorisation domain. Suppose that $[\Lambda], [\Lambda'] \in \mathcal{L}$ are two distinct points lying in both $C(\mathfrak{p}, [\Lambda])$ and $C(\mathfrak{q}, [\Lambda'])$; selecting geodesics in the trees $C(\mathfrak{p}, [\Lambda])$, $C(\mathfrak{q}, [\Lambda'])$ joining $[\Lambda], [\Lambda']$ then there is corresponding sequence of $\mathfrak{p}$-lower modifications $\Lambda \supset \Lambda_1 \supset \ldots \supset \Lambda_n$ and a corresponding sequence of $\mathfrak{q}$-lower modifications $\Lambda \supset \Lambda'_1 \supset \ldots \supset \Lambda'_m$ where $\Lambda_n = a\Lambda'_m$ for some $a \in L^*$ and $\Lambda_n, a\Lambda'_m$ lie in the class $[\Lambda']$. The invariants of Λ/Λ_n as an $R_{\mathfrak{p}}$-module are $0, n$ and the invariants of Λ/Λ'_m as an $R_{\mathfrak{q}}$-module are $0, m$. As $\Lambda_n = a\Lambda'_m$, it easily follows that this is impossible.]

(3.10.10) The complex $\Delta_R(\mathrm{SL}_2(L))$ is a union of all the $\mathfrak{p}$-connected components

$$\Delta_R(\mathrm{SL}_2(L)) = \bigcup_{\mathfrak{p}, [\Lambda]} C(\mathfrak{p}, [\Lambda])$$

where the union runs over all maximal ideals $\mathfrak{p}$ of R and all vertices $[\Lambda]$ in $\mathcal{L}$. That is to say $\Delta_R(\mathrm{SL}_2(L))$ is a connected simplicial complex which is a union of Bruhat-Tits trees.

3.11 Bruhat-Tits nets with complex multiplication

We retain the notation (3.9.1) of §3.9; in particular M is a reduced 2-dimensional commutative algebra over the field L which is the field of fractions of the excellent Dedekind domain R. We may identify the vertices $\mathcal{L}$ of the Bruhat-Tits net $\Delta_R(\mathrm{SL}_2(L))$ with the R-lattice classes of M (see (3.10.7), (3.10.8)).

(3.11.1) Let $\mathrm{Div}(R)$ be the group of divisors on Spec R; we shall write the composition law additively. This group $\mathrm{Div}(R)$ is equipped with its usual partial order $\leq$, where a divisor D is ≥ 0 if and only if it is effective. We may identify fractionary ideals of R with divisors in $\mathrm{Div}(R)$.

(3.11.2) Let Λ be an R-lattice of M. The conductor $\mathrm{cond}(\Lambda)$ of Λ (see (3.9.6)) is an ideal of the Dedekind domain R which depends only on the equivalence

class $[\Lambda]$ of the lattice Λ. We identify this conductor ideal with its corresponding divisor; hence we obtain a conductor map on the set of vertices $\mathcal{L}$ of $\Delta_R(\mathrm{SL}_2(L))$ with values in the group $\mathrm{Div}(R)$ of all divisors of R

$$\mathrm{cond} : \mathcal{L} \to \mathrm{Div}(R).$$

(3.11.3) The triple $(\Delta_R(\mathrm{SL}_2(L)), \mathrm{cond}, M)$ consisting of the global Bruhat Tits net $\Delta_R(\mathrm{SL}_2(L))$ (see §3.10) and the associated conductor map, and the algebra M, is a *Bruhat-Tits net with complex multiplication by* M.

(3.11.4) We define a map

$$D : \mathcal{L} \times \mathcal{L} \to \mathrm{Div}(R)$$

in the following way. Let $[\Lambda], [\Lambda'] \in \mathcal{L}$ be two R-lattice classes; select representative R-lattices Λ, Λ' contained in M of these classes $[\Lambda], [\Lambda']$. For each maximal ideal $\mathfrak{p}$, we have the $R_\mathfrak{p}$-lattices $\Lambda \otimes_R R_\mathfrak{p}, \Lambda' \otimes_R R_\mathfrak{p}$ in M and their associated lattice classes $[\Lambda \otimes_R R_\mathfrak{p}], [\Lambda' \otimes_R R_\mathfrak{p}]$; we put

$$n_\mathfrak{p} = d_\mathfrak{p}([\Lambda \otimes_R R_\mathfrak{p}], [\Lambda' \otimes_R R_\mathfrak{p}])$$

where $d_\mathfrak{p}$ denotes the normalised standard metric on the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$, with respect to the discrete valuation $v_\mathfrak{p}$ (see §3.1). Put

$$D([\Lambda], [\Lambda']) = \sum_\mathfrak{p} n_\mathfrak{p}.\mathfrak{p}$$

where the sum runs over all the maximal ideals $\mathfrak{p}$ of R.

(3.11.5) The map D satisfies these properties:

(I) $D(v_1, v_3) \leq D(v_1, v_2) + D(v_2, v_3)$ for elements v_1, v_2, v_3 of $\mathcal{L}$

(II) $D(v_1, v_2) = D(v_2, v_1)$

(III) $D(v_1, v_2) = 0$ if and only if $v_1 = v_2 \otimes_R \mathcal{I}$ for some $\mathcal{I} \in \mathrm{Pic}(R)$

(IV) $D(v_1, v_2) \geq 0$ for all $v_1, v_2 \in \mathcal{L}$

(V) $D(v_1, v_2) = D(v_1 \otimes_R \mathcal{I}, v_2)$ for all $\mathcal{I} \in \mathrm{Pic}(R)$.

That is to say, D satisfies the axioms of a pseudo-metric on $\mathcal{L}$ with values in the partially ordered group $\mathrm{Div}(R)$ and which is induced by a metric on the quotient space $\mathcal{L}/\mathrm{Pic}(R)$ with values in $\mathrm{Div}(R)$.

[The properties (II), (IV), and (V) follow immediately from the definition. For the proof of the triangle inequality (I), if v_i is represented by the R-lattice Λ_i for all i it is sufficient to prove the inequality

$$d_{\mathfrak{p}}([\Lambda_1 \otimes_R R_{\mathfrak{p}}], [\Lambda_3 \otimes_R R_{\mathfrak{p}}]) \leq d_{\mathfrak{p}}([\Lambda_1 \otimes_R R_{\mathfrak{p}}], [\Lambda_2 \otimes_R R_{\mathfrak{p}}]) +$$

$$d_{\mathfrak{p}}([\Lambda_2 \otimes_R R_{\mathfrak{p}}], [\Lambda_3 \otimes_R R_{\mathfrak{p}}]).$$

But this is the usual triangle inequality for $d_{\mathfrak{p}}$ on the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$ with respect to the discrete valuation ring $R_{\mathfrak{p}}$.

To check (III), suppose that $D([\Lambda], [\Lambda']) = 0$. Then we have that

$$[\Lambda \otimes_R R_{\mathfrak{p}}] = [\Lambda' \otimes_R R_{\mathfrak{p}}] \text{ for all } \mathfrak{p}.$$

Then there are elements $a_{\mathfrak{p}} \in L^*$ such that

$$a_{\mathfrak{p}}\Lambda \otimes_R R_{\mathfrak{p}} = \Lambda' \otimes_R R_{\mathfrak{p}} \text{ for all } \mathfrak{p}.$$

where $a_{\mathfrak{p}} = 1$ for all except finitely many $\mathfrak{p}$. The elements $a_{\mathfrak{p}}$ generate a fractionary ideal I of R where we have $I\Lambda \otimes_R R_{\mathfrak{p}} = \Lambda' \otimes_R R_{\mathfrak{p}}$ for all $\mathfrak{p}$. Hence we obtain the equality $I\Lambda = \Lambda'$ as required. Conversely, if $[\mathcal{I} \otimes \Lambda] = [\Lambda']$ for some locally free R-module $\mathcal{I}$ of rank 1 then it follows from (V) that $D([\Lambda], [\Lambda']) = 0$.]

(3.11.6) Two lattice classes $[\Lambda], [\Lambda']$ satisfy $D([\Lambda], [\Lambda']) \leq \mathfrak{p}$ if and only if they are locally $\mathfrak{p}$-incident (see (3.10.6)).

[It immediately follows from the definition that if the lattices are locally $\mathfrak{p}$-incident then $D([\Lambda], [\Lambda']) \leq \mathfrak{p}$. Conversely suppose that $D([\Lambda], [\Lambda']) \leq \mathfrak{p}$. Then we have

$$d_{\mathfrak{q}}([\Lambda \otimes_R R_{\mathfrak{q}}], [\Lambda' \otimes_R R_{\mathfrak{q}}]) \begin{cases} = 0, & \text{if } \mathfrak{q} \neq \mathfrak{p} \\ \leq 1, & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

where $d_{\mathfrak{p}}$ is the standard normalised metric on the Bruhat-Tits tree with respect to $\mathfrak{p}$. It follows that the two lattice classes are locally $\mathfrak{p}$-incident.]

(3.11.7) Let

$$[\Lambda] = P_0, P_1, \ldots, P_{n-1}, [\Lambda'] = P_n$$

be a finite sequence of points of $\mathcal{L}$ such that for all $0 \leq i \leq n-1$ the points P_i and P_{i+1} are locally $\mathfrak{p}(i)$-incident for some prime ideal $\mathfrak{p}(i)$ of R depending on i; for such a sequence $P_0, \ldots, P_n$, we put

$$D(P_0, \ldots, P_n) = \sum_{i=0}^{n-1} d_{\mathfrak{p}(i)}(P_i, P_{i+1}).\mathfrak{p}(i).$$

We then have

$$D([\Lambda],[\Lambda']) = \min_{\substack{P_0,\ldots,P_n \\ n\in\mathbb{N}}} D(P_0,\ldots,P_n)$$

where the minimum runs over all finite sequences $P_0 = [\Lambda], P_1, \ldots, P_{n-1}, P_n = [\Lambda']$, $n \in \mathbb{N}$, of points of $\mathcal{L}$ for which $D(P_0,\ldots,P_n)$ is defined and where the minimum is taken with respect to the usual ordering on divisors.

[For the proof, the triangle inequality of (3.11.5) shows that the inequality $D([\Lambda],[\Lambda']) \leq D(P_0,\ldots,P_n)$ holds where $P_0 = [\Lambda] = P_0, P_1, \ldots, P_{n-1}, P_n = [\Lambda']$ is any sequence of points of $\mathcal{L}$ such that P_i and P_{i+1} are locally $\mathfrak{p}(i)$-incident for all i. Suppose then that $D([\Lambda],[\Lambda']) = \sum_{i=1}^{m} n_{\mathfrak{q}_i}.\mathfrak{q}_i$ where the $\mathfrak{q}_i$ are distinct maximal ideals of R. We have

$$n_{\mathfrak{q}} = d_{\mathfrak{q}}([\Lambda \otimes_R R_{\mathfrak{q}}],[\Lambda' \otimes_R R_{\mathfrak{q}}]) \quad \text{for all } \mathfrak{q}.$$

Hence there are elements $a_{\mathfrak{q}} \in L^*$ where $a_{\mathfrak{q}} = 1$ for all except finitely many primes $\mathfrak{q}$ and there are isomorphisms of $R_{\mathfrak{q}}$-modules

$$(a_{\mathfrak{q}}\Lambda \otimes_R R_{\mathfrak{q}})/(\Lambda' \otimes_R R_{\mathfrak{q}}) \cong R/\mathfrak{q}^{n_{\mathfrak{q}}} \quad \text{for all } \mathfrak{q}.$$

Hence the elements $a_{\mathfrak{q}}$ generate a fractionary ideal I of R. We then have $I\Lambda \supseteq \Lambda'$ and $(I\Lambda \otimes_R R_{\mathfrak{q}})/(\Lambda' \otimes_R R_{\mathfrak{q}}) \cong R/\mathfrak{q}^{n_{\mathfrak{q}}}$ for all $\mathfrak{q}$. The R-module $I\Lambda/\Lambda$ is then Artin and admits a Jordan-Holder composition series where each factor is of the form $R/\mathfrak{q}$ for some maximal ideal $\mathfrak{q}$ of R. Hence there are R-sublattices Λ_i of $I\Lambda$ such that

$$I\Lambda = \Lambda_0 \supset \Lambda_1 \supset \ldots \supset \Lambda_n = \Lambda'$$

where for all i there is a maximal ideal $\mathfrak{q}$ of R for which there is an R-module isomorphism $\Lambda_i/\Lambda_{i+1} \cong R/\mathfrak{q}$; in particular Λ_i and Λ_{i+1} are locally $\mathfrak{q}$-incident and precisely $n_{\mathfrak{q}}$ of the inclusions $\Lambda_j \supset \Lambda_{j+1}$ for all j are locally $\mathfrak{q}$-incident.

We may then select select the points $Q_i \in \mathcal{L}$ corresponding to the lattices Λ_i, for $0 \leq i \leq n$ and where $n = \sum_{\mathfrak{q}} n_{\mathfrak{q}}$, such that we have $[\Lambda] = Q_0$, $[\Lambda'] = Q_n$ and Q_i, Q_{i+1} are locally $\mathfrak{q}$-incident for all i and some $\mathfrak{q}$; we observe that $D([\Lambda],[\Lambda']) = D(Q_0,\ldots,Q_n)$, as required.]

3.11.8. Theorem. *We have*

$$\mathrm{cond}([\Lambda]) = D([\Lambda],[I])$$

where I is a lattice ideal of S for which the distance $D([\Lambda],[I])$ is minimum. The R-lattice class $[I]$ satisfying this equality is uniquely determined up to multiplication by an element of $\mathrm{Pic}(R)$,

Proof. Let $d_{\mathfrak{p}}$ denote the normalised standard metric on the Bruhat-Tits building $\Delta(\mathrm{SL}_2(L))$ with respect to $R_{\mathfrak{p}}$. Let $\mathrm{Exp}(\Lambda \otimes_R R_{\mathfrak{p}})$ denote the local exponent of the conductor of the $R_{\mathfrak{p}}$-lattice $\Lambda \otimes_R R_{\mathfrak{p}}$ in M with respect to the discrete valuation ring $R_{\mathfrak{p}}$.

The ring $S \otimes_R R_\mathfrak{p}$ is the integral closure of $R_\mathfrak{p}$ in M. By theorem 3.7.3, for each maximal ideal $\mathfrak{p}$ of R there is an $R_\mathfrak{p}$-lattice ideal $J_\mathfrak{p}$ of the ring $S \otimes_R R_\mathfrak{p}$ such that we have the equality

$$\mathrm{Exp}(\Lambda \otimes_R R_\mathfrak{p}) = d_\mathfrak{p}([\Lambda \otimes_R R_\mathfrak{p}], [J_\mathfrak{p}])$$

where $[J_\mathfrak{p}]$ denotes the lattice class of $J_\mathfrak{p}$ with respect to $R_\mathfrak{p}$; furthermore, the lattice class $[J_\mathfrak{p}]$ is uniquely determined by $\Lambda \otimes_R R_\mathfrak{p}$.

For all $\mathfrak{p}$ except finitely many, we have $\Lambda \otimes_R R_\mathfrak{p} = S \otimes_R R_\mathfrak{p}$. Hence we have for all $\mathfrak{p}$ except finitely many

$$\mathrm{Exp}(\Lambda \otimes_R R_\mathfrak{p}) = 0.$$

Hence the collection of lattice ideals $J_\mathfrak{p}$ for all $\mathfrak{p}$ satisfies

(a) $J_\mathfrak{p} = S \otimes_R R_\mathfrak{p}$ for all except finitely many $\mathfrak{p}$;

(b) $\mathrm{Exp}(\Lambda \otimes_R R_\mathfrak{p}) = d_\mathfrak{p}([\Lambda \otimes_R R_\mathfrak{p}], [J_\mathfrak{p}])$ for all $\mathfrak{p}$;

(c) $J_\mathfrak{p}$ is uniquely determined by Λ up to multiplication by an element of L^*.

By Proposition 3.3.1, the ring $S \otimes_R R_\mathfrak{p}$ is either the localisation of $R \times R$ or it is a semi-local Dedekind domain obtained by localising the Dedekind domain S. Hence $S \otimes_R R_\mathfrak{p}$ is a finite $R_\mathfrak{p}$-algebra which is a direct product of a finite number of semi-local Dedekind domains. We obtain that $J_\mathfrak{p}$ is a lattice ideal of $S \otimes_R R_\mathfrak{p}$ of the form

$$J_\mathfrak{p} = \big(\prod_i \mathfrak{q}_i^{m_i}\big) S \otimes_R R_\mathfrak{p}$$

where the $\mathfrak{q}_i$ are maximal ideals of S lying over the prime ideal $\mathfrak{p}$ of R and the exponents m_i are non-negative integers.

Let $I_\mathfrak{p}$ be the ideal of S given by

$$I_\mathfrak{p} = \prod_i \mathfrak{q}_i^{m_i}.$$

We have $I_\mathfrak{p} = J_\mathfrak{p} \cap S$. Then $I_\mathfrak{p}$ is a lattice ideal of S which is uniquely determined by $\Lambda \otimes_R R_\mathfrak{p}$ up to multiplication by an element of L^*. We have

$$I_\mathfrak{p}(S \otimes_R R_\mathfrak{p}) = J_\mathfrak{p} \quad \text{for all } \mathfrak{p}$$

and

$$I_\mathfrak{p} = S \quad \text{for all except finitely many } \mathfrak{p}.$$

Put

$$I = \prod_\mathfrak{p} I_\mathfrak{p}$$

where the product is over all maximal ideals $\mathfrak{p}$ of R. Then I is a lattice ideal of S such that

$$I \otimes_R R_{\mathfrak{p}} = I_{\mathfrak{p}} \quad \text{for all } \mathfrak{p}.$$

Furthermore, I is uniquely determined by Λ up to multiplication by a fractionary ideal of R. We obtain for all $\mathfrak{p}$ the equality

$$\text{Exp}(\Lambda \otimes_R R_{\mathfrak{p}}) = d_{\mathfrak{p}}([\Lambda \otimes_R R_{\mathfrak{p}}], [I \otimes_R R_{\mathfrak{p}}]). \tag{3.11.9}$$

By definition of $\text{cond}([\Lambda])$ we have (see (3.9.6))

$$\text{cond}([\Lambda]) = \sum_{\mathfrak{p}} \text{Exp}_{\mathfrak{p}}(\Lambda).\mathfrak{p}.$$

We have from (3.9.7) the equality

$$\text{Exp}_{\mathfrak{p}}(\Lambda) = \text{Exp}(\Lambda \otimes_R R_{\mathfrak{p}})$$

where $\text{Exp}(\Lambda \otimes_R R_{\mathfrak{p}})$ denotes the exponent of the $R_{\mathfrak{p}}$-lattice $\Lambda \otimes_R R_{\mathfrak{p}}$ in M with respect to the discrete valuation ring $R_{\mathfrak{p}}$. We then derive from (3.11.9) the equalities

$$\text{cond}([\Lambda]) = \sum_{\mathfrak{p}} \text{Exp}_{\mathfrak{p}}(\Lambda).\mathfrak{p} = \sum_{\mathfrak{p}} \text{Exp}(\Lambda \otimes_R R_{\mathfrak{p}}).\mathfrak{p}$$

$$= \sum_{\mathfrak{p}} d_{\mathfrak{p}}([\Lambda \otimes_R R_{\mathfrak{p}}], [I \otimes_R R_{\mathfrak{p}}]).\mathfrak{p} = D([\Lambda], [I]),$$

as required. Furthermore, the lattice class $[I]$ of the lattice ideal I is uniquely determined by $[\Lambda]$ up to multiplication by an element of $\text{Pic}(R)$ as already noted. □

4

Heegner sheaves

Heegner sheaves are sheaves of sets or abelian groups for a Grothendieck topology on a geometric or arithmetic curve. In this chapter, we only consider Heegner sheaves arising from complex multiplication of Drinfeld modules of rank 2. Similar Heegner sheaves may be defined on Spec $\mathbb{Z}$ using Heegner points on the classical modular curve $X_0(N)/\mathbb{Z}$.

Drinfeld-Heegner points on the Drinfeld modular curve $\mathbf{X}_0^{\mathrm{Drin}}(I)$ are defined in §§4.1-4.4 and basic properties are proved. The action of the Hecke operators on Drinfeld-Heegner points is considered in §§4.5-4.6 and in particular the analogue for $\mathbf{X}_0^{\mathrm{Drin}}(I)$ of the classical "Eichler-Shimura congruence" for the modular curve $X_0(N)/\mathbb{Z}$ is there proved, except for some details on algebraic stacks. The analogue of the Shimura-Taniyama-Weil conjecture holds for elliptic curves over function fields, a result due to Drinfeld (see §4.7 and Appendix B); its consequences for Drinfeld-Heegner points on elliptic curves are given in §4.8. Finally, basic constructions of Heegner sheaves are considered in §4.9.

4.1 Drinfeld-Heegner points, Heegner morphisms

(4.1.1) The notation of this chapter is that of §2.1 namely:

k is a finite field with $q = p^m$ elements;
C/k is an integral smooth 1-dimensional projective k-scheme, where k is the exact field of constants;
∞ is a closed point of C/k;
C_{aff} is the affine curve $C \setminus \{\infty\}$;
A is the coordinate ring $H^0(C_{\mathrm{aff}}, \mathcal{O}_{C_{\mathrm{aff}}})$ of the affine curve C_{aff};
F is the fraction field of A.

M.L. Brown: LNM 1849, pp. 75–103, 2004.

Throughout this chapter, I is a non-zero ideal of A and $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ is the corresponding Drinfeld moduli scheme (see §2.4). All Drinfeld modules considered are of rank ≤ 2. Let L be an A-field and let $\overline{L}$ be the algebraic closure of L.

(4.1.2) A Drinfeld module D for A defined over $\overline{L}$ is *singular* if its A-algebra of endomorphisms $\mathrm{End}(D)$ strictly contains A. If D is not singular, we say D is *non-singular*.

(4.1.3) Let $x \in \mathbf{Y}_0^{\mathrm{Drin}}(I)(L)$ be an L-valued point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)$. Let $\overline{x}$ be any point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)(\overline{L})$ lying over x. Then $\overline{x}$ is represented by a pair (D, Z) where $D/\overline{L}$ is a Drinfeld module of rank 2 and Z is an I-cyclic subgroup of D (see §2.4); furthermore, (D, Z) is determined up to $\overline{L}$-isomorphism by x. Denote by D/Z the quotient Drinfeld module obtained by factoring out Z.

The point x is a *Drinfeld-Heegner point* if the pair (D, Z) corresponding to $\overline{x}$ is such that both D and D/Z are singular Drinfeld modules and there is an isomorphism of A-algebras

$$\mathrm{End}(D) \cong \mathrm{End}(D/Z).$$

This property of x is independent of the choice of lifting $\overline{x}$ of x.

(4.1.4) A morphism of A-schemes of finite type $f : U \to \mathbf{Y}_0^{\mathrm{Drin}}(I)$ is *Heegner* if every point of the image of f is Drinfeld-Heegner.

4.1.5. Remark. These definitions correspond directly to those of Heegner points of the classical modular curve $\mathbf{X}_0(N)/\mathbb{Z}$ which is the coarse moduli scheme of elliptic curves equipped with a cyclic subgroup of order N.

4.2 Construction of Drinfeld-Heegner points

Lattices

(4.2.1) Let $x \in \mathbf{Y}_0^{\mathrm{Drin}}(I)(L)$ be a point represented by a pair (D, Z) over $\overline{L}$, as in (4.1.3). Suppose that x is a Drinfeld-Heegner point which lies over the generic point of Spec A, in particular $D/\overline{L}$ is a Drinfeld module of general characteristic. Then there is an isomorphism of A-algebras

$$\mathrm{End}(D) \cong \mathrm{End}(D/Z) \cong O_c$$

where O_c is an order, of conductor c, in an imaginary quadratic extension field K of F with respect to ∞.

Let F_∞ be the completion of F with respect to the place ∞ and let $\hat{\overline{F}}_\infty$ be the completion of the algebraic closure of F_∞; fix an embedding $K \to \hat{\overline{F}}_\infty$.

Then the Drinfeld modules D and D/Z are associated to A-lattices Λ, Λ' of rank 2 contained in $\hat{\overline{F}}_\infty$ (see [Dr, §3] or [DH, Chapter 2]); furthermore, Λ, Λ' are locally free O_c-modules of rank 1.

As there is an I-cyclic isogeny $D \to D/Z$ (see §2.4), we may choose the lattices Λ, Λ', in their equivalence classes under multiplication by elements of $\hat{\overline{F}}_\infty$, to be invertible fractionary O_c-ideals such that $\Lambda \subseteq \Lambda'$ and $J = \Lambda\Lambda'^{-1}$ is an integral ideal of O_c for which there is an isomorphism of A-modules

$$O_c/J \cong A/I.$$

(4.2.2) Let O_c be an order in an imaginary quadratic extension field K of F. Assume that J is a proper ideal of O_c which is a locally free O_c-module of rank 1 and such that there is an isomorphism of A-modules $O_c/J \cong A/I$. Fix an embedding $K \to \hat{\overline{F}}_\infty$. Let Λ be a projective O_c-module of rank 1 which is contained as a lattice in $\hat{\overline{F}}_\infty$. Then $\Lambda' = J^{-1}\Lambda$ is a projective O_c-module of rank 1 also contained as a lattice in $\hat{\overline{F}}_\infty$. Let $D/\hat{\overline{F}}_\infty$ and $D'/\hat{\overline{F}}_\infty$ be the rank 2 Drinfeld modules for A, with complex multiplication by O_c, corresponding to the A-lattices Λ and Λ' respectively. Then the inclusion of O_c-modules $\Lambda \subseteq \Lambda'$ corresponds to an I-cyclic isogeny $f : D \to D'$ of Drinfeld modules; hence the pair $(D, \ker(f))$ defines a Drinfeld-Heegner point in $\mathbf{Y}_0^{\mathrm{Drin}}(I)(\hat{\overline{F}}_\infty)$ lying over the generic point of A.

Specialisation and generisation

(4.2.3) Let $F(c, I)$ be the functor defined on the category $A-Sch$ of A-schemes of finite type

$$\begin{array}{rcl} F(c,I) : A-Sch & \to & Sets \\ S & \to & \left\{ \begin{array}{c} \text{pairs } (D, Z) \text{ where } D/S \text{ is a Drinfeld module of} \\ \text{rank 2 and } Z \text{ is an } I-\text{cyclic subgroup such that} \\ \text{there is an injection of } A-\text{algebras } O_c \to \mathrm{End}(D) \end{array} \right\} \end{array}$$

Then $F(c, I)$ has a coarse moduli scheme $Z(c, I)$ which is finite and flat over A. There are A-scheme morphisms

$$Z(c, I) \to \mathbf{Y}_0^{\mathrm{Drin}}(I)$$

obtained by the natural transformations of functors obtained by "forgetting" the complex multiplication by O_c.

(4.2.4) Let $x \in \mathbf{Y}_0^{\mathrm{Drin}}(I)(\overline{L})$ be a point represented by a pair (D, Z) defined over $\overline{L}$, as in (4.1.3); assume that the Drinfeld modules D and D/Z have isomorphic rings of endomorphisms.

Assume that x lies over a closed point of Spec A. Then D and D/Z are Drinfeld modules of finite characteristic and hence are singular Drinfeld modules. The common endomorphism ring $\mathrm{End}(D)$ then contains an order O_c of conductor c of some imaginary quadratic extension field K of F. Hence x is an $\overline{L}$-valued point of the scheme $Z(c, I)$. As $Z(c, I)$ is finite and flat over A, the point x is the specialisation of a generic point η of $Z(c, I)$; that is to say, x is a specialisation of a Drinfeld-Heegner point η lying over the generic point of Spec A, as in (4.2.1).

4.2.5. Remark. Let x be a point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)(L)$ which corresponds to a pair (D, Z) over $\overline{L}$. Then x is *supersingular* if D is a supersingular Drinfeld module that is to say $\mathrm{End}(D)$ is an order in a quaternion algebra over A; in this event, x necessarily lies over a closed point of A and D is supersingular for every pair (D, Z) representing x.

Suppose that x is a point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ lying over the generic point of A. Then the specialisations of x in this moduli scheme may or may not be supersingular. The supersingular specialisation of points of $\mathbf{Y}_0^{\mathrm{Drin}}(A)$ is considered in [Br1] for the special case where $A = \mathbb{F}_q[T]$. [Note the correction to this paper in: B. Poonen, Drinfeld modules with no supersingular primes. Int. Math. Res. Not. 3 (1998), 151-159.]

4.3 Notation for Drinfeld-Heegner points

(4.3.1) Let

K/F be a separable imaginary quadratic extension field of F;
B be the integral closure of A in K;
τ the element of order 2 of the galois group $\mathrm{Gal}(K/F)$;
c be an effective divisor on C_{aff};
O_c denote the order of K relative to A and with conductor c (§2.2 above);
I be a non-zero ideal of A whose prime ideal components split completely in K/F;
$IB = I_1 I_2$ be a factorisation of ideals where I_1, I_2 are ideals of B such that $I_1^\tau = I_2$.

(4.3.2) We put

$$I_j(O_c) = I + I(c)I_j \subset O_c \text{ for } j = 1, 2,$$

where $I(c)$ is the ideal of A cutting out the divisor c. Then $I_j(O_c)$ is an ideal of O_c for all j and one may check that for all j

$$I_j(O_c) = I_j \cap O_c \text{ if } I \text{ and } c \text{ are coprime.}$$

It follows that if c and I are coprime then $I_j(O_c)$ is an invertible ideal of O_c, i.e. it is a locally free O_c-module of rank 1, for $j = 1, 2$; furthermore, if c and

I are coprime we have isomorphisms of A-algebras

$$O_c/I_j(O_c) \cong B/I_j \cong A/I \quad \text{for } j = 1, 2.$$

(4.3.3) Let a be a divisor class in the Picard group $\mathrm{Pic}(O_c)$ of O_c. Assume that c and the ideal I are coprime. We then obtain, a *Drinfeld-Heegner point* (a, I_1, c) *associated to* K *with conductor* c *and class* a where

$$(a, I_1, c) \in \mathbf{Y}_0^{\mathrm{Drin}}(I)(K[c])$$

(cf. [Br2, §2.7]). The point (a, I_1, c) is constructed as follows (see (4.2.2) above):

Fix an embedding $K \to \hat{\overline{F}}_\infty$. We may select Λ to be a projective O_c-module of rank 1 in the class a and contained as a lattice in $\hat{\overline{F}}_\infty$. Then $\Lambda' = I_1(O_c)^{-1}\Lambda$ is a projective O_c-module of rank 1 contained as a lattice in $\hat{\overline{F}}_\infty$. Let D and D' be the rank 2 Drinfeld modules for A over the field $\hat{\overline{F}}_\infty$ corresponding to the lattices Λ and Λ' respectively. Then D, D' have general characteristic and complex multiplication by O_c. The inclusion of O_c-modules $\Lambda \subset \Lambda'$ corresponds to an I-cyclic isogeny $f : D \to D'$, as its kernel is isomorphic as an A-module to $O_c/I_1(O_c) \cong A/I$ (see (4.3.2)). The pair $(D, \ker(f))$ defines a point in $\mathbf{Y}_0^{\mathrm{Drin}}(I)(\hat{\overline{F}}_\infty)$ which is the Drinfeld-Heegner point (a, I_1, c). By the main theorem of complex multiplication, the Drinfeld modules D, D' are defined over the ring class field field $K[c]$ (see §2.3); hence the point (a, I_1, c) lies in $\mathbf{Y}_0^{\mathrm{Drin}}(I)(K[c])$.

4.4 Galois action on Drinfeld-Heegner points

(4.4.1) With the notation (4.3.1) of the previous section, let

J_K be the idèle group of K;
$C_K = J_K/K^*$ be the idèle class group of K.

(4.4.2) Let $c \geq 0$ be an effective divisor on Spec A which is coprime to I. Denote the Artin reciprocity isomorphism for the abelian extension $K[c]/K$ by

$$[-, K[c]/K] : C_K/\big(K^* G_c/K^*\big) \to \mathrm{Gal}(K[c]/K)$$

where, as in (2.3.2), G_c is the open subgroup of J_K given by

$$G_c = K_\infty^* \prod_{v \neq \infty} \hat{O}_{c,v}^*.$$

For any idèle class α of C_K modulo K^*G_c/K^*, the action of the element $[\alpha, K[c]/K]$ on the Drinfeld-Heegner point (a, I_1, c) is given by the main

theorem of complex multiplication of Drinfeld modules, namely the group $C_K/\big(K^*G_c/K^*\big)$ acts in the evident way on the Picard group $\mathrm{Pic}(O_c)$ and we have

$$(a, I_1, c)^{[\alpha, K[c]/K]} = (a\alpha^{-1}, I_1, c). \tag{4.4.3}$$

More specifically, the group $\mathrm{Gal}(K[c]/K)$ is isomorphic to $\mathrm{Pic}(O_c)$ and the element $\theta \in \mathrm{Pic}(O_c)$ acts on (a, I_1, c) via $(a, I_1, c)^\theta = (a\theta^{-1}, I_1, c)$.

4.5 Hecke operators on $\mathbf{X}_0^{\mathbf{Drin}}(I)$ and the Bruhat-Tits net $\Delta_A(\mathbf{SL}_2(F))$

(4.5.1) Let

z be a closed point of C_{aff} with support disjoint from Spec A/I;
$\mathfrak{m}_z$ be the prime ideal of A defining z.

(4.5.2) The *Hecke correspondence* T_z on the Drinfeld modular curve $\mathbf{X}_0^{\mathrm{Drin}}(I)$ may be defined via modular data. That is to say, if L is an algebraically closed field and x is an L-rational point of $\mathbf{X}_0^{\mathrm{Drin}}(I)/A$ given by the pair (D, Z) where Z is an I-cyclic subgroup of the Drinfeld module D, then

$$T_z(x) = \sum_H (D/H, (Z+H)/H)$$

where H runs over all $\mathfrak{m}_z$-cyclic subgroups of D and where the right hand side here is a cycle on $\mathbf{X}_0^{\mathrm{Drin}}(I)$ of degree $|\kappa(z)| + 1$ over the field L.

(4.5.3) In terms of lattices, T_z may be described as follows. Let x be a point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)/A$ lying over the generic point of Spec A. Then x is represented by a pair (D, Z) over $\hat{\overline{F}}_\infty$. Let Λ be a lattice in $\hat{\overline{F}}_\infty$ corresponding to the Drinfeld module $D/\hat{\overline{F}}_\infty$. Let $\Lambda_1 \supseteq \Lambda$ be an over lattice of Λ such that there is an isomorphism of A-modules $\Lambda_1/\Lambda \cong A/I$ and if the Drinfeld module $D_1/\hat{\overline{F}}_\infty$ corresponds to the lattice Λ_1 then the kernel of the isogeny $D \to D_1$ is equal to Z. That is to say, the point x corresponds to the pair of lattices (Λ, Λ_1).

We have, where z is prime to I,

$$T_z x = T_z(\Lambda, \Lambda_1) = \sum_{\Lambda_2} (\Lambda_2, \Lambda_1 + \Lambda_2)$$

where the sum runs over all lattices Λ_2 containing Λ such that there is an isomorphism of A-modules $\Lambda_2/\Lambda \cong A/\mathfrak{m}_z$.

(4.5.4) The Hecke correspondence T_z induces an endomorphism of the jacobian $J(I) = \mathrm{Jac}(X_0^{\mathrm{Drin}}(I))/F[0]$. The Hecke correspondences T_z, for all z prime to

$\mathrm{Supp}(I)$, commute and generate a commutative $\mathbb{Z}$-subalgebra $\mathbf{T}$ of the ring of endomophisms $\mathrm{End}(J(I))$ of the jacobian. The algebra $\mathbf{T}$ is the *Hecke algebra*.

(4.5.5) The non-zero ideal I of the Dedekind domain A is a product of prime ideals. Suppose that the ideal I factorises as

$$I = \mathfrak{p}^n J$$

where $\mathfrak{p}$ is a prime ideal of A and where $J, \mathfrak{p}$ are coprime ideals of A. Let (D, Z) be a pair representing a point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ defined over an algebraically closed field $\overline{L}$.

The *Atkin-Lehner operator* $w_{\mathfrak{p}}$ is defined on $\mathbf{X}_0^{\mathrm{Drin}}(I)$ by

$$w_{\mathfrak{p}}(D, Z) = (D/Z_{\mathfrak{p}^n}, (D_{\mathfrak{p}^n} + Z)/Z_{\mathfrak{p}^n}).$$

Here the subscript $\mathfrak{p}^n$ denotes the subgroup scheme annihilated by $\mathfrak{p}^n$.

The *Fricke operator* w_I is defined on $\mathbf{X}_0^{\mathrm{Drin}}(I)$ by

$$w_I = \prod_{\mathfrak{p}|I} w_{\mathfrak{p}}.$$

If $\mathfrak{p}$ is not principal then the Atkin-Lehner and Fricke operators are not in general involutions, unlike the case of these operators for the rational function fields of [Br2] and for classical modular curves.

(4.5.6) Let $C[0]$ be the smooth projective integral curve over k whose field of fractions is $F[0]$. Let $\mathbf{J}(I)/C[0]$ be the Néron model of the abelian variety $J(I)/F[0]$. Then the Hecke algebra $\mathbf{T}$ induces a ring of endomorphisms of $\mathbf{J}(I)/C[0]$ and hence a ring of endomorphisms of the closed fibre $\mathbf{J}(I)_z/\kappa(z)$ over $z \in C$ of the Néron model.

4.5.7. Theorem. ("Eichler-Shimura congruence".) *Let z be a closed point of C_{aff}. Let θ_z denote the Frobenius automorphism of $\mathbf{J}(I)_z//\kappa(z)$ and θ_z^t the transpose of θ_z. Suppose that the support of I is prime to z. Then the reduction at z of the Hecke operator T_z is given by*

$$T_z \equiv \theta_z + \theta_z^t \pmod{z}.$$

4.5.8. Remark. This result was stated without proof in [Br2] for the rational function field case. This theorem is an analogue of the Eichler-Shimura congruence for classical modular curves. We give a sketch proof of this theorem below; a complete proof will be given in [Br3].

Sketch proof of theorem 4.5.7. The following outline proof is similar in lines to the proof of [DR, Théorème 1.16] which is the Eichler-Shimura congruence for the classical modular curve $Y_0(n)$ of elliptic curves.

(1) *The stack* $\mathcal{Y}_0^{\mathrm{Drin}}(J)/\mathrm{Spec}\ A$.

Let J be a non-zero ideal of A. Let $A-Sch$ be the category of locally noetherian A-schemes. Let $\mathcal{Y}_0^{\mathrm{Drin}}(J)/\mathrm{Spec}\ A$ be the stack (*champ* in French) defined on $A-Sch$ as follows. For any object S of $A-Sch$ then $\mathcal{Y}_0^{\mathrm{Drin}}(J)(S)$ is the category of rank 2 Drinfeld modules for A equipped with a cyclic J-structure over S and the morphisms are S-isomorphisms of Drinfeld modules over S. The stack $\mathcal{Y}_0^{\mathrm{Drin}}(J)$ over Spec A is a category fibred in groupoids over $A-Sch$.

It may be shown that $\mathcal{Y}_0^{\mathrm{Drin}}(J)$ is an *algebraic stack* of finite type over Spec A (see [DM] for the definition and basic properties of algebraic stacks).

From now on let I be a non-zero ideal of A, z be a closed point of C_{aff} disjoint from Spec A/I; let $\mathfrak{p}$ be the prime ideal of A corresponding to z.

(2) *The coarse moduli sceme of the algebraic stack* $\mathcal{Y}_0^{\mathrm{Drin}}(I)/\mathrm{Spec}\ A$

A *coarse moduli scheme* of the algebraic stack $\mathcal{Y}_0^{\mathrm{Drin}}(I)/\mathrm{Spec}\ A$ is a scheme $Y/\mathrm{Spec}\ A$ equipped with a Spec A-morphism

$$\pi : \mathcal{Y}_0^{\mathrm{Drin}}(I) \to Y$$

such that:

(i) Every Spec A-morphism of $\mathcal{Y}_0^{\mathrm{Drin}}(I)$ to a Spec A-scheme X factors through π.

(ii) If $s : \mathrm{Spec}\ \overline{L} \to \mathrm{Spec}\ A$ is a geometric point of Spec A, where $\overline{L}$ is an algebraically closed field, then π induces a bijection between $Y(\overline{L})$ and the set of $\overline{L}$-isomorphism classes of pairs (D, Z) where $D/\overline{L}$ is a Drinfeld module of rank 2 for A and $Z/\overline{L}$ is an $I-$cyclic subgroup of D.

Let $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ denote the coarse moduli scheme associated to the algebraic stack $\mathcal{Y}_0^{\mathrm{Drin}}(I)$. This coarse moduli scheme exists and is a curve over Spec $A[0]$ where $A[0]$ is the integral closure of A in $F[0]$ (see (2.4.7) and [GR, §8.3]). That is to say, $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ is the coarse moduli scheme associated to the functor on the category $A-Sch$ given by

$$A-Sch \to Sets$$

$$S \mapsto \left\{ \begin{array}{c} S-\text{isomorphism classes of pairs } (D,Z) \text{ where } D/S \text{ is a} \\ \text{Drinfeld module of rank 2 and } Z/S \text{ is an} \\ I-\text{cyclic subgroup of } D \end{array} \right\}$$

(3) *Frobenius*

Let $\overline{L}$ be an algebraically closed A-field and let $D/\overline{L}$ be a Drinfeld module for A. Let J be a non-zero ideal of A. Then D_J denotes the finite subgroupscheme of $\mathbb{G}_a$ annihilated by J; that is to say, if $\overline{L}\{\tau\}$ denotes the non-commutative ring of endomorphisms of $\mathbb{G}_a/\overline{L}$ where τ is the Frobenius $x \mapsto x^p$

then $D/\overline{L}$ is given by a homomorphism $\phi : A \to \overline{L}\{\tau\}$ and we have that D_J is the closed subscheme of $\mathbb{G}_a = \mathrm{Spec}\ \overline{L}[x]$ invariant under A given by

$$D_J = \mathrm{Spec}\ \frac{\overline{L}[x]}{< \phi(a)x,\ \text{for all } a \in J >}.$$

Let $\mathfrak{p}$ be the prime ideal of A correponding to the closed point z of C_{aff}. Let L be an A-field where the kernel of $A \to L$ is the prime ideal $\mathfrak{p}$. Let $F : L \to L$ be the Frobenius $x \mapsto x^{|\kappa(\mathfrak{p})|}$. Then a Drinfeld module D/L for A of characteristic $\mathfrak{p}$ induces a Drinfeld-module over L denoted D^F. We obtain an isogeny of Drinfeld modules

$$D \to D^F.$$

The kernel of the isogeny $D \to D^F$ is a finite $\mathfrak{p}$-cyclic sub-groupscheme of the additive group $\mathbb{G}_a$, as this sub-groupscheme is of the form $\mathrm{Spec}\ L[x]/ < x^{|\kappa(\mathfrak{p})|} >$. Hence the pair

$$(D, \ker(D \to D^F))$$

represents a point of $\mathcal{Y}_0^{\mathrm{Drin}}(\mathfrak{p})(L)$.

Let $D_\mathfrak{p}$ be the $\mathfrak{p}$-torsion subgroup of D. Then $D_\mathfrak{p}$ is a sub-groupscheme of D of rank $|A/\mathfrak{p}|^2$. As the kernel of the isogeny $D \to D^F$ is contained in $D_\mathfrak{p}$ we obtain an isogeny of rank $|A/\mathfrak{p}|$

$$V : D^F \to D/D_\mathfrak{p}$$

called the Verschiebung such that $D \to D/D_\mathfrak{p}$ is the composite isogeny VF.

(4) *Supersingular Drinfeld modules*

Let L be an A-field and let $\overline{L}$ be the algebraic closure of L. Let D/L be a Drinfeld module of rank 2 for A. Then D/L is *supersingular* if the ring of endomorphisms $\mathrm{End}(D \times_L \overline{L})$ of the Drinfeld module $D \times_L \overline{L}/\overline{L}$ is non-commutative. In this case, $\mathrm{End}(D \times_L \overline{L})$ is necessarily an order over A of a quaternion algebra over A and D/L has finite characteristic.

Suppose that D/L has finite characteristic $\mathfrak{p}$, where $\mathfrak{p}$ is a maximal ideal of A. That D/L is supersingular is equivalent to the the following condition: if Z is a $\mathfrak{p}$-cyclic subgroup of D then Z is purely local i.e. $Z = \mathrm{Spec}\ L[X]/(X^q)$ where $q = |A/\mathfrak{p}|$ is the order of the residue field at $\mathfrak{p}$.

(5) *The endomorphisms* $y_\mathfrak{p}$

Let J be a non-zero ideal of A. Let L be a field and D/L be a Drinfeld module of rank 2 for A. Then we define a map y_J by $y_J(D) = D/D_J$. Let (D, Z) be a point of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p})(L)$ where Z is the kernel of an $I\mathfrak{p}$-cyclic isogeny $f : D \to D'$ of Drinfeld modules over L. Then we put

$$y_J : (D, \ker(f : D \to D')) \mapsto (D/D_J, \ker(D/D_J \to D'/D'_J)).$$

The map y_J induces a morphism of algebraic stacks

$$y_J : \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \to \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}).$$

If J is a principal ideal of the form aA of A then the map $a : D \to D$ of multiplication by a induces isomorphisms which form a commutative diagram

$$\begin{array}{ccc} & \overset{f}{} & \\ D & \to & D' \\ \downarrow\cong & & \cong\downarrow \\ D/D_J & \to & D'/D'_J \end{array}$$

If J is a principal ideal then y_J is the identity automorphism of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p})$. We have for any ideals J_1, J_2 of A that $y_{J_1} y_{J_2} = y_{J_1 J_2}$ hence the y_J's form a finite abelian group of endomorphisms of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p})$ which is generated by the morphisms $y_{\mathfrak{p}}$ where $\mathfrak{p}$ runs over all maximal ideals of A. This group is isomorphic to $\mathrm{Pic}(A)$.

(6) *Morphisms*

Let S be a locally noetherian A-scheme. Let D/S be a Drinfeld module of rank 2 for A and let Z/S be an $I\mathfrak{p}$-cyclic subgroup of D. The assignment

$$c : (D, Z) \to (D, Z_I)$$

defines a morphism of algebraic stacks

$$c : \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \to \mathcal{Y}_0^{\mathrm{Drin}}(I).$$

The Atkin-Lehner operator $w_{\mathfrak{p}}$ is defined by

$$w_{\mathfrak{p}}(D, Z) = (D/Z_{\mathfrak{p}}, (D_{\mathfrak{p}} + Z)/Z_{\mathfrak{p}}).$$

Then $w_{\mathfrak{p}}$ defines morphism of algebraic stacks

$$w_{\mathfrak{p}} : \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \to \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}).$$

If Z_1 is an I-cyclic subgroup of D and D has characteristic $\mathfrak{p}$ and F is the Frobenius $x \mapsto x^{|A/\mathfrak{p}|}$ relative to $\mathfrak{p}$, then we put

$$f_1(D, Z_1) = (D, \ker(D \to D/Z_1 \to (D/Z_1)^F)).$$

Then f_1 defines a map of algebraic stacks

$$f_1 : \mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p}) \to \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p}).$$

We obtain a diagram

$$\begin{array}{ccccc} \mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p}) & & & & \mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p}) \\ & \searrow^{f_1} & & \swarrow^{f_2 = w_{\mathfrak{p}} f_1} & \\ & & \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p}) & & \\ & \swarrow^{c} & & \searrow^{c w_{\mathfrak{p}}} & \\ \mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p}) & & & & \mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p}) \end{array}$$

The map cf_1 is the identity. The map $cw_{\mathfrak{p}}f_2 = cw_{\mathfrak{p}}w_{\mathfrak{p}}f_1$ is the map $y_{\mathfrak{p}}$. The map $cw_{\mathfrak{p}}f_1 = cf_2$ is the Frobenius automorphism of $\mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p})$ relative to $\kappa(\mathfrak{p})$.

(7) *End of sketch proof*

Let $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p})^h \otimes_A \kappa(\mathfrak{p})$ denote the algebraic stack obtained from $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$ by removing the supersingular Drinfeld modules of characteristic $\mathfrak{p}$. Then one checks that there is an isomorphism of algebraic stacks

$$f_1 \coprod f_2 : \mathcal{Y}_0^{\mathrm{Drin}}(I)^h \otimes_A \kappa(\mathfrak{p}) \coprod \mathcal{Y}_0^{\mathrm{Drin}}(I)^h \otimes_A \kappa(\mathfrak{p}) \to \mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p})^h \otimes_A \kappa(\mathfrak{p}).$$

The morphisms f_1, f_2 are closed immersions because c is a retraction of f_1 and $cw_{\mathfrak{p}}$ is a retraction of f_2 up to automorphism of $\mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p})$. The algebraic stack $\mathcal{Y}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(\mathfrak{p})$ is reducible and its irreducible components correspond to the prime ideals of $A[0]$ over $\mathfrak{p}$. It follows that the image of f_1 and f_2 is the union of all the irreducible components of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$.

The algebraic stack $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$ is reduced because it is Cohen-Macaulay and generically reduced. The supersingular points are in the image of both f_1 and f_2; for if D is a supersingular rank 2 Drinfeld module for A of characteristic $\mathfrak{p}$ over an algebraically closed field, the only subgroup of rank $\mathfrak{p}$ is $\ker(D \to D^F)$. The irreducible components of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$ arising from f_1 and $w_{\mathfrak{p}}f_1$ intersect at these points. The intersection is transversal because the tangent vecteurs at the two branches are linearly independent: one is annihilated by $d(c)$ and not by $d(cw_{\mathfrak{p}})$ and the other by $d(cw_{\mathfrak{p}})$ and not by $d(c)$. Hence we obtain the following results.

(i) The maps f_1, f_2 are closed immersions. Their images are the totality of irreducible components of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$.

(ii) The irreducible components arising from f_1 and f_2 intersect transversally at the supersingular points. The algebraic stack $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$ which is reduced has only ordinary double points for singularities.

(iii) The Frobenius relative to $\kappa(\mathfrak{p})$ exchanges the irreducible components of $\mathcal{Y}_0^{\mathrm{Drin}}(I\mathfrak{p}) \otimes_A \kappa(\mathfrak{p})$ arising from the images of f_1 and f_2.

Theorem 4.5.7 follows from this. □

(4.5.9) Let $\Delta_A(\mathrm{SL}_2(F))$ be the global Bruhat-Tits net with respect to A (see §3.10). Let $\mathcal{L}$ denote the set of vertices of the simplicial complex $\Delta_A(\mathrm{SL}_2(F))$ (i.e. $\mathcal{L}$ is the set of lattice classes). For any $v \in \mathcal{L}$ let

$$\mathrm{st}_z(v) = \{u \in \mathcal{L} \quad | \quad D(u, v) \leq \mathfrak{m}_z\}$$

denote the z-star of v that is to say the set of vertices of $\mathcal{L}$ which are adjacent to v, and distinct from v, and are connected to v by 1-simplices labelled by

$\mathfrak{m}_z$. That is, $\mathrm{st}_z(v)$ is simply the star of v in the $\mathfrak{m}_z$-connected component $C(\mathfrak{m}_z, v)$ of v (see (3.10.9) and (3.7.10)).

4.5.10. Definition. Let $\mathbb{Z}.\mathcal{L}$ be the free abelian group with $\mathcal{L}$ as a set of generators. Define a Hecke operator T_z on $\mathcal{L}$ by

$$\begin{aligned} T_z : \mathcal{L} &\to \mathbb{Z}.\mathcal{L} \\ v &\mapsto \sum_{w \in \mathrm{st}_z(v)} w. \end{aligned}$$

That is, $T_z(v)$ is the formal sum of the vertices of the z-star of v.

4.6 Drinfeld-Heegner points and Hecke operators

In this section, we apply the results on Bruhat-Tits trees with complex multiplication (Chapter 3). We keep the notation (4.3.1) of §4.3.

(4.6.1) We let

$(\Delta_A(\mathrm{SL}_2(F)), \mathrm{cond}, K)$ be the global Bruhat-Tits net with respect to A with complex multiplication by K where cond is the conductor map (see (3.11.3));
$\mathcal{L}$ be the set of A-lattice classes in K (i.e. $\mathcal{L}$ is the set of vertices of $\Delta_A(\mathrm{SL}_2(F))$);
z be a closed point of C_{aff} with support disjoint from Spec A/I;
$\mathfrak{m}_z$ be the prime ideal of A defining z;
T_z be the Hecke correspondence, associated to z, on $\mathbf{X}_0^{\mathrm{Drin}}(I)$ and on $\mathcal{L}$ (see §4.5);
$\overline{F}$ be the algebraic closure of F.

Let I be the ideal of A as in (4.3.1). Denote by $\mathcal{L}_I$ the set of A-lattice classes of K with conductor prime to I; then $\mathcal{L}_I \subseteq \mathcal{L}$. For a maximal ideal $\mathfrak{p}$ of A prime to I, a $\mathfrak{p}$-*flag* of $\mathcal{L}_I$ is a set of pairwise $\mathfrak{p}$-incident distinct elements of $\mathcal{L}_I$ (see also (3.10.7)).

Let $\Delta_{A,I}$ be the flag complex associated to $\mathcal{L}_I$; this is a simplicial complex $\Delta_{A,I}$ with $\mathcal{L}_I$ as a vertex set and the finite $\mathfrak{p}$-flags as simplices for all maximal ideals $\mathfrak{p}$ of A prime to I. Each simplex corresponds to a $\mathfrak{p}$-flag for a unique maximal ideal $\mathfrak{p}$ of A (by (3.10.4)) except for the 0-simplices. Hence each simplex of dimension ≥ 1 is labelled by one maximal ideal of A; each 0-simplex is labelled by all the maximal ideals and we obtain a labelling map $\mathrm{Sim}_1(\Delta_{A,I}) \to \mathrm{Max}(A)$ as in (3.10.7) for Δ_A. Then $\Delta_{A,I}$ is a subcomplex of Δ_A and the labelling map of $\Delta_{A,I}$ is the restriction of the labelling map of Δ_A.

The global Bruhat-Tits net $\Delta_{A,I}(\mathrm{SL}_2(L))$ is the simplicial complex $\Delta_{A,I}$ equipped with the labelling of 1-simplices $\mathrm{Sim}_1(\Delta_{A,I}) \to \mathrm{Max}(A)$.

The conductor map

$$\mathrm{cond} : \mathcal{L}_I \to \mathrm{Div}(A)$$

is defined to be the restriction of the conductor map cond: $\mathcal{L} \to \mathrm{Div}(A)$ of $(\Delta_A(\mathrm{SL}_2(F)), \mathrm{cond}, K)$ to the subset $\mathcal{L}_I$; by definition the conductor of an element of $\mathcal{L}_I$ is a divisor prime to I. We then obtain the subnet $(\Delta_{A,I}(\mathrm{SL}_2(F)), \mathrm{cond}, K)$ with complex multiplication by K corresponding to A-lattices of K with conductor prime to I.

(4.6.2) There are 2 equivalence relations on the A-lattices in K. The first is that defined in (3.10.2) by multiplying lattices by elements of F^*: if Λ is an A-lattice in K we write $[\Lambda]$ for its equivalence class in $\mathcal{L}$, as in §3.10.

The second equivalence relation is given by multiplying A-lattices by elements of K^*: let c be the conductor of the lattice class $v \in \mathcal{L}$; let Λ be an A-lattice in K with $v = [\Lambda]$ then Λ is a locally free O_c-module of rank 1 and hence it determines a class in the Picard group $\mathrm{Pic}(O_c)$ which depends only on v. This class in $\mathrm{Pic}(O_c)$ is denoted $[v]$ which is equal to $[[\Lambda]]$. We thus have surjective maps of sets

$$\begin{array}{ccccc} \left\{ \begin{array}{c} A-\text{lattices in } K \\ \text{with conductor } c \end{array} \right\} & \to & \left\{ \begin{array}{c} \text{elements of } \mathcal{L} \\ \text{with conductor } c \end{array} \right\} & \to & \mathrm{Pic}(O_c) \\ \Lambda & \mapsto & [\Lambda] & \mapsto & [[\Lambda]]. \end{array}$$

(4.6.3) We define a set theoretic map Ψ from the set of vertices $\mathcal{L}_I$ of the global Bruhat-Tits net $\Delta_{A,I}(\mathrm{SL}_2(F))$ to $\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})$

$$\begin{aligned} \Psi : \mathcal{L}_I &\to \mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F}) \\ v &\mapsto ([v], I_1, \mathrm{cond}(v)). \end{aligned}$$

This map takes the equivalence class v of an A-lattice Λ in K, whose conductor is prime to I, to the Drinfeld-Heegner point $([v], I_1, \mathrm{cond}(v))$ composed of the conductor $\mathrm{cond}(v)$ of the lattice Λ, the Picard element $[v]$ of $\mathrm{Pic}(O_{\mathrm{cond}(v)})$ determined by Λ, and the ideal I_1 (see §4.3 and (4.3.3)).

(4.6.4) The map Ψ extends by linearity to a homomorphism of abelian groups, also denoted by Ψ,

$$\Psi : \mathbb{Z}.\mathcal{L}_I \to \mathrm{Div}\big(\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})\big)$$

where $\mathrm{Div}\big(\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})\big)$ is the group of divisors of $\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})$.

4.6.5. Theorem. *Whenever z is coprime to I, the diagram*

$$\begin{array}{ccc} & \overset{T_z}{} & \\ \mathcal{L}_I & \to & \mathbb{Z}.\mathcal{L}_I \\ \Psi \downarrow & & \downarrow \Psi \\ \mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F}) & \underset{T_z}{\to} & \mathrm{Div}\big(\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})\big) \end{array}$$

is commutative i.e. T_z and Ψ commute.

Proof. Let Λ be an A-lattice in K, with conductor c prime to I, which is a locally free O_c-module of rank 1. Let a in $\mathrm{Pic}(O_c)$ be the class $[[\Lambda]]$ of Λ. Let (a, I_1, c) be the Drinfeld-Heegner point with class a and conductor c (see (4.3.3)), that is to say $\Psi[\Lambda] = (a, I_1, c)$.

By the definition of the Hecke operator T_z on $\mathbf{X}_0^{\mathrm{Drin}}(I)$ (see §4.5), we have

$$T_z(a, I_1, c) = \sum_{\Lambda'} ([[\Lambda']], I_1, \mathrm{cond}(\Lambda')) \tag{4.6.6}$$

where the sum runs over the finitely many A-lattices Λ' of K containing Λ such that Λ' is an $\mathfrak{m}_z$-upper modification of Λ (see (3.10.1)) and where $\mathrm{cond}(\Lambda')$ is the conductor of Λ'. Hence we have

$$T_z(\Psi[\Lambda]) = T_z(a, I_1, c) = \sum_{\Lambda'} ([[\Lambda']], I_1, \mathrm{cond}(\Lambda'))$$

$$= \sum_{\Lambda'} \Psi[\Lambda'] = \Psi\big(\sum_{\Lambda'} [\Lambda']\big).$$

By the definition of the Hecke operator T_z on $\mathcal{L}_I$ (see (4.5.10)) this last term $\Psi\big(\sum_{\Lambda'}[\Lambda']\big)$ is equal to, where $\mathrm{st}_z([\Lambda])$ is the z-star of $[\Lambda]$ in $\mathcal{L}_I$ (see (4.5.9)),

$$\Psi\big(\sum_{\Lambda'} [\Lambda']\big) = \Psi\big(\sum_{v \in \mathrm{st}_z([\Lambda])} v\big) = \Psi\big(T_z[\Lambda]\big).$$

Hence we have shown that $T_z(\Psi[\Lambda]) = \Psi\big(T_z[\Lambda]\big)$ as required.□

(4.6.7) Let $a \in \mathrm{Pic}(O_c)$ be a divisor class of O_c. Then we have a transition homomorphism $t_{c+z,z}$, obtained from the inclusion of orders $O_{c+z} \subset O_c$ (see (2.2.12))

$$t_{c+z,c} : \mathrm{Pic}(O_{c+z}) \to \mathrm{Pic}(O_c).$$

Denote by

$a^\sharp \in \mathrm{Pic}(O_{c+z})$ any class such that $t_{c+z,z}(a^\sharp) = a$;
$a^\flat$ the image of $a \in \mathrm{Pic}(O_c)$ under $t_{c,c-z} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c-z})$,
if $z \in \mathrm{Supp}(c)$.

(4.6.8) We define the element $\Delta(a,c,z)$ of $\mathrm{Div}\big(\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})\big)$, where c and z are prime to I, by the equality

$$\Delta(a,c,z) = T_z(a,I_1,c) - \frac{|O_c^*|}{|A^*|}\mathrm{Tr}_{K[c+z]/K[c]}(a^\sharp, I_1, c+z).$$

By the galois action on Drinfeld-Heegner points (see (4.4.3)), $\Delta(a,c,z)$ is independent of the particular choice of class $a^\sharp$ lifting a; for we have

$$\mathrm{Tr}_{K[c+z]/K[c]}(a^\sharp, I_1, c+z) = \sum_{\theta \in \ker(t_{c+z,c})} (a^\sharp\theta^{-1}, I_1, c+z) = \sum_{\eta \in t_{c+z,c}^{-1}(a)} (\eta, I_1, c+z).$$

(4.6.9) We may then tabulate the values of $\Delta(a,c,z)$, where the left column below gives the values of $\Delta(a,c,z)$ under the hypothesis stated in the right column:

(1) 0	if z remains prime in K/F and is prime to c;
(2) $(a[[\mathfrak{m}'_z]]^{-1}, I_1, c)$	if z is ramified in K/F and is prime to c where $\mathfrak{m}'_z$ is the prime ideal of O_c lying above the ideal $\mathfrak{m}_z$ of A defining z;
(3) $(a[[\mathfrak{p}_1]]^{-1}, I_1, c) + (a[[\mathfrak{p}_2]]^{-1}, I_1, c)$	if z is split completely in K/F and is prime to c where $\mathfrak{m}_z O_c = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct prime ideals of O_c;
(4) $(a^\flat, I_1, c-z)$	if $z \in \mathrm{Supp}(c)$.

Table 4.6.9: values of $\Delta(a,c,z)$

Proof of the table 4.6.9. Let $v \in \mathcal{L}_I$ and let $(a, I_1, c) = \Psi(v) \in \mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})$ be the corresponding Drinfeld-Heegner point given by a pair (D, Z), as in (4.1.3).

Let $\mathrm{st}_z(v)$ be the z-star of $v \in \mathcal{L}_I$ (see (4.5.9)). Let $w \in \mathrm{st}_z(v)$. According to theorem 4.6.5 and theorem 3.11.8, the conductor of w is one of the three possibilities $c+z, c, c-z$. Let $\mathcal{S}(z+nc)$ be the subset of $\mathrm{st}_z(v)$ of elements of conductor $z+nc$ where $-1 \leq n \leq 1$.

The group O_c^*, as a subgroup of K^*, permutes the A-lattices in K and acts as a group of automorphisms of the global Bruhat-Tits net $\Delta_{A,I}(\mathrm{SL}_2(F))$. Hence the quotient group O_c^*/A^* acts as a group of automorphisms of $\mathcal{L}_I$ which preserves adjacency. This group O_c^*/A^* fixes the point v and permutes the elements of $\mathrm{st}_z(v)$. Furthermore, if $\alpha \in O_c^*/A^*$ then we have

$$\Psi(w^\alpha) = \Psi(w), \quad \text{for all } w \in \mathrm{st}_z(v) \text{ and all } \alpha, \tag{4.6.10}$$

as O_c^* induces automorphisms of the underlying Drinfeld modules. Let

$$u = \frac{|O_c^*|}{|A^*|}.$$

As the point $(a, I_1, c) = \Psi(v)$ is defined over $K[c]$ and all the Drinfeld-Heegner points in $\Psi(\mathrm{st}_z(v))$ are definable over the field $K[c+z]$, the galois group

$$G = \mathrm{Gal}(K[c+z]/K[c])$$

acts by permutation on the set of points $\Psi(\mathrm{st}_z(v))$ which is a subset of $\mathbf{X}_0^{\mathrm{Drin}}(I)(K[c+z])$. The group G preserves the conductor of a Drinfeld-Heegner point hence the subsets $\Psi(\mathcal{S}(z+nc))$, $n \in \mathbb{Z}$, are unions of orbits of G on $\Psi(\mathrm{st}_z(v))$.

Let $t_{c+z,c}^{-1}(a)$ be the fibre of the map $t_{c+z,c} : \mathrm{Pic}(O_{c+z}) \to \mathrm{Pic}(O_c)$ over $a \in \mathrm{Pic}(O_c)$ (see (2.2.12)). We have

$$\Psi(\mathcal{S}(c+z)) = \{(b, I_1, c+z) |\ b \in t_{c+z,c}^{-1}(a)\}.$$

For two distinct elements $b_1, b_2 \in t_{c+z,c}^{-1}(a)$, the points $(b_i, I_1, c+z)$, $i = 1, 2$, are distinct on $\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})$ as the I-cyclic isogenies $D \to D_{b_i}$ of Drinfeld modules corresponding to $(b_i, I_1, c+z)$ are not isomorphic over $\bar{F}$ as the lattices Λ_{b_i} in $\hat{\bar{F}}_\infty$, for $i = 1, 2$, corresponding to the Drinfeld modules D_{b_i} have distinct Picard classes $b_1 \neq b_2$. In particular, we have

$$|\Psi(\mathcal{S}(c+z))| = |t_{c+z,c}^{-1}(a)|.$$

The Drinfeld-Heegner points $(b, I_1, c+z)$, where b runs through the elements of $t_{c+z,c}^{-1}(a)$, are permuted transitively by G by the known galois action on Drinfeld-Heegner points (see §4.4 and (2.2.14)). The reciprocity isomorphism becomes $G \cong \ker(t_{c+z,z})$; hence, we have an equality of cardinalities

$$|\Psi(\mathcal{S}(c+z))| = |G|.$$

It follows that, G permutes transitively and faithfully the elements of the set $\Psi(\mathcal{S}(c+z))$; in particular, $\Psi(\mathcal{S}(c+z))$ forms a single orbit under the action of G.

Let $a^\sharp$ in $\mathrm{Pic}(O_{c+z})$ be any element of $t_{c+z,c}^{-1}(a)$. We obtain

$$\sum_{w\in\mathcal{S}(c+z)} \Psi(w) = \sum_{\sigma\in G} n_\sigma (a^\sharp, I_1, c+z)^\sigma. \tag{4.6.11}$$

for some integers n_σ such that (by (4.6.10))

$$n_\sigma \geq u \text{ for all } \sigma \in G \tag{4.6.12}$$

and

$$\sum_{\sigma\in G} n_\sigma = |\mathcal{S}(c+z)|. \tag{4.6.13}$$

The different possibilities for the sets $\mathcal{S}(c+nz)$ are prescribed by the classification of Bruhat-Tits trees with complex multiplication (figures 1,2,3,4 of §3.8). The set $\mathcal{S}(c)$ consists of at most two elements and $\mathcal{S}(c-z)$ has at most one element. More precisely (see §3.8) as the cardinality of $\mathrm{st}_z(v)$ is equal to $|\kappa(z)|+1$, we have

$$|\mathcal{S}(c+z)| = \begin{cases} |\kappa(z)|+1, & \text{if } z\notin \mathrm{Supp}(c) \text{ and } z \text{ is inert in } K/F; \\ |\kappa(z)|-1, & \text{if } z\notin \mathrm{Supp}(c) \text{ and } z \text{ is split in } K/F; \\ |\kappa(z)|, & \text{if } z \text{ is ramified in } K/F \text{ or if } z\in \mathrm{Supp}(c)\ . \end{cases}$$

We then obtain, by the results on ring class fields of §2.3 (see (2.3.11) and (2.3.12)), the equality of orders

$$u.|G| = |\mathcal{S}(c+z)|.$$

Hence by (4.6.12) and (4.6.13) we have $n_\sigma \geq u$ for all $\sigma \in G$ and

$$\sum_{\sigma\in G} n_\sigma = u.|G|.$$

The only possibility here is that

$$n_\sigma = u \ \text{ for all } \sigma.$$

We then obtain from (4.6.11)

$$\sum_{w\in\mathcal{S}(c+z)} \Psi(w) = u \sum_{\sigma\in G} (a^\sharp, I_1, c)^\sigma.$$

By theorem 4.6.5, we may then write the action of the Hecke operator T_z as

$$T_z(a, I_1, c) = \Psi(T_z(v)) = \Psi(\sum_{w \in \mathrm{st}_z(v)} w) = \Big(\sum_{w \in \mathcal{S}(c+z)} + \sum_{w \in \mathcal{S}(c)} + \sum_{w \in \mathcal{S}(c-z)}\Big)\Psi(w)$$

$$= u \sum_{\sigma \in G} (a^\sharp, I_1, c+z)^\sigma + \sum_{w \in \mathcal{S}(c)} \Psi(w) + \sum_{w \in \mathcal{S}(c-z)} \Psi(w). \tag{4.6.14}$$

We then obtain from this equation, where $\Delta(a, c, z)$ is defined in the equation (4.6.8),

$$\Delta(a, c, z) = \sum_{w \in \mathcal{S}(c)} \Psi(w) + \sum_{w \in \mathcal{S}(c-z)} \Psi(w). \tag{4.6.15}$$

Now the form of $\Delta(a, c, z)$ can be obtained from the corresponding Bruhat-Tits building with complex multiplication. In detail we have, following the 4 cases in the table (4.6.9):

(1) if z is inert in K/F and is prime to $\mathrm{Supp}(c)$ then (fig. 1, §3.8) the sets $\mathcal{S}(c)$ and $\mathcal{S}(c-z)$ are both empty whence we have

$$\Delta(a, c, z) = 0;$$

(2) if z is ramified in K/F and is prime to c then (fig. 3, §3.8) $\mathcal{S}(c)$ has exactly one element corresponding to the class $a[[\mathfrak{m}'_z]]^{-1} \in \mathrm{Pic}(O_c)$, where $\mathfrak{m}'_z$ is the prime ideal of O_c lying above $\mathfrak{m}_z$, and $\mathcal{S}(c-z)$ is empty; hence we have

$$\Delta(a, c, z) = (a[[\mathfrak{m}'_z]]^{-1}, I_1, c);$$

(3) if z is split completely in K/F and is prime to c then (fig. 2, §3.8) $\mathcal{S}(c)$ has exactly two elements corresponding to the classes $a[[\mathfrak{p}_1]]^{-1}, a[[\mathfrak{p}_2]]^{-1} \in \mathrm{Pic}(O_c)$, where $\mathfrak{m}_z O_c = \mathfrak{p}_1\mathfrak{p}_2$ is the factorisation of $\mathfrak{m}_z O_c$ into prime ideals of O_c, and $\mathcal{S}(c-z)$ is empty; hence we have

$$\Delta(a, c, z) = (a[[\mathfrak{p}_1]]^{-1}, I_1, c) + (a[[\mathfrak{p}_2]]^{-1}, I_1, c);$$

(4) if $z \in \mathrm{Supp}(c)$ then (figs. 1, 2, and 3, §3.8) $\mathcal{S}(c)$ is empty and $\mathcal{S}(c-z)$ has precisely one element corresponding to the class $a^\flat \in \mathrm{Pic}(O_{c-z})$; hence we have

$$\Delta(a, c, z) = (a^\flat, I_1, c-z). \qquad \square$$

4.6.16. Remark. This table and the table 4.8.5 below generalise theorems 2.9.5; and 2.10.3 of [Br2] even for the case of rational function fields. These

prior results only considered, amongst other restrictions, the Drinfeld-Heegner points $(1, I_1, c)$ associated to the principal divisor class 1 of $\mathrm{Pic}(O_c)$.

4.6.17. Theorem. *Let $c \in \mathrm{Div}_+(A)$ be a divisor prime to I and let $a \in \mathrm{Pic}(O_c)$. For some $\sigma \in \mathrm{Gal}(K[c]/K)$ we have, where w_I is the Fricke operator and τ is the non-trivial element of $\mathrm{Gal}(K_\infty/F_\infty)$,*

$$w_I(a, I_1, c) = (a, I_1, c)^{\tau\sigma}.$$

Proof. Let (D, Z) be a pair defined over $\hat{\overline{F}}_\infty$ representing the Drinfeld-Heegner point (a, I_1, c), where Z is an I-cyclic subgroup of the Drinfeld module D. On the one hand, we have from the definition of w_I (see (4.5.5))

$$w_I(a, I_1, c) = (D/Z_I, (D_I + Z)/Z_I).$$

As Z is itself an I-cyclic subgroup we have $Z_I = Z \subset D_I$ and hence this gives, where $I_1(O_c), I_2(O_c)$ are the ideals of O_c defined in (4.3.2),

$$w_I(a, I_1, c) = (D/Z, D_I/Z) = (a[[I_1(O_c)^{-1}]], I_2, c)$$

where $I_1(O_c)^{-1}$ is the fractionary ideal of O_c which is the inverse of $I_1(O_c)$.

We obtain that

$$w_I^2(a, I_1, c) = (a[[I_1(O_c)^{-1} I_2(O_c)^{-1}]], I_1, c).$$

The ideal class $[[I_1(O_c)I_2(O_c)]]^{-1} \in \mathrm{Pic}(O_c)$ lies in the image of the map $\mathrm{Pic}(A) \to \mathrm{Pic}(O_c)$ obtained from the inclusion $A \to O_c$. In particular, w_I^2 acts as the identity on the Drinfeld-Heegner point (a, I_1, c) if and only if $I_1(O_c)I_2(O_c)$ is a principal ideal of O_c.

On the other hand, the Galois action on Drinfeld-Heegner points (see §4.4) gives that

$$(a, I_1, c)^{[\alpha, K[c]/K]} = (a\alpha^{-1}, I_1, c) \tag{4.6.18}$$

where $[\alpha, K[c]/K] \in \mathrm{Gal}(K[c]/K)$ denotes the image of the idèle α under the reciprocity map. Let τ be the non-trivial element of $\mathrm{Gal}(K_\infty/F_\infty)$. Let Λ be the rank 2 A-lattice contained in K_∞ associated to the Drinfeld module D. As τ is a continuous automorphism for the ∞-adic topology, the lattice associated to the Drinfeld module D^τ is Λ^τ. The two ideals of O_c given by $I_i(O_c)$, $i = 1, 2$, (see (4.4.3)) are conjugates under the action of τ; that is to say we have $I_1(O_c) = I_2(O_c)^\tau$. It follows that we have

$$(a, I_1, c)^\tau = (D^\tau, Z^\tau) = (a^\tau, I_2, c).$$

Therefore by (4.6.18), there is an element $\sigma = [\alpha, K[c]/K] \in \mathrm{Gal}(K[c]/K)$ such that

$$(a, I_1, c)^{\tau\sigma} = (a^\tau, I_2, c)^\sigma = (a[[I_1(O_c)^{-1}]], I_2, c) = w_I(a, I_1, c). \quad \square$$

4.6.19. Theorem. *Let $c, z \in \mathrm{Div}_+(A)$ be divisors where z is a prime divisor such that $z \notin \mathrm{Supp}(c)$. Assume that z and c are both prime to $\mathrm{Supp}(I)$. Let Z be a place of $K[c+z]$ lying over z. Let $a^\sharp \in \mathrm{Pic}(O_{c+z})$ be any class lifting $a \in \mathrm{Pic}(O_c)$. Then we have:*
(i) *the reductions modulo Z of the points $(a^\sharp, I_1, c+z)$ and (a, I_1, c) in $\mathbf{X}_0^{\mathrm{Drin}}(I)(\kappa(Z))$ satisfy*

$$\mathrm{Frob}_z(a^\sharp, I_1, c+z) \equiv (a, I_1, c) \pmod{Z}$$

where Frob_z denotes the Frobenius automorphism relative to z of $\mathbf{X}_0^{\mathrm{Drin}}(I) \otimes_A \kappa(z)$ (i.e. Frob_z is given on coordinates by $x \mapsto x^{|\kappa(z)|}$);
(ii) *if z is inert and unramified in K/F then the point $(a, I_1, c) \pmod{Z}$ is defined over the quadratic extension field of $\kappa(z)$.*

Proof. The results on ring class fields given in §2.3 show that the places of K lying over z are unramified in the extension $K[c]/K$ and the places of $K[c]$ lying above z are all totally ramified in the extension $K[c+z]/K[c]$.

As in (4.6.8) let $\Delta(a, c, z)$ be the element of $\mathrm{Div}\big(\mathbf{X}_0^{\mathrm{Drin}}(I)(\bar{F})\big)$ given by the equality

$$\Delta(a, c, z) = T_z(a, I_1, c) - \frac{|O_c^*|}{|A^*|}\mathrm{Tr}_{K[c+z]/K[c]}(a^\sharp, I_1, c+z).$$

From the table 4.6.9, the divisor $\Delta(a, c, z)$ has at most two prime components, depending on the splitting of z in K/F. Hence the prime divisor components of the divisor $T_z(a, I_1, c)$, of which there are $|\kappa(z)| + 1$ in number, are the galois conjugates over $\mathrm{Gal}(K[c+z]/K[c])$ of $(a^\sharp, I_1, c+z)$ except possibly for at most two components; as the factors of z are totally ramified in $K[c+z]/K[c]$ we obtain that the prime components of $T_z(a, I_1, c)$ are all congruent to $(a^\sharp, I_1, c+z)$ modulo Z with at most two exceptional components.

We now consider three cases, corresponding to cases (1), (2), and (3) of table 4.6.9, depending on the splitting of the prime z in the field extension K/F.

(1) Suppose that z remains prime in K/F and is prime to c. Then we have $\Delta(a, c, z) = 0$; hence the prime components of $T_z(a, I_1, c)$ are all congruent to $(a^\sharp, I_1, c+z)$ modulo Z. The Eichler-Shimura congruence (theorem 4.5.7) shows that there are points x, y in the divisor $T_z(a, I_1, c)$ which satisfy

$$x \equiv \mathrm{Frob}_z(a, I_1, c) \text{ modulo } Z \text{ and } \mathrm{Frob}_z(y) \equiv (a, I_1, c) \text{ modulo } Z.$$

It follows that all the prime components x of $T_z(a, I_1, c)$ satisfy $\mathrm{Frob}_z(x) \equiv (a, I_1, c)$ modulo Z and that the reduction modulo Z of the point (a, I_1, c) is defined over a quadratic extension field of $\kappa(z)$. This proves both (i) and (ii) if z remains prime in K/F.

(2) Suppose that z is ramified in K/F and is prime to c. Let $z^\sharp$ be the unique prime of K lying over z. Let $\mathfrak{m}_z$ be the unique prime ideal of B lying above the point z of A. Let $\mathfrak{m}'_z = O_c \cap \mathfrak{m}_z$ be the unique prime ideal of O_c lying above z. By the table 4.6.9 we have

$$\Delta(a, c, z) = (a[[\mathfrak{m}'_z]]^{-1}, I_1, c).$$

The action of Galois on Drinfeld-Heegner points (§4.4) shows that

$$(a[[\mathfrak{m}'_z]]^{-1}, I_1, c) = \mathrm{Frob}_{z^\sharp}(a, I_1, c).$$

where $\mathrm{Frob}_{z^\sharp}$ is the Frobenius element of the galois group $\mathrm{Gal}(K[c]/K)$ above $z^\sharp$. Hence we have, as the residue field at $z^\sharp$ is isomorphic to the residue field at z,

$$(a[[\mathfrak{m}'_z]]^{-1}, I_1, c) \equiv \mathrm{Frob}_z(a, I_1, c) \text{ (modulo } Z).$$

As all the other $|\kappa(z)|$ components of $T_z(a, I_1, c)$ are of the form $(b, I_1, c + z)$ where $t_{c+z,c}(b) = a$, these components are congruent to each other modulo Z; the Eichler-Shimura congruence (theorem 4.5.7) shows that all prime components x of $T_z(a, I_1, c)$ of this form $(a^\sharp, I_1, c + z)$ satisfy $\mathrm{Frob}_z(x) \equiv (a, I_1, c)$ modulo Z.

(3) Suppose that z is split completely in K/F and is prime to c. Then we have $\mathfrak{m}_z O_c = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct prime ideals of O_c. We have from table 4.6.9

$$\Delta(a, c, z) = (a[[\mathfrak{p}_1]]^{-1}, I_1, c) + (a[[\mathfrak{p}_2]]^{-1}, I_1, c).$$

The action of Galois on Drinfeld-Heegner points (§4.4) shows that

$$(a[[\mathfrak{p}_i]]^{-1}, I_1, c) = \mathrm{Frob}_{\mathfrak{p}_i}(a, I_1, c) \text{ for } i = 1, 2.$$

where $\mathrm{Frob}_{\mathfrak{p}_i} \in \mathrm{Gal}(K[c]/K)$ is a Frobenius element above $\mathfrak{p}_i$ for $i = 1, 2$. The place Z lies over precisely one of the primes $\mathfrak{p}_1, \mathfrak{p}_2$; we may assume that it is the place $\mathfrak{p}_1$. The point $(a[[\mathfrak{p}_1]]^{-1}, I_1, c)$ then satisfies

$$(a[[\mathfrak{p}_1]]^{-1}, I_1, c) \equiv \mathrm{Frob}_z(a, I_1, c) \pmod{Z}.$$

The Eichler-Shimura congruence (theorem 4.5.7) now shows that at least one point in the divisor $T_z(a, I_1, c)$ is congruent to $\mathrm{Frob}_z(a, I_1, c)$ modulo z and that all other components x of $T_z(a, I_1, c)$ are congruent to each other and satisfy $\mathrm{Frob}_z(x) \equiv (a, I_1, c)$ modulo Z. In conclusion, we have that all the prime components x of $T_z(a, I_1, c)$ of this form $(a^\sharp, I_1, c+z)$ satisfy $\mathrm{Frob}_z(x) \equiv (a, I_1, c)$ modulo Z. □

4.6.20. Remarks. (i) Supose that z is a prime divisor of $\mathrm{Div}_+(A)$ which remains inert in K/F. Then the Drinfeld modules corresponding to (a, I_1, c) have complex multiplication by K; hence they have supersingular reduction at z. Therefore the reduction at z of these Drinfeld modules are defined over a quadratic extension field of $\kappa(z)$. This gives another proof of part (ii) of the previous theorem 4.6.19.

(ii) This theorem 4.6.19 generalises [Br2, Theorem 2.9.5(iii)] where the case z is inert in K/F is considered for the rational function field case. The result there is stated differently as

$$(a^\sharp, I_1, c + z) \equiv \ \mathrm{Frob}_z(a, I_1, c) \ (\mathrm{mod}\ Z).$$

This is equivalent to the statement in the theorem above; for in the case where z is inert the Drinfeld modules corresponding to the point (a, I_1, c) have supersingular reduction at z and therefore these reductions are defined over a quadratic field extension of $\kappa(z)$.

4.7 Elliptic curves and Drinfeld modular curves

Let F_∞ denote the completion of F with respect to the place ∞. Let E/F be an elliptic curve such that $E \times_F F_\infty/F_\infty$ is a Tate curve; that is to say, E has split multiplicative reduction at ∞. This is equivalent to the closed fibre above ∞ of a ∞-minimal model of E/F being a nodal cubic where the tangents at the node are rational over the residue field $\kappa(\infty)$.

Let I be a non-zero ideal of the ring A. We write $X_0^{\mathrm{Drin}}(I)/F$ for the generic fibre of the moduli scheme $\mathbf{X}_0^{\mathrm{Drin}}(I)$ (see §2.4). The Drinfeld modular curve $X_0^{\mathrm{Drin}}(I)/F$ has exact field of constants equal to the Hilbert class field $F[0]$ of F that is to say, the maximal unramified abelian extension of F which is split completely at ∞.

Let E/F be an elliptic curve. Then a *Weil parametrisation* of E is a finite surjective morphism of F-schemes

$$\pi : X_0^{\mathrm{Drin}}(I) \to E.$$

4.7.1. Theorem. (Drinfeld). *Let E/F be an elliptic curve such that $E \times_F F_\infty/F_\infty$ is a Tate curve. Let I, which is an ideal of A, be the conductor of E/F without the component at ∞. Then there is a Weil parametrisation*

$$\pi : X_0^{\mathrm{Drin}}(I) \to E. \quad \square$$

4.7.2. Remark. A brief proof of this for the case of the rational function field $F = \mathbb{F}_q[T]$ is given in [Br2, Theorem 4.1]. A proof for Tate elliptic curves over

arbitrary global fields of positive characteristic has been given by Gekeler and Reversat [GR]. Both proofs are heavily dependent on the work of Drinfeld; nevertheless, they are not identical. The difference lies in the manner that the splitting of an elliptic curve from the jacobian of the modular curve $X_0^{\mathrm{Drin}}(I)$ is obtained. Gekeler and Reversat use Hecke operators for this whereas in [Br2] this is splitting is obtained by a theorem of Zarhin namely the so-called "the isogeny conjecture" for abelian varieties over function fields.

[This theorem 4.7.1 is given a complete proof in Appendix B; for some examples of Weil parametrisations, see §B.11.]

4.8 Drinfeld-Heegner points and elliptic curves

We keep the notation (4.3.1) of §4.3.

(4.8.1) Let E/F be an elliptic curve equipped with an origin, that is to say a 1-dimensional abelian variety. We assume that $E \times_F F_\infty/F_\infty$ is a Tate curve, where F_∞ is the completion of F at ∞. Hence E/F admits a Weil parametrisation where I is the conductor of E/F without the component at ∞ (see §4.7 and theorem 4.7.1)

$$\pi : X_0^{\mathrm{Drin}}(I) \to E$$

that is to say, π is a finite surjective morphism of F-schemes where $X_0^{\mathrm{Drin}}(I)/F$ is the generic fibre of the modular surface $\mathbf{X}_0^{\mathrm{Drin}}(I)/A$. We may translate π in the group scheme E so that $\pi^{-1}(0)$ consists of at least one cusp of $X_0^{\mathrm{Drin}}(I)$.

(4.8.2) For any effective divisor c on C_{aff}, with support prime to Supp I, let (a, I_1, c) be the Drinfeld-Heegner point in $X_0^{\mathrm{Drin}}(I)(K[c])$ defined in (4.3.3); the point

$$\pi(a, I_1, c) \in E(K[c]),$$

written (a, I_1, c, π), is a $K[c]$-rational point of the elliptic curve E which we call a *Drinfeld-Heegner point of the elliptic curve* E.

(4.8.3) Let l be any prime number distinct from the characteristic of F. Let $T_l(E)$ be the l-adic Tate module of E, that is to say $T_l(E)$ is the dual of $H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l)$ where F^{sep} denotes the separable closure of F. For z a closed point of Spec A which is prime to Supp(I), we put

$$a_z = \mathrm{Tr}(\mathrm{Frob}_z | T_l(E))$$

which is the trace of a Frobenius element $\mathrm{Frob}_z \in \mathrm{Gal}(F^{\mathrm{sep}}/F)$ at z acting on the Tate module $T_l(E)$. We have that a_z is an integer in $\mathbb{Z}$. Put

$$\Delta(a, c, z, \pi) = a_z(a, I_1, c, \pi) - \frac{|O_c^*|}{|A^*|} \mathrm{Tr}_{K[z+c]/K[c]}(a^\sharp, I_1, c + z, \pi)$$

where $a^\sharp$ is any element of $\mathrm{Pic}(O_{c+z})$ lifting a under $t_{c+z,c}$.

(4.8.4) Suppose that z is a closed point of C_{aff}. Assume that z and $c \in \mathrm{Div}_+(A)$ are coprime to $\mathrm{Supp}(I)$. We may then tabulate the values of $\Delta(a, c, z, \pi)$, where the notation is exactly that of the table 4.6.9:

(1) 0	if z remains prime in K/F and is prime to c;
(2) $(a[[\mathfrak{m}'_z]]^{-1}, I_1, c, \pi)$	if z is ramified in K/F and is prime to c where $\mathfrak{m}'_z$ is the prime ideal of O_c lying above the ideal $\mathfrak{m}_z$ of A defining z;
(3) $(a[[\mathfrak{p}_1]]^{-1}, I_1, c, \pi) + (a[[\mathfrak{p}_2]]^{-1}, I_1, c, \pi)$	if z is split completely in K/F and is prime to c where $\mathfrak{m}_z O_c = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct prime ideals of O_c;
(4) $(a^\flat, I_1, c - z, \pi)$	if $z \in \mathrm{Supp}(c)$, where $a^\flat = t_{c,c-z}(a)$.

Table 4.8.5: values of $\Delta(a, c, z, \pi)$

Proof of table 4.8.5. This follows immediately from the table 4.6.9 using the Eichler-Shimura congruence theorem 4.5.7; namely, we have

$$T_z(a, I_1, c, \pi) = a_z(a, I_1, c, \pi)$$

where a_z is the trace of the Frobenius at z on $T_l(E)$. □

4.8.6. Theorem. *Let τ be the non-identity element of the group $\mathrm{Gal}(K_\infty/F_\infty)$ and ϵ be the sign in the functional equation of the L-function of E. Let $\overline{F}$ be the algebraic closure of F. For some $\sigma \in \mathrm{Gal}(K[c]/K)$ we have*

$$(a, I_1, c, \pi)^\tau + \epsilon(a, I_1, c, \pi)^\sigma \in E(\overline{F})_{\mathrm{tors}}.$$

Proof. Let s be a cusp of $X_0^{\mathrm{Drin}}(I)$ for which $\pi(s) = 0$. We have from theorem 4.6.17, that for some element σ in the galois group $\mathrm{Gal}(K[c]/K)$

$$((a, I_1, c) - s)^{\tau\sigma} = w_I\big[(a, I_1, c) - s\big] + (w_I(s) - s^{\tau\sigma}). \tag{4.8.7}$$

The points $w_I(s)$ and $s^{\tau\sigma}$ are also cusps of $X_0^{\mathrm{Drin}}(I)$; by applying π to the preceding equation (4.8.7) we obtain

$$(a, I_1, c, \pi)^{\tau\sigma} = -\epsilon(a, I_1, c, \pi) + \pi(w_I(s) - s^{\tau\sigma}) \tag{4.8.8}$$

as $\pi(s) = 0$ and as w_I acts on E as $-\epsilon$, where $\epsilon = \pm 1$ is the sign in the functional equation of E. The class of the divisor $w_I(s) - s^{\tau\sigma}$ is torsion in the jacobian $J(I)$ by theorem 2.4.9; hence $\pi(w_I(s) - s^{\tau\sigma})$ is a torsion element of the abelian group $E(\bar{F})$, as required. □

4.8.9. Theorem. *Let $c, z \in \mathrm{Div}_+(A)$ be divisors where z is a prime divisor such that $z \notin \mathrm{Supp}(c)$. Assume that z and c are both prime to $\mathrm{Supp}(I)$. Let Z be a place of $K[c+z]$ lying over z. Let $a^\sharp \in \mathrm{Pic}(O_{c+z})$ be any class lifting $a \in \mathrm{Pic}(O_c)$. In the group $E_z(\kappa(Z))$, where E_z denotes the reduction modulo z of the Néron model of E, we then have the relation*

$$\mathrm{Frob}_z(a^\sharp, I_1, c + z, \pi) \equiv (a, I_1, c, \pi) \text{ (modulo } Z)$$

Proof. This is an immediate consequence of theorem 4.6.19(i). □

4.9 Heegner sheaves

(4.9.1) We shall in this section only consider Heegner sheaves arising from Drinfeld-Heegner points. But Heegner sheaves may be constructed similarly on Spec $\mathbb{Z}$ using Heegner points on the modular curves $\mathbf{X}_0(N)/\mathbb{Z}$ classifying elliptic curves equipped with a cyclic subgroup of order N.

An example of a Heegner sheaf is given by the "singular moduli" of elliptic curves. Let $X_0(1)/\mathbb{Q}$ be the modular curve classifying elliptic curves i.e. $X_0(1)$ is the "j-line" Spec $\mathbb{Q}[j]$ of the modular j-invariant of elliptic curves. For any field extension $k/\mathbb{Q}$ let $\mathcal{H}(k)$ denote the subset of k-rational points of $X_0(1)$ which correspond to elliptic curves with complex multiplication, that is to say $\mathcal{H}(k)$ is the set of singular moduli which are rational over k; then $\mathcal{H}(k)$ is the set of sections over k of a sheaf of sets $\mathcal{H}$ for the étale topology on Spec $\mathbb{Q}$. This sheaf $\mathcal{H}$ is a *Heegner sheaf.*

(4.9.2) We use the terminology of Milne [M2] for the étale and flat Grothendieck topologies on a scheme. For a scheme X then

$X_{\text{ét}}$ denotes the small étale site on X; i.e. $X_{\text{ét}}$ is the full subcategory of the category of X-schemes consisting of all X-schemes Y where the structure map $Y \to X$ is étale and where this subcategory is equipped with the étale topology;

X_{fl} denotes the big flat site on X [M2, p.47]; i.e. X_{fl} is the full subcategory of the category of X-schemes consisting of all X-schemes Y where the structure map $Y \to X$ is locally of finite type and where this subcategory is equipped with the flat topology.

(4.9.3) Define a presheaf $\mathcal{H}$ of sets on Spec A_{fl} as follows: for any morphism $U \to \text{Spec } A$, locally of finite type, put (see (4.1.4))

$$H^0_{\text{fl}}(U, \mathcal{H}) = \{f : U \to \mathbf{Y}_0^{\text{Drin}}(I) | f \text{ is a Heegner morphism of } A - \text{schemes}\}.$$

That is to say, $H^0_{\text{fl}}(U, \mathcal{H})$ is the subset of $\mathbf{Y}_0^{\text{Drin}}(I)(U)$ consisting of Heegner morphisms.

It is immediately checked that $\mathcal{H}$ is a presheaf.

4.9.4. Proposition. *The presheaf $\mathcal{H}$ is a sheaf of sets for the flat topology on* Spec A.

Proof. Let U be an A-scheme which is locally of finite type. Let $(g_i : U_i \to U)_{i \in I}$ be a covering of U for the flat site; that is to say, for each element i of the index set I the morphism of A-schemes $g_i : U_i \to U$ is flat and locally of finite type, and the union $\bigcup_{i \in I} g_i(U_i)$ of the images of the underlying topological spaces $g_i(U_i)$ is equal to the topological space U.

Now $\mathcal{H}$ is a sub-presheaf for the flat topology of the representable sheaf $\text{Hom}_A(-, \mathbf{Y}_0^{\text{Drin}}(I))$ on Spec A_{fl}. Hence we obtain a commutative diagram of sets, where we write $\mathbf{Y}$ in place of $\mathbf{Y}_0^{\text{Drin}}(I)$,

$$\begin{array}{ccccc} \text{Hom}_A(U, \mathbf{Y}) & \to & \prod_i \text{Hom}_A(U_i, \mathbf{Y}) & \overset{\to}{\underset{\to}{}} & \prod_{i,j} \text{Hom}_A(U_i \times_U U_j, \mathbf{Y}) \\ \uparrow & & \uparrow & & \uparrow \\ H^0_{\text{fl}}(U, \mathcal{H}) & \to & \prod_i H^0_{\text{fl}}(U_i, \mathcal{H}) & \overset{\to}{\underset{\to}{}} & \prod_{i,j} H^0_{\text{fl}}(U_i \times_U U_j, \mathcal{H}) \end{array}$$

where the top row is an exact diagram and the vertical arrows are injections. A diagram chase now shows that the map

$$H^0_{\text{fl}}(U, \mathcal{H}) \to \prod_{i \in I} H^0_{\text{fl}}(U_i, \mathcal{H})$$

is injective. It further shows that if the element $f' \in \prod_{i\in I} H^0_{\mathfrak{fl}}(U_i, \mathcal{H})$ is equalized under the two maps

$$\prod_{i\in I} H^0_{\mathfrak{fl}}(U_i, \mathcal{H}) \overset{\rightarrow}{\underset{\rightarrow}{}} \prod_{i,j\in I} H^0_{\mathfrak{fl}}(U_i \times_U U_j, \mathcal{H})$$

then f' arises from an element $f \in \mathrm{Hom}_A(U, \mathbf{Y}_0^{\mathrm{Drin}}(I))$; the element f' is a family of elements $f'_i \in H^0_{\mathfrak{fl}}(U_i, \mathcal{H})$, $i \in I$, and that f' arises from the element f implies that we have a commutative diagram of A-schemes for all $i \in I$

$$\begin{array}{ccc} & f & \\ U & \rightarrow & \mathbf{Y}_0^{\mathrm{Drin}}(I) \\ & g_i \nwarrow & \uparrow f'_i \\ & & U_i \end{array}$$

As we have $\bigcup_{i\in I} g_i(U_i) = U$ on the underlying topological spaces and the f'_i are Heegner morphisms, it follows that all geometric points of the image of f are Drinfeld-Heegner that is to say that f is a Heegner morphism. By the definition of $\mathcal{H}$, the element f' is then the image of an element $f \in H^0_{\mathfrak{fl}}(U, \mathcal{H})$. Hence the diagram

$$H^0_{\mathfrak{fl}}(U, \mathcal{H}) \rightarrow \prod_{i\in I} H^0_{\mathfrak{fl}}(U_i, \mathcal{H}) \overset{\rightarrow}{\underset{\rightarrow}{}} \prod_{i,j\in I} H^0_{\mathfrak{fl}}(U_i \times_U U_j, \mathcal{H})$$

is exact and $\mathcal{H}$ is a sheaf. □

(4.9.5) We call $\mathcal{H}$ a *Heegner sheaf on* Spec $A_{\mathfrak{fl}}$ and it is a subsheaf of the representable sheaf defined by the relative curve $\mathbf{Y}_0^{\mathrm{Drin}}(I)/A$.

(4.9.6) There are various different sheaves associated to $\mathcal{H}$; for example, we have the following.

Let K be an imaginary quadratic extension of the field F with respect to ∞. For any morphism $U \rightarrow$ Spec A locally of finite type, let $H^0_{\mathfrak{fl}}(U, \mathcal{H}_K)$ be the subset of $H^0_{\mathfrak{fl}}(U, \mathcal{H})$ of Heegner morphisms $f : U \rightarrow \mathbf{Y}_0^{\mathrm{Drin}}(I)$ where the geometric points of the
image of f all have complex multiplication by K; that is to say, we put

$$H^0_{\mathfrak{fl}}(U, \mathcal{H}_K) =$$

$$\{f \in H^0_{\mathfrak{fl}}(U, \mathcal{H}) | \text{ the geometric points of the image of } f \text{ have CM by } K\}.$$

In this instance a Drinfeld-Heegner point of $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ and represented by an isogeny $D \rightarrow D'$ of Drinfeld modules over a separably closed field has CM by K if and only if the common ring of endomorphisms of D, D' contains an

A-order of the field K. It may be checked as in the proof of proposition 4.9.4 that $\mathcal{H}_K$ is a subsheaf of $\mathcal{H}$ for the flat topology.

(4.9.7) Let O_c be an order of K with respect to A and with conductor c, where K is an imaginary quadratic extension of the field F with respect to ∞. For any morphism $U \to \operatorname{Spec} A$ locally of finite type, let $H^0_{\mathrm{fl}}(U, \mathcal{H}_{O_c})$ be the subset of $H^0_{\mathrm{fl}}(U, \mathcal{H})$ of Heegner morphisms $f : U \to \mathbf{Y}_0^{\mathrm{Drin}}(I)$ where the geometric points of f all have rings of endomorphisms which contain O_c as an A-subalgebra. Then $\mathcal{H}_{O_c}$ is a subsheaf of $\mathcal{H}$ for the flat topology.

(4.9.8) Let $x \in \mathbf{Y}_0^{\mathrm{Drin}}(I)$. Assume that x is a Drinfeld-Heegner point (see (4.1.3)). The *atomic Heegner sheaf* $\mathcal{H}_x$ is the subsheaf of $\mathcal{H}$ defined by

$$H^0_{\mathrm{fl}}(U, \mathcal{H}_x) = \{f : U \to \mathbf{Y}_0^{\mathrm{Drin}}(I) | \text{ the image of } f \text{ is contained in } \{x\}\}.$$

(4.9.9) Assume that the curve $\mathbf{X}_0^{\mathrm{Drin}}(I)/A$ has an A'-rational point

$$u : \operatorname{Spec} A' \to \mathbf{X}_0^{\mathrm{Drin}}(I)$$

where $A \to A'$ is a morphism of A-algebras which is locally of finite type. Let $J(I)$ be the relative Picard scheme of the relative curve $\mathbf{X}_0^{\mathrm{Drin}}(I) \times_A A'/A'$. Let $\mathcal{J}(I)$ be the representable sheaf of abelian groups for the flat topology on $\operatorname{Spec} A'_{\mathrm{fl}}$ defined by the commutative group scheme $J(I)/A'$. Via the point u, we obtain a morphism of A'-schemes

$$f : \mathbf{X}_0^{\mathrm{Drin}}(I) \times_A A' \to J(I), \quad x \mapsto x - u.$$

Let $\mathcal{J}_{\mathcal{H},A'}$ be the subsheaf of abelian groups of $\mathcal{J}(I)$ generated by the subsheaf of sets $f_*\mathcal{H}$ of $\mathcal{J}(I)$; that is to say, $\mathcal{J}_{\mathcal{H},A'}$ is the smallest subsheaf of abelian groups of $\mathcal{J}(I)$ containing the Heegner sheaf $f_*\mathcal{H}$ on $\operatorname{Spec} A'_{\mathrm{fl}}$.

(4.9.10) Extending the construction in (4.9.9) and (4.9.6), for an imaginary quadratic extension field K/F, we may define the subsheaf $\mathcal{J}_{K,\mathcal{H},A'}$ of $\mathcal{J}_{\mathcal{H},A'}$ which is the subsheaf of abelian groups of $\mathcal{J}_{\mathcal{H},A'}$ generated by the restriction of $\mathcal{H}_K$ to $\operatorname{Spec} A'_{\mathrm{fl}}$.

Let O_c be an order of K with respect to A and with conductor c. Let $\mathcal{J}_{O_c,\mathcal{H},A'}$ be the subsheaf of abelian groups of $\mathcal{J}_{\mathcal{H},A'}$ generated by the restriction of $\mathcal{H}_{O_c}$ to $\operatorname{Spec} A'_{\mathrm{fl}}$ (cf. (4.9.7)).

(4.9.11) Extending the construction in (4.9.9), let $x \in \mathbf{Y}_0^{\mathrm{Drin}}(I)$. Assume that x is a Drinfeld-Heegner point (see (4.1.3), (4.9.8) and (4.9.9)). We may define the subsheaf of abelian groups $\mathcal{J}_{x,\mathcal{H},A'}$ of $\mathcal{J}_{\mathcal{H},A'}$ generated by the restriction of the atomic Heegner sheaf $\mathcal{H}_x$ to $\operatorname{Spec} A'_{\mathrm{fl}}$.

(4.9.12) Extending again the construction of (4.9.9), let E/A be a relative curve over Spec A equipped with a finite surjective map of A-schemes $f : \mathbf{X}_0^{\mathrm{Drin}}(I) \to E$. We assume that E/A is a commutative A-group-scheme and that the generic fibre of E/A is an elliptic curve over F.

Let $\mathcal{E}$ be the representable sheaf of abelian groups for the flat topology on Spec A_{fl} defined by the commutative group scheme E/A. Let $\mathcal{E}_{\mathcal{H}}$ be the subsheaf of abelian groups of $\mathcal{E}$ generated by the subsheaf of sets $f_*\mathcal{H}$ of $\mathcal{E}$ obtained via f; that is to say, $\mathcal{E}_{\mathcal{H}}$ is the smallest subsheaf of abelian groups of $\mathcal{E}$ containing the image of the Heegner sheaf $\mathcal{H}$ on Spec A_{fl}.

We may similarly define the sheaves of abelian groups for the flat topology, which are subsheaves of the sheaf $\mathcal{E}$ on Spec A_{fl},

$$\mathcal{E}_{K,\mathcal{H}},\ \mathcal{E}_{O_c,\mathcal{H}},\ \mathcal{E}_{x,\mathcal{H}}.$$

These sheaves of abelian groups are generated by the subsheaves of sets $f_*\mathcal{H}_K,\ f_*\mathcal{H}_{O_c},\ f_*\mathcal{H}_x$ respectively.

It is the cohomology of the sheaf $\mathcal{E}_{K,\mathcal{H}}$ that arises in the proof given in [Br2] and in chapter 7 below of the Tate conjecture for the elliptic surface E/A.

5

The Heegner module

Let, where the notation of §2.1 holds,

K/F be an imaginary quadratic extension of F with respect to ∞;
Σ_F be the set of all places of F;
$\tilde{I}$ be a finite subset of Σ_F;
R be a commutative ring;
$\rho : \Sigma_F \setminus \tilde{I} \ \rightarrow \ R, \ \ v \mapsto a_v, \ $ be a map of sets.

We construct in §5.3 a discrete galois R-module $\mathcal{H}(\rho)$ over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ called the *Heegner module attached to ρ and K/F with coefficients in R.*

The Heegner module $\mathcal{H}(\rho)$ is defined by generators and relations over the ring R. The generators are the symbols $< b, c >$ where c runs over all effective divisors on Spec A and b runs over all divisor classes of $\mathrm{Pic}(O_c)$, the Picard group of the order O_c of K with conductor c. The relations are explicitly given in (5.3.5)-(5.3.8); they are derived from the action of the Hecke operators on Drinfeld-Heegner points.

The most important case of this construction of $\mathcal{H}(\rho)$ arises from elliptic curves. Suppose that E/F is an elliptic curve equipped with a finite surjective morphism of curves

$$\psi : X_0^{\mathrm{Drin}}(I) \rightarrow E.$$

For any prime number l different from the characteristic of F, the curve E provides a continuous l-adic representation

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \rightarrow \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l))$$

which is unramified at all except a finite set of places of F. Let K/F be an imaginary quadratic extension field of F in which all primes dividing the

M.L. Brown: LNM 1849, pp. 105–222, 2004.

conductor of E, except ∞, split completely. Let $\tilde{I}$ be the finite set of places of F at which ρ is ramified; let

$$a_v = \mathrm{Tr}(\rho(\mathrm{Frob}_v)|H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l))$$

be the trace on $H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l)$ of a Frobenius element of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ above the place v for all places $v \in \Sigma_F \setminus \tilde{I}$ of F. The character $\sigma : v \mapsto a_v$ of this representation ρ takes its values in $R = \mathbb{Z}$. The Heegner module $\mathcal{H}(\sigma)$ attached to σ and K/F with coefficients in $\mathbb{Z}$ is a discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module equipped with a galois-equivariant homomorphism (see examples 5.3.18)

$$f : \mathcal{H}(\sigma)^{(0)} \to E(F^{\mathrm{sep}})$$

where $\mathcal{H}(\sigma)^{(0)}$ is the direct summand of $\mathcal{H}(\sigma)$ generated by the symbols $< b, c >$ where c runs over all effective divisors on Spec A prime to the finite set $\tilde{I}$. The image of this homomorphism f is precisely the subgroup of $E(F^{\mathrm{sep}})$ generated by the Drinfeld-Heegner points. In particular, the image of f may contain points of finite and of infinite order over $\mathbb{Z}$.

After some preliminaries in §§5.1,5.2, the Heegner module $\mathcal{H}(\rho)$ is defined in §5.3. Basic properties of the Heegner module are given in §§5.7-5.11. In particular, we prove that, under a simple hypothesis, $\mathcal{H}(\rho)$ is a faithfully flat R-module (see §5.9). In §§5.4-5.6, we consider Čech galois cohomology; this is used partially to prove some of the fundamental properties of the Heegner module but is used more extensively in the next chapter on the cohomology of the Heegner module.

The notation of §2.1 holds throughout this chapter.

5.1 Group rings of finite abelian groups

We recall some results on commutative group algebras. For more details, see [CR, Chapters 3 and 4].

(5.1.1) Let G be a finite abelian group and let L be a field. Let ζ_n, for any $n \in \mathbb{N}$, be a primitive nth root of unity over L and $L(\zeta_n)$ denote the cyclotomic field generated by ζ_n over L.

(5.1.2) Let $p \geq 0$ be the characteristic of the field L. The abelian group G is canonically a direct product

$$G = G_1 \times G_2$$

where G_1 is a p-group and G_2 has order prime to p; we take $G_2 = G$ and $G_1 = \{1\}$ if $p = 0$.

The *group algebra* $L[G]$ is L-isomorphic to a tensor product of group algebras

$$L[G] \cong L[G_1] \otimes_L L[G_2].$$

Furthermore, $L[G_1]$ is an artin local ring with residue field L and $L[G_2]$ is a direct product of cyclotomic fields

$$L[G_2] \cong \prod_{i=1}^{t} L(\zeta_{a_i})$$

where $a_1, \ldots, a_t$ are positive integers.

The group G_2 is a direct product of finite cyclic groups of orders $n_1, n_2, \ldots, n_r$ which are prime to p and where n_i divides n_{i+1} for all i. This sequence of integers $n_1, \ldots n_r$, where $n_i | n_{i+1}$ for all i, is uniquely determined by the group G. The integers $a_1, \ldots, a_t$ of the above decomposition of $L[G_2]$ are equal to the integers, counting multiplicities,

$$\operatorname{lcm}(j_1, \ldots, j_r)$$

where $j_1, \ldots, j_r$ run through the positive integral divisors of $n_1, \ldots, n_r$, respectively. Denoting by $d(n)$ the number of positive integral divisors of an integer n, we have in particular the formula

$$t = \prod_{i=1}^{r} d(n_i).$$

(5.1.3) The rational group algebra $\mathbb{Q}[G]$ has a unique maximal order A over $\mathbb{Z}$; namely, A is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[G]$. Under the isomorphism $\mathbb{Q}[G] \cong \bigoplus_{i=1}^{t} \mathbb{Q}(\zeta_{a_i})$, the order A is given by

$$A \cong \bigoplus_{i=1}^{t} A_{a_i}$$

where A_n denotes the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$.

(5.1.4) The integral group ring $\mathbb{Z}[G]$ is a $\mathbb{Z}$-lattice of the group algebra $\mathbb{Q}[G]$ and is a sublattice of A. The conductor of $\mathbb{Z}[G]$ is the ideal of A defined by

$$\{x \in \mathbb{Q}[G] \mid xA \subseteq \mathbb{Z}[G]\}.$$

5.1.5. Proposition. (i) (Jacobinski) *Under the isomorphism* $\mathbb{Q}[G] \cong \bigoplus_{i=1}^{t} \mathbb{Q}(\zeta_{a_i})$, *the conductor of* $\mathbb{Z}[G]$ *is equal to*

$$\bigoplus_{i=1}^{t} |G| \mathfrak{D}_{a_i}^{-1}$$

where $\mathfrak{D}_{a_i}^{-1}$ *is the inverse different ideal of the ring of integers* A_{a_i}.
(ii) *The generic points of* Spec $\mathbb{Z}[G]$ *correspond bijectively with the subgroups* Γ *of* G *for which the quotient group* G/Γ *is cyclic.*

Proof. (i) This is the special case of Jacobinski's theorem for abelian group rings. For the proof, see [CR, Theorem 27.8].
(ii) Let $\mathfrak{p}$ be a generic point of Spec $\mathbb{Z}[G]$. By part (i), $\mathbb{Z}[G]$ is an order in a direct product of rings of integers of cyclotomic extensions of $\mathbb{Q}$. The localization $\mathbb{Z}[G]_{\mathfrak{p}}$ at $\mathfrak{p}$ is then isomorphic to a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some integer n. The elements of finite order of the multiplicative group $\mathbb{Q}(\zeta_n)^*$ are $\pm\zeta_n^r$, $r \in \mathbb{Z}$. Hence the torsion subgroup of $\mathbb{Z}[G]_{\mathfrak{p}}^*$ is isomorphic to $< -1, \zeta_n >$, which is the cyclic subgroup of order n or $2n$ of $\mathbb{C}^*$ generated by ζ_n and -1. Therefore the ring isomorphism $\mathbb{Z}[G]_{\mathfrak{p}} \cong \mathbb{Q}(\zeta_n)$ induces a homomorphism of finite abelian groups

$$f_{\mathfrak{p}} : G \to < -1, \zeta_n > .$$

The kernel $\Gamma_{\mathfrak{p}}$ of $f_{\mathfrak{p}}$ is a subgroup of G for which the quotient group $G/\Gamma_{\mathfrak{p}}$ is cyclic. This gives a map

$$\left\{ \begin{array}{c} \text{generic points of} \\ \text{Spec } \mathbb{Z}[G] \end{array} \right\} \to \left\{ \begin{array}{c} \text{subgroups } \Gamma \text{ of } G \\ \text{for which } G/\Gamma \text{ is cyclic.} \end{array} \right\}$$

$$\mathfrak{p} \mapsto \Gamma_{\mathfrak{p}} = \ \ker(G \to \mathbb{Z}[G]_{\mathfrak{p}}^*).$$

Conversely, given a subgroup Γ of G for which the quotient group is cyclic of order n, we may define a surjective homomorphism with kernel equal to Γ

$$h : G \to < \zeta_n >,$$

where $< \zeta_n >$ is the subgroup of $\mathbb{C}^*$ generated by ζ_n. Then h induces a surjective homorphism of rings

$$H : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_n].$$

The kernel of H is a prime ideal $\mathfrak{p}_\Gamma$ of $\mathbb{Z}[G]$ which is a generic point of the spectrum of this ring. The two maps

$$\mathfrak{p} \mapsto \Gamma_{\mathfrak{p}}, \ \ \Gamma \mapsto \mathfrak{p}_\Gamma$$

are mutually inverse and define the bijection stated in the proposition. □

5.2 The group rings Δ_c of Picard groups

(5.2.1) Let

K/F be an imaginary quadratic extension, with respect to ∞;
$\mathrm{Div}_+(A)$ be the semigroup of effective divisors on Spec A;
O_c be the order of K, with respect to A, with conductor $c \in \mathrm{Div}_+(A)$;
$K[c]/K$ be the ring class field with conductor $c \in \mathrm{Div}_+(A)$ (§2.3).

Let $\mathrm{Pic}(O_c)$ denote the Picard group of the order O_c of K. We write Δ_c for the integral group ring $\mathbb{Z}[\mathrm{Pic}(O_c)]$. A free basis of Δ_c over $\mathbb{Z}$ is the set of elements of $\mathrm{Pic}(O_c)$ represented by symbols

$$< b, c >, \text{ where } b \text{ runs through all elements of } \mathrm{Pic}(O_c).$$

For each divisor $c \in \mathrm{Div}_+(A)$, put

$$\Delta_{\leq c} = \bigoplus_{0 \leq c' \leq c} \Delta_{c'}.$$

The direct sum is well defined as there are only finitely many divisors c' satisfying $0 \leq c' \leq c$.

(5.2.2) If $c_1 \leq c_2$ are effective divisors in $\mathrm{Div}_+(A)$ then the inclusion $O_{c_2} \subset O_{c_1}$ defines a surjective transition homomorphism (as in (2.2.12))

$$t_{c_2,c_1} : \mathrm{Pic}(O_{c_2}) \to \mathrm{Pic}(O_{c_1}).$$

This induces a surjective group ring homomorphism

$$t^{\Delta}_{c_2,c_1} : \Delta_{c_2} \to \Delta_{c_1}$$

where, if $c_1 \leq c_2 \leq c_3$ are divisors in $\mathrm{Div}_+(A)$, we have

$$t^{\Delta}_{c_3,c_2} \circ t^{\Delta}_{c_2,c_1} = t^{\Delta}_{c_3,c_1}.$$

(5.2.3) The group rings Δ_c with the transition homomorphisms $t^{\Delta}_{c,c'}$ form a filtered inverse system $\{\Delta_c, t^{\Delta}_{c,c'}\}$ of commutative rings; that is to say, for any pair of divisors $c_1, c_2 \in \mathrm{Div}_+(A)$ with $c_1 \geq c$ and $c_2 \geq c$ there is a divisor $c_3 \in \mathrm{Div}_+(A)$ with $c_3 \geq c_1$ and $c_3 \geq c_2$ where the following diagram of transition homomorphisms is commutative

$$\begin{array}{ccc} & t^{\Delta}_{c_3,c_2} & \\ \Delta_{c_3} & \to & \Delta_{c_2} \\ t^{\Delta}_{c_3,c_1} \downarrow & & \downarrow \; t^{\Delta}_{c_2,c} \\ \Delta_{c_1} & \to & \Delta_c \\ & t^{\Delta}_{c_1,c} & \end{array}$$

(5.2.4) The group $\mathrm{Pic}(O_c)$ acts naturally on its group algebra Δ_c by permuting the standard generators

$$< a, c > . < b, c >=< ab, c > \text{ for all } < a, c >, < b, c >\in \mathrm{Pic}(O_c).$$

Similarly, the algebra $\Delta_{c'}$, for any divisor c' with $0 \leq c' \leq c$, is a Δ_c-module of finite type. The group $\mathrm{Pic}(O_c)$ acts naturally on $\Delta_{c'}$ for $c' \leq c$ via the recipe

$$< a, c > . < b, c' >= t^{\Delta}_{c,c'}(< a, c >) < b, c' > \text{ for all } < a, c >\in \mathrm{Pic}(O_c).$$

Hence the group $\mathrm{Pic}(O_c)$ acts on $\Delta_{\leq c}$ via its action on the components $\Delta_{c'}$ for $c' \leq c$. In this way, $\Delta_{\leq c}$ is a module of finite type over the ring Δ_c.

(5.2.5) Let **Div** be the category associated to the partially ordered set $\mathrm{Div}_+(A)$ with its usual order on divisors:-

(1) the objects of the category **Div** are the elements of $\mathrm{Div}_+(A)$;
(2) there is a unique morphism $c_2 \to c_1$ in **Div** if and only if $c_2 \geq c_1$; if $c_2 \not\geq c_1$ then there is no morphism $c_2 \to c_1$.

Let **Rings** denote the category of commutative rings. Then the assignment $c \to \Delta_c$ defines a covariant functor

$$\begin{array}{rccc} \Delta: & \textbf{Div} & \to & \textbf{Rings} \\ & c & \mapsto & \Delta_c \\ & \{c_2 \geq c_1\} & \mapsto & \{t^{\Delta}_{c_2,c_1} : \Delta_{c_2} \to \Delta_{c_1}\} \end{array}$$

where all the ring homomorphisms $t^{\Delta}_{c_2,c_1}$ are surjective.

5.3 The Heegner module of a galois representation

Let ρ be a finite dimensional continuous representation over a local field of the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$, where F^{sep} denotes the separable closure of F. Let K/F be an imaginary quadratic field extension with respect to ∞. We construct in this section a discrete galois module $\mathcal{H}(\rho)$ over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ called the *canonical Heegner module of ρ and K/F* (see (5.3.8) and (5.3.11)). When the representation ρ is that of the Tate module of an elliptic curve E/F with split multiplicative reduction at ∞, then there is a direct summand $\mathcal{H}(\rho)^{(0)}$ of $\mathcal{H}(\rho)$ which is equipped with a galois-equivariant homomorphism (see Examples 5.3.18)

$$\mathcal{H}(\rho)^{(0)} \to E(F^{\mathrm{sep}}).$$

The Heegner module $\mathcal{H}(\rho)$ is defined by generators and relations. The generators are the symbols $< b, c >$ where c runs over all divisors in $\mathrm{Div}_+(A)$, coprime to a finite exceptional set of divisors, and b runs over all divisor classes of $\mathrm{Pic}(O_c)$ the Picard group of the order O_c of K with conductor c. The relations are explicitly given in (5.3.6) (see also (5.3.13)); they are derived from the action of the Hecke operators on Drinfeld-Heegner points.

Construction of the Heegner module $\mathcal{H}(\rho)$

(5.3.1) Let (where the notation of §2.1 and of (5.2.1) holds)

K/F be an imaginary quadratic extension of F with respect to ∞;
Σ_F be the set of all places of F;
$\tilde{I}$ be a finite subset of Σ_F;
R be a commutative ring;
$\rho : \Sigma_F \setminus \tilde{I} \to R, \ v \mapsto a_v,$ be a map of sets.

(5.3.2) There are natural transition homomorphisms, for $c' \leq c$ in $\mathrm{Div}_+(A)$,

$$\Delta_{\leq c'} \hookrightarrow \Delta_{\leq c}$$

obtained from the inclusions $\Delta_{c'} \subseteq \Delta_{\leq c}$; we put

$$\Delta = \bigoplus_{c \in \mathrm{Div}_+(A)} \Delta_c = \varinjlim_{c \in \mathrm{Div}_+(A)} \Delta_{\leq c}.$$

We may extend $t^{\Delta}_{c,c-z} : \Delta_c \to \Delta_{c-z}$ to a homomorphism of abelian groups

$$t^{\Delta}_{c,c-z} : \Delta \to \Delta$$

by defining $t^{\Delta}_{c,c-z}$ to be zero on any component $\Delta_{c'}$ of $\Delta = \bigoplus_{c' \in \mathrm{Div}_+(A)} \Delta_{c'}$ for which $c' \neq c$. We also write $t^{\Delta}_{c,c-z}$ for the homomorphism $\Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{c-z} \otimes_{\mathbb{Z}} R$ induced by $t^{\Delta}_{c,c-z}$.

(5.3.3) For each divisor c in $\mathrm{Div}_+(A)$ and prime element z in the support of c we put

$$e_{c,c-z} = \sum_{<b,c>\in \ker(t_{c,c-z})} <b,c>$$

that is to say, $e_{c,c-z} \in \Delta_c$ is the sum of the elements in the kernel of the group homomorphism $t_{c,c-z} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c-z})$. The element $e_{c,c-z} \in \Delta_c$ is the scalar multiple of an idempotent in the rational group algebra $\Delta_c \otimes_{\mathbb{Z}} \mathbb{Q}$ in that we have

$$e_{c,c-z}^2 = |\ker(t_{c,c-z})| e_{c,c-z}.$$

(5.3.4) For each divisor c in $\mathrm{Div}_+(A)$ and each prime element $z \notin \tilde{I}$ in the support of c, we define a homomorphism of $\Delta_c \otimes_{\mathbb{Z}} R$-modules

$$\tilde{K}_{c,c-z} : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$$

by

$$\tilde{K}_{c,c-z} = a_z t^{\Delta}_{c,c-z} - \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z} i_c$$

where $i_c : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$ is the natural inclusion and $a_z \in R$, as in (5.3.1), is equal to $\rho(z)$. The homomorphism $\tilde{K}_{c,c-z}$ is induced from a homomorphism of $\Delta_c \otimes_{\mathbb{Z}} R$-modules

$$\Delta_c \otimes_{\mathbb{Z}} R \to (\Delta_c \otimes_{\mathbb{Z}} R) \oplus (\Delta_{c-z} \otimes_{\mathbb{Z}} R).$$

We may extend $\tilde{K}_{c,c-z}$ by linearity to an R-module homomorphism

$$\tilde{K}_{c,c-z} : \Delta \otimes_{\mathbb{Z}} R \to \Delta \otimes_{\mathbb{Z}} R$$

by defining $\tilde{K}_{c,c-z}$ to be zero on any component $\Delta_{c'}$ of Δ for which $c' \neq c$ and composing it with the inclusion map $\Delta_{\leq c} \subseteq \Delta$.

(5.3.5) For each divisor c in $\mathrm{Div}_+(A)$ and each prime divisor $z \notin \tilde{I}$ in the support of c, we define the homomorphism of $\Delta_c \otimes_{\mathbb{Z}} R$-modules

$$\epsilon(c,z) : \Delta_{c-z} \otimes_{\mathbb{Z}} R \to \Delta_{\leq c-z} \otimes_{\mathbb{Z}} R$$

via the formula (where the notation $\mathfrak{m}'_z, \mathfrak{p}_1, \mathfrak{p}_2, [[\mathfrak{m}'_z]]$, etc, is similar to that of table 4.6.9):

$\epsilon(c,z) =$

(1) 0	if z remains prime in K/F and is prime to $c-z$;
(2) $< [[\mathfrak{m}'_z]]^{-1}, c-z >$	if z is ramified in K/F and is prime to $c-z$ where $\mathfrak{m}'_z$ is the prime ideal of O_{c-z} lying above the ideal $\mathfrak{m}_z$ of A defining z;
(3) $< [[\mathfrak{p}_1]]^{-1}, c-z > + < [[\mathfrak{p}_2]]^{-1}, c-z >$	if z is split completely in K/F and is prime to $c-z$ where $\mathfrak{m}_z O_{c-z} = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct prime ideals of O_{c-z};
(4) $t^{\Delta}_{c-z,c-2z}$	if $z \in \mathrm{Supp}(c-z)$.

The homomorphism $\epsilon(c,z)$ is either an element of Δ_{c-z} acting on $\Delta_{c-z} \otimes_{\mathbb{Z}} R$ or is equal to $t^{\Delta}_{c-z,c-2z}$.

(5.3.6) For each divisor c in $\mathrm{Div}_+(A)$ and each prime divisor $z \notin \tilde{I}$ in the support of c, we define the homomorphism of Δ_c-modules

$$K_{c,c-z} : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$$

via the formula

$$K_{c,c-z} = \tilde{K}_{c,c-z} - \epsilon(c,z) \circ t^{\Delta}_{c,c-z}.$$

That is to say we have for all $\delta \in \Delta_c \otimes_{\mathbb{Z}} R$

$$K_{c,c-z}(\delta) = (a_z - \epsilon(c,z)) t^{\Delta}_{c,c-z}(\delta) - \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z}\delta.$$

These homomorphisms $K_{c,c-z}$ are modelled on the action of the Hecke operators on Drinfeld-Heegner points (see tables 4.6.9 and 4.8.5).

We may extend by linearity the homomorphisms of $\Delta_c \otimes_{\mathbb{Z}} R$-modules

$$K_{c,c-z} : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$$

to homomorphisms of R-modules

$$K_{c,c-z} : \Delta \otimes_{\mathbb{Z}} R \to \Delta \otimes_{\mathbb{Z}} R$$

by defining $K_{c,c-z}$ to be zero on any component $\Delta_{c'} \otimes_{\mathbb{Z}} R$ of $\Delta \otimes_{\mathbb{Z}} R$ for which $c' \neq c$ and composing $K_{c,c-z}$ with the inclusion map $\Delta_{\leq c} \otimes_{\mathbb{Z}} R \subset \Delta \otimes_{\mathbb{Z}} R$.

(5.3.7) Let $c \in \mathrm{Div}_+(A)$. Define $\Gamma_{\leq c}$ to be the $\Delta_c \otimes_{\mathbb{Z}} R$-submodule of $\Delta_{\leq c} \otimes_{\mathbb{Z}} R$ generated by the all the submodules $K_{c',c'-z}(\Delta_{c'} \otimes_{\mathbb{Z}} R)$, the images of the $K_{c',c'-z}$, where $z \notin \tilde{I}$ runs over all the closed points in the support of c' and c' runs over all divisors such that $c' \leq c$ and $c' \in \mathrm{Div}_+(A)$ i.e. we have

$$\Gamma_{\leq c} = < K_{c',c'-z}(\Delta \otimes_{\mathbb{Z}} R) \text{ for all } 0 \leq c' \leq c,\ z \in \mathrm{Supp}(c') \setminus \tilde{I} > .$$

(5.3.8) Let $c \in \mathrm{Div}_+(A)$. Put

$$\mathcal{H}_c = (\Delta_{\leq c} \otimes_{\mathbb{Z}} R)/\Gamma_{\leq c}.$$

The module $\mathcal{H}_c$ is evidently a $\Delta_c \otimes_{\mathbb{Z}} R$-module, as it is a quotient of two $\Delta_c \otimes_{\mathbb{Z}} R$-modules.

There are natural transition homomorphisms

$$\mathcal{H}_{c'} \to \mathcal{H}_c, \quad \text{for } c' \leq c \text{ in } \mathrm{Div}_+(A),$$

obtained from the inclusions $\Delta_{\leq c'} \subseteq \Delta_{\leq c}$; we put

$$\mathcal{H}(\rho) = \varinjlim_{c \in \mathrm{Div}_+(A)} \mathcal{H}_c$$

where the limit runs over all elements $c \in \mathrm{Div}_+(A)$. We also write $< a, c >$ for the image in $\mathcal{H}(\rho)$ of the element $< a, c > \in \mathrm{Pic}(O_c)$. Then $\mathcal{H}(\rho)$ is the *Heegner module of ρ, K/F, with coefficients in R.*

Let $< \tilde{I} >$ be the subsemi-group of $\mathrm{Div}_+(A)$ generated by the elements of $\tilde{I} \setminus \{\infty\}$; that is to say, $< \tilde{I} >$ is the set of effective divisors $c \in \mathrm{Div}_+(A)$ such that $\mathrm{Supp}(c) \subseteq \tilde{I}$. If $d \in < \tilde{I} >$, let $\mathcal{H}(\rho)^{(d)}$ be the submodule of $\mathcal{H}(\rho)$ which is the image of the evident homomorphism, where $\Delta_{c,R} = \Delta_c \otimes_{\mathbb{Z}} R$,

$$\begin{aligned} \bigoplus_{c \in \mathrm{Div}_+(A),\ \mathrm{Supp}(c) \cap \tilde{I} = \emptyset} \Delta_{c+d,R} &\ \to\ \mathcal{H}(\rho) \\ \bigoplus_c \delta_c &\mapsto \textstyle\sum_c \delta_c. \end{aligned}$$

Then $\mathcal{H}(\rho)$ clearly decomposes as a direct sum of submodules

$$\mathcal{H}(\rho) = \bigoplus_{d \in < \tilde{I} >} \mathcal{H}(\rho)^{(d)}.$$

Galois action on the Heegner module $\mathcal{H}(\rho)$

(5.3.9) An abelian group A with an action by the group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is called a *discrete galois module* if

$$A = \bigcup_U A^U$$

where U runs over all open subgroups of finite index of the profinite topological group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$; this condition is equivalent to the stabiliser of every element of A being an open subgroup of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$.

(5.3.10) The galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $\Delta_{\leq c} \otimes_{\mathbb{Z}} R$ via the reciprocity isomorphism for the ring class field extension $K[c]/K$ (see (2.3.4))

$$\psi : \mathrm{Gal}(K[c]/K) \cong \mathrm{Pic}(O_c), \text{ where } c \in \mathrm{Div}_+(A),$$

and the action (see (5.2.4)) of $\mathrm{Pic}(O_c)$ on $\Delta_{\leq c} \otimes_{\mathbb{Z}} R$. That is to say, the galois group $\mathrm{Gal}(K[c]/K)$ acts by permuting the symbols $< b, c' >$ for all $c' \leq c$ and $b \in \mathrm{Pic}(O_{c'})$ via the recipe

$$< b, c' >^g = < t_{c,c'}(\psi(g))^{-1} b, c' > \quad \text{for all } g \in \mathrm{Gal}(K[c]/K).$$

This reciprocity isomorphism takes the ring class field inclusions

$$K[c'] \subseteq K[c], \quad \text{for } c' \leq c,$$

to the surjective transition homomorphisms

$$t_{c,c'} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O'_c).$$

Hence the surjective homomorphism of profinite groups

$$\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Gal}\Big(\bigcup_{c \in \mathrm{Div}_+(A)} K[c]/K \Big)$$

induces the structure of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module on $\mathcal{H}(\rho)$. Furthermore, submodules $\mathcal{H}(\rho)^{(d)}$, for $d \in < \tilde{I} >$, are sub-$\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules of $\mathcal{H}(\rho)$. By (5.3.8), we obtain a decomposition of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\rho) = \bigoplus_{d \in < \tilde{I} >} \mathcal{H}(\rho)^{(d)}.$$

5.3.11 Definition. The discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module $\mathcal{H}(\rho)$ is the *Heegner module of ρ and K/F with coefficients in R.*

The finite set $\tilde{I}$ is the *exceptional* set of prime divisors of $\mathcal{H}(\rho)$. To distinguish the coefficient ring R, we sometimes write $\mathcal{H}(\rho, R)$ in place of $\mathcal{H}(\rho)$ and $\mathcal{H}_c(R)$ in place of $\mathcal{H}_c$; similarly for the components $\mathcal{H}(\rho, R)^{(d)}$, where $d \in < \tilde{I} >$, of $\mathcal{H}(\rho, R)$.

Explicit form of the Heegner module

We have the explicit formula for the homomorphism $\tilde{K}_{c,c-z}$, for a class $b \in \mathrm{Pic}(O_c)$ and each prime divisor $z \in \mathrm{Supp}(c) \setminus \tilde{I}$, where $< b, c > \in \mathrm{Pic}(O_c)$ and $c \in \mathrm{Div}_+(A)$,
(5.3.12)

$$\tilde{K}_{c,c-z} < b, c >= a_z < b^\flat, c - z > - \frac{|O^*_{c-z}|}{|A^*|} \sum_{<a,c> \in \ \ker(t_{c,c-z})} < ab, c >$$

where $< b^\flat, c - z >$ is the element $t_{c,c-z}(< b, c >)$ of $\mathrm{Pic}(O_{c-z})$.

Similar explicit formulae may be written for the homomorphisms $K_{c,c-z}$. For example, if z is split completely in K/F, prime to $c - z$, and coprime to $\tilde{I}$, then we have

$$K_{c,c-z} < b, c >= a_z < b^\flat, c - z > - \frac{|O^*_{c-z}|}{|A^*|} \sum_{<a,c> \in \ \ker(t_{c,c-z})} < ab, c >$$

$$- < [[\mathfrak{p}_1]]^{-1} b^\flat, c - z > - < [[\mathfrak{p}_2]]^{-1} b^\flat, c - z > .$$

(5.3.13) The elements of the canonical Heegner module $\mathcal{H}(\rho)$ are R-linear combinations of symbols $< b, c >$ where $c \in \mathrm{Div}_+(A)$ and $b \in \mathrm{Pic}(O_c)$. The relations between these symbols are generated by the relations for all z coprime to $\tilde{I}$

$$a_z < b^\flat, c - z >= \frac{|O^*_{c-z}|}{|A^*|} \sum_{<a,c> \in \ \ker(t_{c,c-z})} < ab, c > + \epsilon(c, z) < b^\flat, c - z >$$

where $\epsilon(c, z)$ is given by the formulae of (5.3.5) and where $b^\flat$ is the image of b in $\mathrm{Pic}(O_{c-z})$.

(5.3.14) The Galois action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the elements of $\mathcal{H}(\rho)$ is given by, where $g \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$,

$$< b, c >^g =< \phi(g)^{-1} b, c >$$

where ϕ is the reciprocity homomorphism

$$\phi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Pic}(O_c).$$

The case of a galois representation

The most important case of this construction of $\mathcal{H}(\rho)$ arises from galois representations and especially those arising from elliptic curves.

(5.3.15) Let E be a local field equipped with its usual topology i.e. E is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ or is a complete field for a discrete valuation with finite residue field. Let

V be a finite dimensional vector space over E; the space V is then equipped with its induced topology;
$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_E(V)$ be a continuous representation of the profinite galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ which is ramified at only finitely many places of F;
$\tilde{I}$ be the finite set of places of F at which ρ is ramified;
$a_v = \mathrm{Tr}(\rho(\mathrm{Frob}_v)|V)$ be the trace on V of a Frobenius element of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ above the place v for all places $v \in \Sigma_F \setminus \tilde{I}$ of F.

(5.3.16) Let R be a subring of the local field E such that $a_v \in R$ for all $v \in \Sigma_F \setminus \tilde{I}$. We let ρ also denote the map

$$\rho : \Sigma_F \setminus \tilde{I} \quad \to \quad R,\ v \mapsto a_v.$$

That is to say, ρ also denotes the character of the representation V. Let K/F be an imaginary quadratic extension field, with respect to ∞. Then associated to ρ, R, and K/F, is the Heegner module

$$\mathcal{H}(\rho) = \varinjlim_{c \in \mathrm{Div}_+(A)} \mathcal{H}_c(\rho)$$

with coefficients in R which is the discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module constructed above (see (5.3.11)). Similarly, for any R-algebra S, let

$$f \circ \rho : \Sigma_F \setminus \tilde{I} \quad \to \quad S,\ v \mapsto f(a_v)$$

be the composite of ρ with the structure map $f : R \to S$. We then have the Heegner module

$$\mathcal{H}(f \circ \rho, S) = \varinjlim_{c \in \mathrm{Div}_+(A)} \mathcal{H}_c(f \circ \rho, S)$$

of $f \circ \rho$, K/F, and with coefficients in S.

5.3.17. Remarks. (1) The Heegner module $\mathcal{H}(\rho)$ is constructed from the *character* of the representation ρ; in particular, the coefficient ring R of the Heegner module can be taken to be any ring which contains all values of the character of ρ.

(2) In the case of elliptic curves over global fields (see examples 5.3.18 below), the associated representation ρ satisfies the integrality restriction that its character takes values in $\mathbb{Z}$; thus we may in this instance take the ring R to be $\mathbb{Z}$ or more generally $\mathbb{Z}/n\mathbb{Z}$.

(3) *(The universal Heegner module.)* Let S be the non-noetherian ring

$$\mathbb{Z}[X_v, v \in \Sigma_F \setminus \tilde{I}]$$

which is the polynomial ring in infinitely many indeterminates X_v indexed by the elements of $\Sigma_F \setminus \tilde{I}$. Take ρ to be the map

$$\rho : \Sigma_F \setminus \tilde{I} \quad \to \quad S, \quad v \mapsto X_v.$$

Let $\mathcal{H} = \varinjlim \mathcal{H}_c$ be the corresponding Heegner module of ρ and K/F with coefficients in S.

Then $\mathcal{H}$ is a *universal Heegner module for K/F and $\tilde{I}$* in that for any map $\psi : \Sigma_F \setminus \tilde{I} \to R$ there is a homomorphism of rings $S \to R$ given by $X_v \mapsto \psi(v)$ such that there is an isomorphism of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\psi, R) \cong \mathcal{H} \otimes_S R$$

where

$$\mathcal{H}(\psi, R) = \varinjlim \mathcal{H}_c(\psi)$$

is the Heegner module of ψ and K/F with coefficients in R.

5.3.18 Examples. (1) *(Elliptic curves over F.)* Let E/F be an elliptic curve such that $E \times_F F_\infty/F_\infty$ is a Tate curve, where F_∞ is the completion of F at ∞. Then (theorem 4.7.1, see also §B.11 of Appendix B) there is a finite surjective morphism of F-curves

$$\pi : X_0^{\mathrm{Drin}}(I) \to E$$

where the ideal I of A is the conductor of E without the component at ∞. Let l be any prime number distinct from the characteristic of F. Let ρ be the 2-dimensional l-adic representation of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ corresponding to E where F^{sep} is the separable closure of F; that is to say ρ is the continuous homomorphism

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \otimes_F F^{\mathrm{sep}}, \mathbb{Q}_l)).$$

We put for all places v of F

$$a_v = \mathrm{Tr}(\rho(\mathrm{Frob}_v) | \ (H^1_{\text{ét}}(E \otimes_F F^{\mathrm{sep}}, \mathbb{Q}_l)^{I_v})$$

$$= |E_v(\kappa(v))| - 1 - |\kappa(v)|$$

where E_v denotes the closed fibre of the Néron model of E at v and I_v is an inertia subgroup of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ over v. Let $\tilde{I}$ be the finite subset of Σ_F given by

$$\tilde{I} = \mathrm{Supp}(I) \cup \{\infty\}.$$

Thus $\tilde{I}$ is the set of ramified places of ρ. Then the representation ρ provides a map of sets

$$\rho : \Sigma_F \setminus \tilde{I}, \quad v \mapsto a_v.$$

The map ρ satisfies the integrality hypothesis

$$a_v \in \mathbb{Z} \text{ for all } v \in \Sigma_F.$$

Let K be an imaginary quadratic extension field of F in which all primes dividing the conductor of E, except ∞, split completely. Let

$$\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c(\rho)$$

be the canonical Heegner module of ρ and K/F with coefficients in $\mathbb{Z}$. Let $\mathcal{H}(\rho)^{(0)}$ be the direct summand of $\mathcal{H}(\rho)$ corresponding to the divisor $0 \in < \tilde{I} >$ (see (5.3.8)). By the table 4.6.9, and the definition of $\mathcal{H}(\rho)$ by generators and relations, we obtain a homomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\rho)^{(0)} \to E(K^{\mathrm{sep}})$$

given by (for the notation, see (4.8.2) and (5.3.8))

$$< b, c > \mapsto (b, I_1, c, \pi)$$

where $c \in \mathrm{Div}_+(A)$ is prime to $\tilde{I}$ and $b \in \mathrm{Pic}(O_c)$ and whose image consists of the $\mathbb{Z}$-linear combinations of Drinfeld-Heegner points of E rational over all the ring class fields $K[c]$.

(2) *(Elliptic curves over* $\mathbb{Q}$*.)* Let $E/\mathbb{Q}$ be an elliptic curve with semistable reduction at all non-archimedian places of $\mathbb{Q}$. Let $N \in \mathbb{N}$ be the conductor of E. Then there is a finite surjective morphism (according to Wiles [W])

$$\pi : X_0(N) \to E$$

where $X_0(N)/\mathbb{Q}$ is the modular curve classifying elliptic curves equipped with a cyclic subgroup of order N. Let l be any prime number and $\mathbb{Q}^{\mathrm{sep}}$ be the algebraic closure of $\mathbb{Q}$. Let σ be the 2-dimensional l-adic representation of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})$ corresponding to E, that is to say σ is the continuous homomorphism

$$\sigma : \mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q}) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \otimes_{\mathbb{Q}} \mathbb{Q}^{\mathrm{sep}}, \mathbb{Q}_l)).$$

We put for all finite places p of $\mathbb{Q}$

$$a_p = \mathrm{Tr}(\sigma(\mathrm{Frob}_p)|\ (H^1_{\text{ét}}(E \otimes_{\mathbb{Q}} \mathbb{Q}^{\mathrm{sep}}, \mathbb{Q}_l)^{I_p})$$
$$= |E_p(\mathbb{F}_p)| - 1 - p$$

where $\mathbb{F}_p$ denotes the finite field with p elements, E_p denotes the closed fibre of the Néron model of E over the discrete valuation ring $\mathbb{Z}_{p\mathbb{Z}}$, and I_p denotes an inertia subgroup of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})$ over p. Let $\tilde{N}$ be the finite subset of $\Sigma_{\mathbb{Q}}$ given by

$$\tilde{N} = \mathrm{Supp}(N) \cup \{\infty\}$$

where ∞ is the archimedian place of $\mathbb{Q}$. Thus $\tilde{N}$ is the set of ramified places of σ. Then the representation σ provides a map of sets

$$\sigma : \Sigma_{\mathbb{Q}} \setminus \tilde{N}, \quad p \mapsto a_p.$$

The representation σ satisfies the integrality hypothesis

$$a_p \in \mathbb{Z} \text{ for all prime numbers } p.$$

Let $K/\mathbb{Q}$ be an imaginary quadratic extension field of $\mathbb{Q}$ in which all primes dividing the conductor N of E split completely. If B is the ring of integers of K then $NB = N_1N_2$ where N_1, N_2 are two ideals of B conjugate under $\mathrm{Gal}(K/F)$. One may then construct a canonical Heegner module

$$\mathcal{H}(\sigma) = \varinjlim_{n \in \mathbb{N}\setminus\{0\}} \mathcal{H}_n(\sigma)$$

of σ and $K/\mathbb{Q}$ with coefficients in $\mathbb{Z}$, exactly as above. This Heegner module then admits a decomposition (as in (5.3.8))

$$\mathcal{H}(\sigma) = \bigoplus_{n \in \mathbb{N}\setminus\{0\},\ \mathrm{Supp}(n) \subseteq \tilde{N}} \mathcal{H}(\sigma)^{(n)}$$

where n runs over all positive integers divisible only by primes dividing $\tilde{N}$. By the analogue of the table 4.6.9 for Hecke operators acting on the Heegner points of E and the definition of $\mathcal{H}(\sigma)$ by generators and relations, we would then have a homomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\sigma, \mathbb{Q})^{(1)} \to E(\mathbb{Q}^{\mathrm{sep}})$$

given by (where the notation is the evident variant of (4.8.2) and (5.3.8))

$$< b, n > \mapsto (b, N_1, n, \pi)$$

whose image consists of the linear combinations of Heegner points of E which are rational over the ring class fields $K[n]$ where $n \in \mathbb{N}$ is prime to $\tilde{N}$.

[We do not detail this case of elliptic curves over $\mathbb{Q}$ and the corresponding Heegner module in this paper. For more details on Heegner points on $E/\mathbb{Q}$, see for example [GB]. For the Shimura-Taniyama-Weil conjecture, see [W].]

5.4 Čech galois cohomology

We give in this section a brief account of the relation between Čech galois cohomology of a finite galois extension of schemes and derived functor galois cohomology.

The first part of this section (up to proposition 5.4.33) is largely a transposition of [M2, Chap. III, §2] on Čech étale cohomology to galois cohomology of a finite galois extension of fields or, more generally, schemes. In the final part, we define Čech galois cohomology with respect to a *filter* ((5.4.34) et seq).

Galois coverings

(5.4.1) Let X be a locally noetherian scheme and G be a finite group. Let G_X denote the X-scheme $\coprod_{\sigma\in G} X_\sigma$ where $X_\sigma = X$ for all σ; thus G_X is a disjoint union of copies of X. The group G acts on the X-scheme G_X by permuting the components via

$$\sigma|_{X_\rho} = \mathrm{id}_X \ : \ X_\rho \to X_{\rho\sigma} \quad \text{for all } \rho, \sigma \in G.$$

(5.4.2) Suppose that $Y \to X$ is a finite morphism of locally noetherian schemes and the finite group G acts on Y as an X-scheme. Recall that $Y \to X$ is *galois with galois group* G if $Y \to X$ is faithfully flat and the morphism

$$\psi : G_Y \to \ Y \times_X Y, \ \psi|_{Y_\sigma} = \{y \mapsto (y, y\sigma)\}$$

is an isomorphism.

This condition on Y/X is equivalent to: there is a faithfully flat morphism $U \to X$, locally of finite type, such that $Y \times_X U$ is isomorphic with its G-action to G_U (see [M2, Chap. I, Remark 5.4]). In particular, if $Y \to X$ is galois then it is an étale morphism.

(5.4.3) Let X be a connected locally noetherian scheme and $\overline{x} \to X$ be a geometric point. Let $\pi_1(X, \overline{x})$ denote the Grothendieck fundamental group of X with base point $\overline{x}$. Let $\mathbf{FEt}/X$ be the category of X-schemes which are finite and étale over X. Let $\pi_1(X, \overline{x}) - \mathbf{sets}$ denote the category of finite sets equipped with a continuous action by the profinite group $\pi_1(X, \overline{x})$. Then the functor

$$\begin{aligned} \mathbf{FEt}/X \ &\to \ \pi_1(X, \overline{x}) - \mathbf{sets} \\ Y &\mapsto \mathrm{Hom}_X(\overline{x}, Y) \end{aligned}$$

is an equivalence of categories (see [M2, Chap. 1, §5] and [Mu]). Here $\mathrm{Hom}_X(\overline{x}, Y)$ denotes the set of liftings of $\overline{x} \to X$ to $\overline{x} \to Y$.

The site $[X'/X]$

(5.4.4) Suppose for the rest of this section §5.4 that

X is a connected quasi-compact locally noetherian scheme;
$\overline{x} \to X$ is a geometric point of X;
X' is a connected finite galois covering of X with galois group G.

(5.4.5) Let $[\mathbf{Sch}/X]$ denote the category of schemes over X. For any integer $n \geq 1$, denote by $(X')^n$ the X-scheme $X' \times_X X' \times_X \ldots \times_X X'$ (n factors). Let $[X'/X]$ denote the full subcategory of $[\mathbf{Sch}/X]$ whose objects are morphisms $Y \to X$ which are finite and étale and such that there is an integer $n \geq 1$ and a finite surjective morphism of X-schemes $(X')^n \to Y$. It follows that such a morphism $(X')^n \to Y$ is a finite étale covering of Y.

As G is the galois group of the finite galois connected covering X'/X then G is a quotient of $\pi_1(X, \overline{x})$ by an open subgroup. Hence under the equivalence of categories between $\mathbf{FEt}/X$ and $\pi_1(X, \overline{x}) - \mathbf{sets}$, the category $[X'/X]$ is equivalent to the category of all finite sets equipped with an action by the group G.

The category $[X'/X]$ admits finite fibre products. Every morphism in $[X'/X]$ is étale (by [M2, Ch. I, Cor. 3.6]).

5.4.6. Remarks. (i) Let U be an object of $[X'/X]$ which is connected. Then there is a finite surjective étale morphism of X-schemes $f : X' \to U$ and f is galois.

[For the proof, as U is an object of $[X'/X]$ there is an integer $n \geq 1$ and a surjective finite étale morphism of X-schemes $f : (X')^n \to U$. The map f is finite and étale hence f is an open and closed morphism (that f is open follows from [M2, Chap 1, theorem 2.12]). Hence if C is a connected component of $(X')^n$ then the morphism f restricts to a finite étale surjective morphism $f|_C : C \to U$ of X-schemes. But the connected components of $(X')^n$ are X-isomorphic to X'. Hence in every case there is a finite surjective étale morphism $f : X' \to U$.

Let $\phi \in \mathrm{Hom}_X(\overline{x}, U)$. Denote by $\mathrm{Hom}_\phi(\overline{x}, X')$ the subset of $\mathrm{Hom}_X(\overline{x}, X')$ of maps $h : \overline{x} \to X'$ such that the diagram

$$\begin{array}{ccc} \overline{x} & \overset{h}{\to} & X' \\ & {\scriptstyle\phi}\searrow & \downarrow f \\ & & U \end{array}$$

is commutative. We have

$$\coprod_{\phi \in \mathrm{Hom}_X(\overline{x}, U)} \mathrm{Hom}_\phi(\overline{x}, X') = \mathrm{Hom}_X(\overline{x}, X').$$

The sets $\mathrm{Hom}_X(\overline{x}, X')$ and $\mathrm{Aut}_X(X')$ are in bijection as X'/X is galois by hypothesis (5.4.4). If $g \in \mathrm{Aut}_X(X')$ then g gives a map

$$\begin{array}{ccccc} \overline{x} & \stackrel{h}{\rightarrow} & X' & \stackrel{g}{\rightarrow} & X' \\ & \phi \searrow & \downarrow f & & \downarrow f \\ & & U & & U \end{array}$$

Hence we have a map $f \circ g \circ h : \overline{x} \to U$. If the map $f \circ g \circ h$ coincides with ϕ then $g \in \mathrm{Aut}_U(X')$ (by [M2, Chap 1, Corollary 3.13]). Hence $\mathrm{Aut}_X(X')$ acts on the set $\mathrm{Hom}_X(\overline{x}, X') = \coprod_{\phi \in \mathrm{Hom}_X(\overline{x}, U)} \mathrm{Hom}_\phi(\overline{x}, X')$ and this permutation action is faithful and transitive because X'/X is galois; furthermore, the group $\mathrm{Aut}_X(X')$ permutes the subsets $\mathrm{Hom}_\phi(\overline{x}, X')$ amongst themselves. An element $g \in \mathrm{Aut}_X(X')$ preserves a subset $\mathrm{Hom}_\phi(\overline{x}, X')$ if and only if $g \in \mathrm{Aut}_U(X')$ in which case g then preserves all subsets $\mathrm{Hom}_\phi(\overline{x}, X')$ for all $\phi \in \mathrm{Hom}_X(\overline{x}, U)$. Hence we have

$$|\mathrm{Aut}_X(X')| = |\mathrm{Aut}_U(X')|.|\mathrm{Hom}_X(\overline{x}, U)|$$

and hence $\mathrm{Aut}_U(X')$ has the same number of elements as $\mathrm{Hom}_\phi(\overline{x}, X')$. It results that $f : X' \to U$ is galois, as required.]

(ii) Suppose that D/E is a finite galois extension of fields and $X = \mathrm{Spec}\ E$, $X' = \mathrm{Spec}\ D$. Then the opposite category $[X'/X]^{\mathrm{op}}$ of $[X'/X]$ is equivalent to the category of all finite étale E-algebras which are direct products of a finite number of subfields of D.

(5.4.7) For any object U of $[X'/X]$, define the category $[X'/U]_X$ as follows. We have that $[X'/U]_X$ is the full subcategory of the category of schemes over U whose objects are morphisms $Y \to U$ which are finite and étale and such that there is an integer $n \geq 1$ and a finite surjective morphism of X-schemes $(X')^n \to Y$. Evidently, $[X'/U]_X$ is a full subcategory of $[X'/X]$; the category $[X'/X]_X$ is equivalent to $[X'/X]$.

(5.4.8) Let Z be a locally noetherian scheme. Let $[\mathbf{Sch}/Z]$ denote the category of schemes over X. Let $[\mathbf{C}/Z]$ denote the full subcategory of $[\mathbf{Sch}/Z]$ whose objects are morphisms $Y \to Z$ which are étale and of finite type.

We recall that a covering of an object Y of $[\mathbf{C}/Z]$ is a family $\{f_i : U_i \to Y\}_{i \in I}$, where I is a set, such that each f_i is étale and of finite type and Y is the set-theoretic union of the images of the f_i i.e.

$$Y = \bigcup_{i \in I} f_i(U_i).$$

We recall also that the category $[\mathbf{C}/Z]$ together with the class of all such coverings of all objects of $[\mathbf{C}/Z]$ is the *étale site of* Z written $Z_{\text{ét}}$.

(5.4.9) Let U be an object of $[X'/X]$. Then a covering of U in $[X'/X]$ is a family of finite étale morphisms

$$\{g_\lambda : U_\lambda \to U\}_{\lambda \in \Lambda}$$

in $[X'/X]$ such that $U = \bigcup_\lambda g_\lambda(U_\lambda)$.

Similarly one may define a covering of an object V of the category $[X'/U]_X$ (see (5.4.7)) for any object U of $[X'/X]$: a covering of V is a family of finite étale morphisms in $[X'/U]_X$ with target V such that V is the set-theoretic union of the images of the morphisms of the family.

(5.4.10) The category $[X'/X]$ equipped with the family of coverings of all its objects is a Grothendieck topology as it verifies these conditions:

(a) an isomorphism $\phi : U \to U$ is a covering of U;
(b) if $\{g_\lambda : U_\lambda \to U\}_\lambda$ is a covering and $\{g_{\lambda\mu} : U_{\lambda\mu} \to U_\lambda\}_\mu$ is a covering for all λ then $\{g_{\lambda\mu} \circ g_\lambda : U_{\lambda\mu} \to U\}_{\lambda,\mu}$ is a covering of U;
(c) if $\{g_\lambda : U_\lambda \to U\}_\lambda$ is a covering and $V \to U$ is a morphism in $[X'/X]$ then $\{g_\lambda \times_U \mathrm{id}_V : U_\lambda \times_U V \to V\}_\lambda$ is a covering of V.

This site $[X'/X]$ is a subsite of the étale site $X_{\text{ét}}$ on X. Similarly, for any object U of $[X'/X]$, the category $[X'/U]_X$ equipped with the family of coverings of all its objects is a Grothendieck topology.

Sheaves on the site $[X'/X]$

(5.4.11) A presheaf (of abelian groups) on the site $[X'/X]$ is a contravariant functor

$$\mathcal{P} : [X'/X]^{\text{op}} \to \mathbf{Ab}$$

where $\mathbf{Ab}$ denotes the category of abelian groups. A presheaf $\mathcal{P}$ is a sheaf (of abelian groups) if it satisfies the usual sheaf condition with respect to coverings, that is to say, the diagram

$$\mathcal{P}(U) \to \prod_\lambda \mathcal{P}(U_\lambda) \overset{\to}{\underset{\to}{}} \prod_{\lambda,\mu} \mathcal{P}(U_\lambda \times_U U_\mu)$$

is exact for all coverings $\{U_\lambda \to U\}_{\lambda \in \Lambda}$ of $[X'/X]$.

The categories of sheaves and presheaves (of abelian groups) on $[X'/X]$ are defined in the evident way (see [M2, Chapter 2]) and are denoted by $\mathrm{Sh}[X'/X]$ and $\mathrm{Prsh}[X'/X]$, respectively. Similarly, for any object U of $[X'/X]$, one may

define the category of sheaves $\mathrm{Sh}[X'/U]_X$ and the category of presheaves $\mathrm{Prsh}[X'/U]_X$ on the site $[X'/U]_X$.

5.4.12. Proposition. *The category of sheaves of abelian groups* $\mathrm{Sh}[X'/X]$ *on* $[X'/X]$ *is equivalent to the category of* $\mathbb{Z}[G]$*-modules where* G *is the galois group of the finite galois extension* X'/X*. In particular, short exact sequences of sheaves on* $[X'/X]$ *correspond to short exact sequences of* $\mathbb{Z}[G]$*-modules.*

Proof. If M is a $\mathbb{Z}[G]$-module then we define a presheaf $\mathcal{S}_M$ on the site $[X'/X]$ by putting for any object U of the category $[X'/X]$

$$\Gamma(U, \mathcal{S}_M) = \mathrm{Hom}_G(\mathrm{Hom}_X(\overline{x}, U), M)$$

where $\overline{x}$ is the fixed geometric point of X and where $\mathrm{Hom}_X(\overline{x}, -)$ is the functor giving the equivalence of categories between $\mathbf{FEt}/G$ and $\pi_1(X, \overline{x}) - \mathbf{sets}$ of (5.4.3). In particular, if U is an object of $[X'/X]$ and is a connected scheme equipped with a finite étale surjective morphism $U \to X$ such that X'/U is galois with galois group H, then we have

$$\Gamma(U, \mathcal{S}_M) = M^H.$$

The presheaf $\mathcal{P} = \mathcal{S}_M$ is a sheaf. Let $(U_i \to U)_{i \in I}$ be a covering of U in $[X'/X]$. As X is quasi-compact, (see (5.4.4)) the scheme U also is quasi-compact. Hence there is a finite subset I' of I such that $(U_i \to U)_{i \in I'}$ is a covering of U in $[X'/X]$. Hence we obtain a commutative diagram where the vertical maps are inclusions

$$\begin{array}{ccccc} \mathcal{P}(U) & \to & \prod_{i \in I'} \mathcal{P}(U_i) & \overset{\to}{\to} & \prod_{i,j \in I'} \mathcal{P}(U_i \times_U U_j) \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{P}(U) & \to & \prod_{i \in I} \mathcal{P}(U_i) & \overset{\to}{\to} & \prod_{i,j \in I} \mathcal{P}(U_i \times_U U_j) \end{array}$$

It follows that if the top row here is an exact diagram then the bottom row is exact. Hence to show that $\mathcal{P}$ is a sheaf we need only consider those coverings $(U_i \to U)_{i \in I}$ of U in $[X'/X]$ such that the set I is finite.

Suppose then that $(U_i \to U)_{i \in I}$ is a covering in $[X'/X]$ where I is finite. Let $V = \coprod_{i \in I} U_i$. Then $V \to U$ is also a covering of U in $[X'/X]$ and $V \to X$ is finite and étale. We have an isomorphism of diagrams

$$\begin{array}{ccccc} \mathcal{P}(U) & \to & \prod_i \mathcal{P}(U_i) & \overset{\to}{\to} & \prod_{i,j} \mathcal{P}(U_i \times_U U_j) \\ \cong\downarrow & & \cong\downarrow & & \cong\downarrow \\ \mathcal{P}(U) & \to & \mathcal{P}(V) & \overset{\to}{\to} & \mathcal{P}(V \times_U V) \end{array}$$

Hence we may reduce to the case of a covering of the form $h : V \to U$ of $[X'/X]$. As X is connected the scheme U has only finitely many connected

components. Furthermore, if U is a disjoint union $U = U_1 \coprod U_2$ of two objects of $[X'/X]$ then we have

$$\Gamma(U, \mathcal{S}_M) = \Gamma(U_1, \mathcal{S}_M) \times \Gamma(U_2, \mathcal{S}_M)$$

and $h^{-1}(U_1) \to U_1$, $h^{-1}(U_2) \to U_2$ are coverings of U_1, U_2 in $[X'/X]$. To show that $\mathcal{P}$ is a sheaf, we may therefore reduce to the case where U is connected. By remark 5.4.6(i), there is then a finite surjective étale galois morphism $f : X' \to U$.

If V' is a connected component of V then the map $V' \to X$ is finite and étale and surjective; hence V' is an object of $[X'/X]$. Furthermore, $h|_{V'} : V' \to U$ is then a finite étale morphism in $[X'/X]$. As $h|_{V'}$ is finite it is a closed morphism and as it is étale $h|_{V'}$ is an open morphism; hence $h|_{V'}(V')$ is an open and closed subscheme of U and hence $h|_{V'}$ is surjective as U is connected. Hence $h|_{V'} : V' \to U$ is a finite étale covering of U. Hence to show that $\mathcal{P}$ is a sheaf, we may reduce to the case where the scheme V is connected. By remark 5.4.6(i), there is then a finite surjective étale galois morphism $f : X' \to V$ with galois group H_V, say, and the composite $X' \to V \to U$ is galois with galois group H_U, say. Hence we have

$$\mathcal{P}(V) = M^{H_V} \quad \text{and} \quad \mathcal{P}(U) = M^{H_U}.$$

As $X' \to U$ is galois we have a commutative diagram where the second column is an exact diagram (by [M2, Chap. II, Proposition 1.4])

$$\begin{array}{ccccc}
\mathcal{P}(V \times_U V) & \to & \mathcal{P}(X' \times_U X') & \cong & \prod_{i=1}^{i=|H_U|} M \\
\uparrow\ \uparrow & & \uparrow\ \uparrow & & \\
\mathcal{P}(V) = M^{H_V} & \to & \mathcal{P}(X') = M & & \\
\uparrow & & \uparrow & & \\
\mathcal{P}(U) & = & \mathcal{P}(U) = M^{H_U} & &
\end{array}$$

It follows by a diagram chase that the first column is also an exact diagram; hence $\mathcal{P}$ is a sheaf.

If $M \to M'$ is a homomorphism of $\mathbb{Z}[G]$-modules then this induces a homomorphism of sheaves $\mathcal{S}_M \to \mathcal{S}_{M'}$ on $[X'/X]$. Let $\mathcal{F}$ be a sheaf on $[X'/X]$; then $\mathcal{F}(X')$ is naturally a $\mathbb{Z}[G]$-module. If $\mathcal{F} \to \mathcal{F}'$ is a morphism of sheaves on $[X'/X]$ then $\mathcal{F}(X') \to \mathcal{F}'(X')$ is a homomorphism of $\mathbb{Z}[G]$-modules. Furthermore, the map

$$\mathrm{Hom}_{\mathbb{Z}[G]}(M, M') \to \mathrm{Hom}(\mathcal{S}_M, \mathcal{S}_{M'})$$

is an isomorphism and the natural homomorphism $\mathcal{F} \to \mathcal{S}_{\mathcal{F}(X')}$ is an isomorphism of sheaves on $[X'/X]$. Hence $M \mapsto \mathcal{S}_M$ and $\mathcal{F} \mapsto \mathcal{F}(X')$ establishes an equivalence of categories between the abelian category of sheaves $\mathrm{Sh}[X'/X]$ on $[X'/X]$ and the abelian category of $\mathbb{Z}[G]$-modules. □

5.4.13. Proposition. *The category* $\mathrm{Sh}[X'/X]$ *has enough injectives. Under the equivalence of abelian categories between* $\mathrm{Sh}[X'/X]$ *and the category of* $\mathbb{Z}[G]$*-modules (see proposition 5.4.12), the right derived functors* $H^i_{[X'/X]}(X, -)$ *of the global section functor*

$$\mathcal{S} \mapsto \Gamma(X, \mathcal{S})$$

coincide with the group cohomology $H^i(G, -)$ *of the finite group* G *on the category of* $\mathbb{Z}[G]$*-modules.*

Proof. That $\mathrm{Sh}[X'/X]$ has enough injectives follows from the equivalence of categories (see proposition 5.4.12) between $\mathrm{Sh}[X'/X]$ and the category of $\mathbb{Z}[G]$-modules and that the latter category has enough injectives. The global section functor on $\mathrm{Sh}[X'/X]$ corresponds to the functor on $\mathbb{Z}[G]$-modules given by

$$M \mapsto M^G.$$

Hence the right derived functors of the global section functor may be computed via the group cohomology of $\mathbb{Z}[G]$-modules.□

5.4.14. Proposition. *The category of presheaves* $\mathrm{Prsh}[X'/X]$ *has enough injectives.*

Proof. The abelian category $\mathrm{Prsh}[X'/X]$ satisfies the conditions $AB5$ and $AB3^*$ of Grothendieck (see [BD, Chapter 5]); the property $AB5$ expresses that in the abelian category $\mathrm{Prsh}[X'/X]$ any family of objects has a direct sum and any filtered direct limit of exact sequences is exact; the property $AB3^*$ expresses that in $\mathrm{Prsh}[X'/X]$ any family of objects has a direct product. Hence in order to show that $\mathrm{Prsh}[X'/X]$ has enough injectives we only need show that it has a family of generators, by [M2, Chap III, Lemma 1.3]. We recall that a family of objects $\{A_j\}_{j\in J}$ is a family of generators of $\mathrm{Prsh}[X'/X]$ if given a monomorphism $B \to A$ in $\mathrm{Prsh}[X'/X]$ that is not an isomorphism there is an index j and a morphism $A_j \to A$ that does not factor though $B \to A$.

Given an object $\pi : U \to X$ of $[X'/X]$ we have the corresponding site $[X'/U]_X$ (see (5.4.5) and (5.4.7)) and a morphism of sites $\pi : [X'/U]_X \to [X'/X]$. Then there is a functor defined by restriction $\pi^p : \mathrm{Prsh}[X'/X] \to \mathrm{Prsh}[X'/U]_X$ where $\Gamma(V, \pi^p\mathcal{P}) = \Gamma(V, \mathcal{P})$ for any $V \to U$ in $[X'/U]_X$. This functor π^p admits a left adjoint which is the functor "extension by zero" $\pi_! : \mathrm{Prsh}[X'/U]_X \to \mathrm{Prsh}[X'/X]$. We have explicitly for $P \in \mathrm{Prsh}[X'/U]_X$ and $V \to X$ in $[X'/X]$ that

$$(\pi_!\mathcal{P})(V) = \varinjlim \mathcal{P}(V')$$

where the limit is taken over all commutative squares

$$\begin{array}{ccc} V' & \leftarrow & V \\ \downarrow & & \downarrow \\ U & \rightarrow & X \end{array}$$

in $[X'/X]$. It is trivial to check that $\pi_!$ is a left adjoint to π^p.

Let $\mathbb{Z}$ denote the constant presheaf $\mathbb{Z}$ on $[X'/U]_X$ that is to say $\Gamma(U', \mathbb{Z}) = \mathbb{Z}$ for any object U' of $[X'/U]_X$. Let $\mathbb{Z}_U = \pi_!\mathbb{Z}$ be the extension by zero of $\mathbb{Z}$ on $[X'/U]_X$. Then we have for any $\mathcal{P} \in \mathrm{Prsh}[X'/X]$

$$\mathrm{Hom}_X(\mathbb{Z}_U, \mathcal{P}) \cong \mathrm{Hom}_U(\mathbb{Z}, \pi^p\mathcal{P}) \cong \mathcal{P}(U).$$

A family of generators for $\mathrm{Prsh}[X'/X]$ is then formed by taking the presheaf $\mathbb{Z}_U$ in $\mathrm{Prsh}[X'/X]$ for each isomorphism class of objects $U \to X$ of $[X'/X]$, as required.□

5.4.15 Example. We consider the category $\mathrm{Prsh}[X'/X]$ in the case where $X' = X$.

Let $\mathbf{N}$ denote the full subcategory of the category of sets and whose objects are finite non-empty sets where there is just one set $[n]$ of each cardinality $n \in \mathbb{N} - \{0\}$.

The underlying category of the site $[X'/X']$ is equivalent to the category of all non-empty finite sets and is therefore equivalent to the category $\mathbf{N}$.

The category of presheaves $\mathrm{Prsh}[X'/X']$ is equivalent to the category of all families $\{A_n\}_{n\geq 1}$ of abelian groups A_n indexed by the positive integers $n \in \mathbb{N} - \{0\}$ and equipped with a compatible set of "restriction" homomorphisms $f_{nm} : A_m \to A_n$ for all morphisms $f_{nm} : [n] \to [m]$ in the category $\mathbf{N}$.

(5.4.16) Suppose only for this paragraph that D/E is a finite galois extension of fields and that $X = \mathrm{Spec}\ E$ and $X' = \mathrm{Spec}\ D$. Let $\mathcal{S}$ be a sheaf on the étale site $X_{\text{ét}}$. Then the restriction $\mathcal{S}|_{[X'/X]}$ of $\mathcal{S}$ to $[X'/X]$ is also a sheaf on the site $[X'/X]$. The cohomology groups $H^i_{[X'/X]}(X, \mathcal{S}|_{[X'/X]})$ are related to the étale cohomology groups $H^i_{\text{ét}}(X, \mathcal{S})$ by a spectral sequence. Let E^{sep} be the separable closure of the field E; the sheaf $\mathcal{S}$ is given by a discrete $\mathrm{Gal}(E^{\mathrm{sep}}/E)$-module M and we have isomorphisms

$$H^i_{\text{ét}}(X, \mathcal{S}) \cong H^i(\mathrm{Gal}(E^{\mathrm{sep}}/E), M)$$

and

$$H^i_{[X'/X]}(X, \mathcal{S}|_{[X'/X]}) \cong H^i(\mathrm{Gal}(D/E), H^0(\mathrm{Gal}(E^{\mathrm{sep}}/D), M)).$$

The Hochschild-Serre spectral sequence for M and the galois extension D/E may be written as

$$E_2^{i,j} = H^i_{[X'/X]}(X, \mathcal{S}^{(j)}) \Rightarrow H^{i+j}_{\text{ét}}(X, \mathcal{S}).$$

where $\mathcal{S}^{(j)}$ is the sheaf on $[X'/X]$ associated to the $\mathbb{Z}[G]$-module $H^j_{\text{ét}}(X', \mathcal{S})$ (see proposition 5.4.12). In conclusion, we have that $H^i_{[X'/X]}(X, \mathcal{S}|_{[X'/X]})$ is the $E_2^{i,0}$-term in a Hochschild-Serre spectral sequence whose abutment is $H^i_{\text{ét}}(X, \mathcal{S})$.

Čech cohomology on the site $[X'/X]$

(5.4.17) Let I be a set. Denote by I^p the pth power of I consisting of ordered p-tuples of elements of I. For any integer j such that $0 \leq j \leq p$ let

$$\delta_j : I^{p+1} \to I^p$$

denote the jth deletion map defined by

$$\delta_j : (i_0, \ldots, i_p) \mapsto (i_0, \ldots, i_{j-1}, i_{j+1}, \ldots, i_p).$$

(5.4.18) Let $\mathcal{P}$ be a presheaf of abelian groups on the site $[X'/X]$. Let $U \to X$ be a morphism in $[X'/X]$. Let $\mathcal{U} = \{f_i : U_i \to U\}_{i \in I}$ be a covering of U in $[X'/X]$.

For any $p+1$-tuple $\mathbf{i} = (i_0, \ldots, i_p)$ of indices $i_j \in I$ we put

$$U(\mathbf{i}) = U_{i_0} \times_U U_{i_1} \times_U \ldots \times_U U_{i_p}.$$

The projection morphism

$$U(\mathbf{i}) \to U(\delta_j \mathbf{i})$$

induces a restriction map

$$\text{res}(\delta_j|\mathbf{i}) : \Gamma(U(\delta_j \mathbf{i}), \mathcal{P}) \to \Gamma(U(\mathbf{i}), \mathcal{P}).$$

Define a complex

$$\mathcal{C}(\mathcal{U}/U, \mathcal{P}) = \{\mathcal{C}^p(\mathcal{U}/U, \mathcal{P}), d^p\}_{p \in \mathbb{N}}$$

in the following way: we put

$$\mathcal{C}^p(\mathcal{U}/U, \mathcal{P}) = \prod_{\mathbf{i} \in I^{p+1}} \Gamma(U(\mathbf{i}), \mathcal{P})$$

and

$$d^p : \mathcal{C}^p(\mathcal{U}/U, \mathcal{P}) \to \mathcal{C}^{p+1}(\mathcal{U}/U, \mathcal{P})$$

is the coboundary homomorphism defined by

$$s = (s_{\mathbf{i}})_{\mathbf{i}\in I^{p+1}} \in \mathcal{C}^p(\mathcal{U}/U, \mathcal{P})$$

$$(d^p s)_{\mathbf{i}} = \sum_{j=0}^{p+1} (-1)^j \mathrm{res}(\delta_j|\mathbf{i})(s_{\delta_j \mathbf{i}}).$$

It is immediately checked that $d^p \circ d^{p-1} = 0$ hence $\mathcal{C}(\mathcal{U}/U, \mathcal{P})$ is indeed a complex.

(5.4.19) The cohomology groups of the complex $\{\mathcal{C}^p(\mathcal{U}/U, \mathcal{P}), d^p\}_{p\in\mathbb{N}}$ are the Čech cohomology groups

$$\check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{P})$$

of the presheaf $\mathcal{P}$ on $[X'/X]$ with respect to the covering $\mathcal{U}$ of U.

(5.4.20) A second covering $\mathcal{V} = \{g_j : V_j \to U\}_{j\in J}$ of U in $[X'/X]$ is a *refinement* of the covering $\mathcal{U}/U$ if there is a map $\sigma : J \to I$ such that g_j factors through $f_{\sigma(j)}$ for all j, that is to say the map g_j is equal to the composite map

$$V_j \overset{h_j}{\to} U_{\sigma(j)} \overset{f_{\sigma(j)}}{\to} U$$

for some morphism h_j.

The map $\sigma : J \to I$ induces maps $\sigma^{(p)}$ for all $p \geq 0$

$$\sigma^{(p)} : \mathcal{C}^p(\mathcal{U}/U, \mathcal{P}) \to \mathcal{C}^p(\mathcal{V}/U, \mathcal{P}), \quad s = (s_{\mathbf{i}})_{\mathbf{i}\in I^{p+1}} \mapsto ((\sigma^{(p)} s)_{\mathbf{j}})_{\mathbf{j}\in J^{p+1}}$$
$$\text{where } (\sigma^{(p)} s)_{j_0 \ldots j_p} = \mathrm{res}_{h_{j_0}\times\ldots\times h_{j_p}}(s_{\sigma(j_0)\ldots\sigma(j_p)}).$$

The maps $\sigma^{(p)}$ commute with the coboundary maps d and hence induce homomorphisms on the cohomology

$$\rho^p(\mathcal{V}, \mathcal{U}, \sigma, \{h_j\}_{j\in J}) : \check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{P}) \to \check{H}^p_{[X'/X]}(\mathcal{V}/U, \mathcal{P}).$$

It is straightforward to show that the homomorphism

$$\rho^p(\mathcal{V}, \mathcal{U}) = \rho^p(\mathcal{V}, \mathcal{U}, \sigma, \{h_j\}_{j\in J})$$

is independent of the choices of maps σ and h_j and depends only on the coverings $\mathcal{V}$ and $\mathcal{U}$ of U (see [M2, Chap. III, Lemma 2.1]). Hence if $\mathcal{W}$ is a refinement of $\mathcal{V}$ we have

$$\rho^p(\mathcal{W}, \mathcal{U}) = \rho^p(\mathcal{W}, \mathcal{V}) \circ \rho^p(\mathcal{V}, \mathcal{U}).$$

(5.4.21) The Čech cohomology groups of the presheaf $\mathcal{P}$ over U are

$$\check{H}^p_{[X'/X]}(U,\mathcal{P}) = \varinjlim \check{H}^p_{[X'/X]}(\mathcal{U}/U,\mathcal{P})$$

where the limit is taken over all coverings $\mathcal{U}$ of U in $[X'/X]$.

(5.4.22) Suppose that $\mathcal{P}$ is a presheaf on the étale site $X_{\text{ét}}$. The Čech cohomology groups $\check{H}^p_{\text{ét}}(U,\mathcal{P})$ on the étale site $X_{\text{ét}}$ are defined to be (see [M2, Chap. III, §2])

$$\check{H}^p_{\text{ét}}(U,\mathcal{P}) = \varinjlim \check{H}^p_{\text{ét}}(\mathcal{U}/U,\mathcal{P})$$

where the limit is taken over all coverings $\mathcal{U}$ of U in the étale site $U_{\text{ét}}$.

5.4.23. Proposition. *The functors $\check{H}^p_{[X'/X]}(\mathcal{U}/U,-)$ and $\check{H}^p_{[X'/X]}(U,-)$ on the category* $\mathrm{Prsh}[X'/X]$ *are the right derived functors of $\check{H}^0_{[X'/X]}(\mathcal{U}/U,-)$ and $\check{H}^0_{[X'/X]}(U,-)$ for any U in $[X'/X]$ and any covering $\mathcal{U}$ of U in $[X'/X]$.*

Proof. The abelian category $\mathrm{Prsh}[X'/X]$ has enough injectives by proposition 5.4.14. Hence in order to prove this statement above, we have to show that these functors $\check{H}^p_{[X'/X]}(\mathcal{U}/U,-)$ and $\check{H}^p_{[X'/X]}(U,-)$ associate long exact sequences to short exact sequences in $\mathrm{Prsh}[X'/X]$ and that $\check{H}^p_{[X'/X]}(\mathcal{U}/U,-)$, for all $p \geq 1$, are zero on injective elements of the abelian category $\mathrm{Prsh}[X'/X]$.

The argument for the rest of this proof is similar to that of [M2, Chap. II, pp. 97-99]. Let

$$0 \to \mathcal{P}_1 \to \mathcal{P}_2 \to \mathcal{P}_3 \to 0$$

be an exact sequence of presheaves in $\mathrm{Prsh}[X'/X]$. Then the sequence of abelian groups

$$0 \to \mathcal{C}^p(\mathcal{U},\mathcal{P}_1) \to \mathcal{C}^p(\mathcal{U},\mathcal{P}_2) \to \mathcal{C}^p(\mathcal{U},\mathcal{P}_3) \to 0$$

is exact for all p as it is a product of exact sequences of abelian groups. We then obtain an exact sequence of Čech complexes

$$0 \to \{\mathcal{C}^p(\mathcal{U},\mathcal{P}_1), d^p\}_{p\in\mathbb{N}} \to \{\mathcal{C}^p(\mathcal{U},\mathcal{P}_2), d^p\}_{p\in\mathbb{N}} \to \{\mathcal{C}^p(\mathcal{U},\mathcal{P}_3), d^p\}_{p\in\mathbb{N}} \to 0.$$

The cohomology of these complexes therefore form a long exact sequence

$$0 \to \check{H}^0_{[X'/X]}(\mathcal{U}/U,\mathcal{P}_1) \to \check{H}^0_{[X'/X]}(\mathcal{U}/U,\mathcal{P}_2) \to \check{H}^0_{[X'/X]}(\mathcal{U}/U,\mathcal{P}_3) \to$$

$$\check{H}^1_{[X'/X]}(\mathcal{U}/U,\mathcal{P}_1) \to \dots$$

This long exact sequence remains exact when we take the direct limits over all coverings $\mathcal{U}$ of U in the site $[X'/X]$; hence we obtain the long exact sequence

of Čech cohomology

$$0 \to \check{H}^0_{[X'/X]}(U, \mathcal{P}_1) \to \check{H}^0_{[X'/X]}(U, \mathcal{P}_2) \to \check{H}^0_{[X'/X]}(U, \mathcal{P}_3) \to \check{H}^1_{[X'/X]}(U, \mathcal{P}_1) \dots$$

as required.

In the proof of proposition 5.4.14, for any object U in $[X'/X]$ we have constructed a presheaf $\mathbb{Z}_U$ in $\mathrm{Prsh}[X'/X]$ such that for any $\mathcal{Q}$ in $\mathrm{Prsh}[X'/X]$ we have

$$\mathrm{Hom}_X(\mathbb{Z}_U, \mathcal{Q}) \cong \Gamma(U, \mathcal{Q}).$$

Explicitly we have for any V in $[X'/X]$ that

$$\Gamma(V, \mathbb{Z}_U) = \bigoplus_{\mathrm{Hom}_X(V,U)} \mathbb{Z}.$$

But the sequence of presheaves formed from the covering $\mathcal{U}$ of U

$$\bigoplus_{\mathbf{i} \in I} \mathbb{Z}_{U(\mathbf{i})} \leftarrow \bigoplus_{\mathbf{i} \in I^2} \mathbb{Z}_{U(\mathbf{i})} \leftarrow \bigoplus_{\mathbf{i} \in I^3} \mathbb{Z}_{U(\mathbf{i})} \leftarrow \dots \tag{5.4.24}$$

is exact in $\mathrm{Prsh}[X'/X]$; this may be proved in identical fashion to the corresponding exact sequence at the foot of page 98 of [M2, Chapter III]. For the reader's convenience, we give the details. The property to be proved is that for all schemes V in $[X'/X]$ the sequence

$$\bigoplus_{\mathbf{i} \in I} \Gamma(V, \mathbb{Z}_{U(\mathbf{i})}) \leftarrow \bigoplus_{\mathbf{i} \in I^2} \Gamma(V, \mathbb{Z}_{U(\mathbf{i})}) \leftarrow \bigoplus_{\mathbf{i} \in I^3} \Gamma(V, \mathbb{Z}_{U(\mathbf{i})}) \leftarrow \dots \tag{5.4.25}$$

is exact. For any U-scheme W and any map $\phi \in \mathrm{Hom}_X(V, U)$ we write $\mathrm{Hom}_\phi(V, W)$ for the set of morphisms $\psi : V \to W$ such that the diagram

$$\begin{array}{ccc} V & \xrightarrow{\psi} & W \\ & {\scriptstyle\phi}\searrow \quad \swarrow & \\ & U & \end{array}$$

is commutative. We have for $\mathbf{i} = (i_0, \dots, i_r) \in I^{r+1}$

$$\mathrm{Hom}_X(V, U(\mathbf{i})) = \bigcup_{\phi \in \mathrm{Hom}_X(V,U)} \prod_{j=0}^{r} \mathrm{Hom}_\phi(V, U_{i_j}).$$

If we put

$$S(\phi) = \bigcup_i \mathrm{Hom}_\phi(V, U_i)$$

then we have

$$\bigcup_{i \in I^{r+1}} \mathrm{Hom}_X(V, U(\mathbf{i})) = \bigcup_{\phi \in \mathrm{Hom}_X(V,U)} S(\phi)^{r+1}.$$

Furthermore, $\bigoplus_{\mathbf{i}\in I^{r+1}} \Gamma(V, \mathbb{Z}_{U(\mathbf{i})})$ is the free abelian group on the set of generators $\bigcup_{\mathrm{Hom}_X(V,U)} S(\phi)^{r+1}$. Hence the complex (5.4.25) above may be written as

$$\bigoplus_{\phi\in \mathrm{Hom}_X(V,U)} \Big\{ \bigoplus_{S(\phi)} \mathbb{Z} \leftarrow \bigoplus_{S(\phi)^2} \mathbb{Z} \leftarrow \bigoplus_{S(\phi)^3} \mathbb{Z} \leftarrow \dots \Big\}.$$

The complex inside the parentheses is the standard complex associated to $\bigoplus_{S(\phi)} \mathbb{Z}$; that is to say, the coboundary map is given by

$$\big(\partial^{r+1}((m_{\mathbf{i}})_{\mathbf{i}\in S(\phi)^{r+1}})\big)_{\mathbf{j}} = \sum_{k=1}^{r+1} \sum_{(i_1\dots i_{k-1}\hat{i}_k i_{k+1}\dots i_{r+1})=\mathbf{j}} (-1)^k m_{i_1 i_2 \dots i_{r+1}}.$$

This standard complex is exact and a contracting homotopy for it is given by, where $\psi \in S(\phi)$ is some fixed element,

$$k_r : \bigoplus_{S(\phi)^r} \mathbb{Z} \to \bigoplus_{S(\phi)^{r+1}} \mathbb{Z}$$

$$\big(k_r(m_{\mathbf{i}})_{\mathbf{i}\in S(\phi)^r}\big)_{i_1 i_2 \dots i_{r+1}} = \begin{cases} m_{i_1\dots i_r} & \text{if } i_1 = \psi \\ 0 & \text{otherwise.} \end{cases}$$

This proves the exactness of the sequence (5.4.24).

Suppose that $\mathcal{P}$ is an injective presheaf in $\mathrm{Prsh}[X'/X]$. Applying the functor $\mathrm{Hom}_X(-, \mathcal{P})$ to this exact sequence (5.4.24) we obtain, as $\mathcal{P}$ is injective, the exact sequence

$$\mathrm{Hom}_X(\bigoplus_{\mathbf{i}\in I} \mathbb{Z}_{U(\mathbf{i})}, \mathcal{P}) \to \mathrm{Hom}_X(\bigoplus_{\mathbf{i}\in I^2} \mathbb{Z}_{U(\mathbf{i})}, \mathcal{P}) \to \mathrm{Hom}_X(\bigoplus_{\mathbf{i}\in I^3} \mathbb{Z}_{U(\mathbf{i})}, \mathcal{P}) \to \dots$$

But this is isomorphic to the Čech complex for $\mathcal{P}$ namely

$$\mathcal{C}^p(\mathcal{U}/U, \mathcal{P}) = \prod_{\mathbf{i}\in I^{p+1}} \Gamma(U(\mathbf{i}), \mathcal{P}) \cong \mathrm{Hom}_X(\bigoplus_{\mathbf{i}\in I^{p+1}} \mathbb{Z}_{U(\mathbf{i})}, \mathcal{P}).$$

Hence this Čech complex is exact and we obtain that $\check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{P}) = 0$ for all $p \geq 1$ as required. □

Comparison of Čech cohomology and derived functor cohomology

(5.4.26) Suppose that $\mathcal{P}$ is a presheaf on the étale site $X_{\text{ét}}$. If $\mathcal{U}$ is a covering of X in $[X'/X]$ then $\check{H}^p_{[X'/X]}(\mathcal{U}/X, \mathcal{P})$ evidently coincides with the Čech cohomology group $\check{H}^p_{\text{ét}}(\mathcal{U}/X, \mathcal{P})$ computed with the covering $\mathcal{U}$ in the étale site $X_{\text{ét}}$ [M2, Chap. III, §2].

The Čech cohomology groups

$$\check{H}^p_{[X'/X]}(X,\mathcal{P}) \quad \text{and} \quad \check{H}^p_{\text{ét}}(X,\mathcal{P})$$

do not in general coincide; for instance, if $X' = X$ then $H^p_{[X'/X]}(X,\mathcal{P}) = 0$ for all $p > 0$ and any presheaf $\mathcal{P}$ on $X_{\text{ét}}$ whereas $\check{H}^p_{\text{ét}}(X,\mathcal{P})$ may be non-zero for $p > 0$.

(5.4.27) The map $U \to \check{H}^p_{[X'/X]}(U,\mathcal{P})$ defines a presheaf of abelian groups on $[X'/X]$ which is written

$$\check{\mathcal{H}}^p_{[X'/X]}(\mathcal{P}).$$

(5.4.28) Let $\mathcal{S}$ be a sheaf of abelian groups on $[X'/X]$. Then the (usual) derived functor cohomology of $\mathcal{S}$ is denoted by (see proposition 5.4.13)

$$H^p_{[X'/X]}(X,\mathcal{S}).$$

Let $U \to X$ be an object of $[X'/X]$. Then

$$U \mapsto H^p_{[X'/X]}(U,\mathcal{S})$$

is a presheaf of abelian groups on $[X'/X]$ which is written

$$\mathcal{H}^p_{[X'/X]}(\mathcal{S}).$$

5.4.29. Proposition. *Let $U \to X$ be in $[X'/X]$ and let $\mathcal{U}$ be a covering of U in $[X'/X]$. Let $\mathcal{S}$ be a sheaf of abelian groups on $[X'/X]$. Then there is a spectral sequence*

$$\check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})) \quad \Rightarrow \quad H^{p+q}_{[X'/X]}(U,\mathcal{S})$$

and natural isomorphisms

$$\check{H}^p_{[X'/X]}(U,\mathcal{S}) \cong H^p_{[X'/X]}(U,\mathcal{S}) \text{ for all } p \geq 0.$$

Proof. For any sheaf $\mathcal{S}$ on $[X'/X]$ we have a natural isomorphism

$$\check{H}^0_{[X'/X]}(\mathcal{U}/U, \mathcal{H}^0_{[X'/X]}(\mathcal{S})) \cong H^0_{[X'/X]}(U,\mathcal{S})$$

as follows from the definitions. Let $\mathcal{I}$ be any sheaf on $[X'/X]$ which is injective in the category of sheaves on $[X'/X]$. As $\mathcal{I}$ is then injective in the category $\mathrm{Prsh}[X'/X]$, by proposition 5.4.23 we have

$$\check{H}^i_{[X'/X]}(\mathcal{U}/U,\mathcal{I}) = 0 \quad \text{for all } i > 0.$$

Hence we have

$$\check{H}^i_{[X'/X]}(\mathcal{U}/U, \mathcal{H}^0_{[X'/X]}(\mathcal{I})) = 0 \quad \text{for all } i > 0.$$

That is to say the functor $\mathcal{H}^0_{[X'/X]}(-)$ takes injective sheaves to presheaves which are acyclic for the functor

$$\check{H}^i_{[X'/X]}(\mathcal{U}/U, -).$$

As $\check{H}^i_{[X'/X]}(\mathcal{U}/U, -)$ are the right derived functors on $\mathrm{Prsh}[X'/X]$ of the functor $\check{H}^0_{[X'/X]}(\mathcal{U}/U, -)$, (see (5.4.23)), we may apply [M2, Appendix B, Theorem 1] to conclude the existence of the spectral sequence of composite functors stated in the proposition.

For the last part, it suffices to prove the isomorphism when U is a connected scheme in $[X'/X]$; for in general the scheme U is a disjoint union of such schemes. Hence by remark 5.4.6(i), there is a map of X-schemes $X' \to U$ which is a finite étale galois covering of U in the site $[X'/X]$ with galois group J, say. Furthermore, the map $X' \to U$ is a covering of U which is a final object in the category of all coverings of U in the site $[X'/X]$, where a morphism of coverings is a refinement (see (5.4.20)). Hence we have natural isomorphisms

$$\check{H}^p_{[X'/X]}(U, \mathcal{S}) \cong \varinjlim \check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{S})$$

$$\cong \check{H}^p_{[X'/X]}(X'/U, \mathcal{S}).$$

By the computation of [M2, Example 2.6, Chap. III], the Čech cohomology group $\check{H}^p_{[X'/X]}(X'/U, \mathcal{S})$ of this galois covering is naturally isomorphic to the group cohomology $H^p(J, \mathcal{S}(X'))$ of J where $\mathcal{S}(X')$ denotes the J-module of sections of the sheaf $\mathcal{S}$ over X'. By proposition 5.4.13, the derived functor cohomology group $H^p_{[X'/X]}(X'/U, \mathcal{S})$ is naturally isomorphic to $H^p(J, \mathcal{S}(X'))$. This proves that $\check{H}^p_{[X'/X]}(U, \mathcal{S})$ and $H^p_{[X'/X]}(U, \mathcal{S})$ are naturally isomorphic for all $p \geq 0$. □

5.4.30. Proposition. *Let $\mathcal{S}$ be an object of* $\mathrm{Sh}[X'/X]$. *Then we have*

$$\check{H}^p_{[X'/X]}(U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})) = 0 \quad \textit{for all } q > 0,\ p \geq 0,\ \textit{and all } U \textit{ in } [X'/X].$$

Proof. We may reduce immediately to the case where U is a connected scheme in $[X'/X]$. By remark 5.4.6(i), there is a morphism of X-schemes $X' \to U$ which is finite étale and galois. The covering $X' \to U$ is then a final object in the category of all coverings of U in $[X'/X]$. Hence we obtain isomorphisms for all $p, q \geq 0$

$$\check{H}^p_{[X'/X]}(U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})) \cong \check{H}^p_{[X'/X]}(X'/U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})).$$

Now the Čech complex $\{\mathcal{C}^p(X'/U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})), d^p\}_{p\in\mathbb{N}}$ is given by

$$\mathcal{C}^p(X'/U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})) = \prod_{\mathbf{i}\in I^{p+1}} \Gamma(X'(\mathbf{i}), \mathcal{H}^q_{[X'/X]}(\mathcal{S}))$$

where I is a set with 1 element and if $\mathbf{i} \in I^{p+1}$ we have

$$X'(\mathbf{i}) = X' \times_U X' \times_U \ldots \times_U X' (p+1 \text{ factors}).$$

But for $\mathbf{i} \in I^{p+1}$ we have the isomorphism

$$X'(\mathbf{i}) \cong \coprod_{\mathrm{Gal}(X'/U)^p} X'$$

where the disjoint union runs over all elements of the pth power of the galois group $\mathrm{Gal}(X'/U)$. Hence we obtain the isomorphisms

$$\Gamma(X'(\mathbf{i}), \mathcal{H}^q_{[X'/X]}(\mathcal{S})) \cong \prod_{\sigma\in\mathrm{Gal}(X'/U)^p} H^q_{[X'/X]}(X', \mathcal{S}) \cong 0 \quad \text{for all } q > 0$$

where we have $H^q_{[X'/X]}(X', \mathcal{S}) \cong 0$ for all $q > 0$ (by proposition 5.4.13). Hence the groups $\mathcal{C}^p(X'/U, \mathcal{H}^q_{[X'/X]}(\mathcal{S}))$ are zero for all $q > 0$ and all $p \geq 0$; hence the Čech complex $\{\mathcal{C}^p(X'/U, \mathcal{H}^q_{[X'/X]}(\mathcal{S})), d^p\}_{p\in\mathbb{N}}$ is zero for all $q > 0$, whence the result holds. □

Flabby sheaves on $[X'/X]$

5.4.31. Definition. A sheaf $\mathcal{S}$ of abelian groups on $[X'/X]$ is *flabby* if

$$H^i_{[X'/X]}(U, \mathcal{S}) = 0 \quad \text{for all } U \text{ in } [X'/X] \quad \text{and for all } i > 0.$$

This condition is equivalent to the $\mathbb{Z}[G]$-module $H^0_{[X'/X]}(X', \mathcal{S})$ corresponding to $\mathcal{S}$ being cohomologically trivial (see proposition 5.4.33(i) below and proposition 5.4.12).

[This corresponds to the notion of a flabby sheaf on the étale site; see [M2, Chap. III, Example 1.9].]

5.4.32. Proposition. *Let $\mathcal{S}$ be a sheaf of abelian groups on $[X'/X]$. Then $\mathcal{S}$ is flabby if and only if $\check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{S}) = 0$ for all $p > 0$, for any $U \to X$ in $[X'/X]$, and any covering $\mathcal{U}$ of U in $[X'/X]$.*

Proof. '⇒' As $\mathcal{S}$ is a flabby sheaf we have $\mathcal{H}^p_{[X'/X]}(\mathcal{S}) = 0$ for $p > 0$.

Hence the spectral sequence of proposition 5.4.29 shows that there are isomorphisms

$$\check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{S}) \cong H^p_{[X'/X]}(U, \mathcal{S}) = 0 \text{ for all } p > 0.$$

'$\Leftarrow$' For any U in $[X'/X]$, we have

$$\check{H}^p_{[X'/X]}(U, \mathcal{S}) = \varinjlim \check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{S}) \cong 0 \text{ for all } p > 0.$$

Hence we obtain from proposition 5.4.29 the isomorphisms

$$H^p_{[X'/X]}(U, \mathcal{S}) \cong \check{H}^p_{[X'/X]}(U, \mathcal{S}) \cong 0 \text{ for all } p > 0.$$

Hence $\mathcal{S}$ is a flabby sheaf on $[X'/X]$. □

5.4.33. Proposition. (i) *Let $\mathcal{M}$ be a sheaf on the site $[X'/X]$. Then $\mathcal{M}$ is a flabby sheaf if and only if the discrete G-module $H^0_{[X'/X]}(X', \mathcal{M})$ is cohomologically trivial.*
(ii) *If R is a commutative ring then the sheaf on the site $[X'/X]$ associated to the group algebra $R[G]$ is flabby.*

Proof. (i) That $M = H^0_{[X'/X]}(X', \mathcal{M})$ is cohomologically trivial means that for any subgroup J of G we have

$$H^i(J, M) = 0 \text{ for all } i > 0.$$

The galois cohomology of modules over $\mathbb{Z}[G]$ coincides with the cohomology of the corresponding sheaves on the site $[X'/X]$ (see proposition 5.4.13). Furthermore, from the equivalence of categories between the finite $\pi_1(X, \overline{x})$-sets and the finite étale coverings of X (see (5.4.3)), we obtain that M is cohomologically trivial if and only if for any scheme U in $[X'/X]$ which is a finite étale over X we have

$$H^i_{[X'/X]}(U, \mathcal{M}) \cong 0 \text{ for all } i \geq 1.$$

Hence M is cohomologically trivial if and only if the corresponding sheaf $\mathcal{M}$ is a flabby on $[X'/X]$.
(ii) The G-module $R[G]$ is cohomologically trivial as it is an induced module (see [CF, Chap. IV, §9]) whence the associated sheaf (see proposition 5.4.12) is flabby from the result of part (i) above. □

Filters on the site $[X'/X]$

(5.4.34) Let U be an object of $[X'/X]$ and let $\mathcal{U} = \{U_i \to U\}_{i \in I}$ be a covering of U in the site $[X'/X]$ where I is a set of indices. Let $\mathcal{P}$ be a presheaf in

$\mathrm{Prsh}[X'/X]$. The Čech complex

$$\mathcal{C}(\mathcal{U}/U, \mathcal{P}) = \{\mathcal{C}^p(\mathcal{U}/U, \mathcal{P}), d^p\}_{p\in\mathbb{N}}$$

is defined in (5.4.18) where

$$\mathcal{C}^p(\mathcal{U}/U, \mathcal{P}) = \prod_{i\in I^{p+1}} \Gamma(U(\mathbf{i}), \mathcal{P}).$$

(5.4.35) For each integer $p \geq 1$, let I^{p+1} be the set of $p+1$-tuples $(i_0, i_1, \ldots, i_p)$ of elements of I.

Let S be a subset of the integers $\{0, 1, 2, \ldots, p\}$. Denote by δ_S the map of sets

$$\delta_S : I^{p+1} \to I^{p+1-|S|}$$

where $\delta_S(\mathbf{i})$ is the element of $I^{p+1-|S|}$ obtained by deleting from $\mathbf{i} = (i_0, i_1, \ldots, i_p)$ the elements i_s for all $s \in S$.

If the set S is a singleton there are precisely $p+1$ deletion maps $I^{p+1} \to I^p$ of this form namely the maps, where we write $\delta_k = \delta_{\{k\}}$ for $k \in \{0, 1, 2, \ldots, p\}$,

$$\delta_k : I^{p+1} \to I^p, \quad \mathbf{i} \to \delta_k\mathbf{i}, \quad k = 0, \ldots, p,$$

given by

$$\mathbf{i} \mapsto (i_0, i_1, \ldots, i_{k-1}, i_{k+1}, \ldots, i_p).$$

(5.4.36) Let $C(I)$ be the category whose set of objects is

$$\bigcup_{p\geq 1}^{\infty} I^p$$

and if $\mathbf{i} \in I^p$ and $\mathbf{j} \in I^q$ then the set of morphisms $\mathrm{Morph}(\mathbf{i}, \mathbf{j})$, that is the arrows $\mathbf{i} \to \mathbf{j}$, is a finite set, possibly empty, of deletion maps

$$\mathrm{Morph}(\mathbf{i}, \mathbf{j}) = \{\delta_S \mid \delta_S(\mathbf{i}) = \mathbf{j},\ |S| = p - q,\ S \subseteq \{0, 1, 2, \ldots, p\}\}.$$

The category $C(I)$ is the category of finite sequences of elements of I where the morphisms are given by deletion of elements of sequences.

5.4.37. Definition. Let $\mathcal{A}$ be a full subcategory of $C(I)$. For each $p \geq 0$ let $\mathcal{A}_{p+1}$ denote the set of objects of the category $\mathcal{A}$ which lie in I^{p+1}. We assume that $\mathcal{A}$ satisfies the condition that for all integers $0 \leq k \leq p$ we have

$$\delta_k\mathcal{A}_{p+1} \subseteq \mathcal{A}_p.$$

A *filter* $\mathcal{F}$ with respect to $\mathcal{A}$ is a covariant functor

$$\mathcal{F} : \mathcal{A} \to [X'/X].$$

(5.4.38) Associated to the covering $\mathcal{U}/U$ in $[X'/X]$ is a *standard filter*

$$\mathcal{S} : C(I) \to [X'/X]$$

given by (see (5.4.18))

$$\mathbf{i} \mapsto U(\mathbf{i}) = U_{i_0} \times_U \ldots \times_U U_{i_p}$$

for every $p+1$-tuple $\mathbf{i} = (i_0, \ldots, i_p) \in I^{p+1}$. The morphisms of the category $C(I)$ become under the functor $\mathcal{S}$ the projection morphisms amongst the schemes $U(\mathbf{i})$.

(5.4.39) Let $\mathcal{A}, \mathcal{B}$ be full subcategories of $C(I)$ such that for all integers $0 \leq k \leq p$ we have

$$\delta_k \mathcal{A}_{p+1} \subseteq \mathcal{A}_p, \quad \delta_k \mathcal{B}_{p+1} \subseteq \mathcal{B}_p.$$

Let

$$\mathcal{F} : \mathcal{A} \to [X'/X], \quad \mathcal{G} : \mathcal{B} \to [X'/X]$$

be filters with respect to $\mathcal{A}, \mathcal{B}$, respectively.

The filter $\mathcal{F}$ is *subordinate* to $\mathcal{G}$ if $\mathcal{A}$ is a full subcategory of $\mathcal{B}$ and, denoting the restriction of the functor $\mathcal{G}$ to the subcategory $\mathcal{A}$ by $\mathcal{G}|_{\mathcal{A}}$, there is a natural transformation of functors

$$\tau : \mathcal{F} \to \mathcal{G}|_{\mathcal{A}}.$$

In particular, we say that the filter $\mathcal{F}$ is *subordinate to the covering* $\mathcal{U}/U$ if the restriction $\mathcal{S}_{\mathcal{A}}$ to the subcategory $\mathcal{A}$ of the standard filter $\mathcal{S} : C(I) \to \mathbf{Sch}/X$ which gives the covering $\mathcal{U}/U$ admits a natural transformation of functors $\tau : \mathcal{F} \to \mathcal{S}_{\mathcal{A}}$.

That is to say, the filter $\mathcal{F}$ with respect to $\mathcal{A}$ is *subordinate to the covering* $\mathcal{U}/U$ if for each $\mathbf{i} \in \mathcal{A}_{p+1}$ there is a morphism of X-schemes

$$\tau(\mathbf{i}) : \mathcal{F}(\mathbf{i}) \to U(\mathbf{i})$$

such that the diagram

$$\begin{array}{ccc} \mathcal{F}(\mathbf{i}) & \overset{\tau(\mathbf{i})}{\to} & U(\mathbf{i}) \\ \mathcal{F}(\delta_k) \downarrow & & \downarrow \mathcal{F}(\delta_k) \\ \mathcal{F}(\delta_k \mathbf{i}) & \overset{\tau(\delta_k \mathbf{i})}{\to} & U(\delta_k \mathbf{i}) \end{array}$$

is commutative for all k and all $\mathbf{i}$.

The standard filter $\mathcal{S}$ associated to the covering $\mathcal{U}/U$ is a final object in the category of filters subordinate to $\mathcal{U}/U$.

Čech cohomology with respect to a filter

(5.4.40) Let $\mathcal{P}$ be a presheaf in the category $\mathrm{Prsh}[X'/X]$. Let I be a set and let $\mathcal{F} : \mathcal{A} \to [X'/X]$ be a filter with respect to a full subcategory $\mathcal{A}$ of $C(I)$ which satisfies the condition that for all integers $0 \leq k \leq p$ we have

$$\delta_k \mathcal{A}_{p+1} \subseteq \mathcal{A}_p.$$

Put for all integers $p \geq 0$

$$\mathcal{C}^p(\mathcal{F}, \mathcal{P}) = \prod_{i \in \mathcal{A}_{p+1}} \Gamma(\mathcal{F}(\mathbf{i}), \mathcal{P}).$$

We have the restriction homomorphisms

$$\mathrm{res}(\delta_k|\mathbf{i}) : \Gamma(\mathcal{F}(\delta_k \mathbf{i}), \mathcal{P}) \to \Gamma(\mathcal{F}(\mathbf{i}), \mathcal{P}).$$

We then define a complex

$$\mathcal{C}(\mathcal{F}, \mathcal{P}) = \{\mathcal{C}^p(\mathcal{F}, \mathcal{P}), d^p\}_{p \in \mathbb{N}}$$

with the coboundary maps d^p

$$d^p : \mathcal{C}^p(\mathcal{F}, \mathcal{P}) \to \mathcal{C}^{p+1}(\mathcal{F}, \mathcal{P})$$

where the coboundary of the element

$$s = (s_{\mathbf{i}})_{\mathbf{i} \in \mathcal{A}_{p+1}} \in \mathcal{C}^p(\mathcal{F}, \mathcal{P})$$

is given by

$$(d^p s)_{\mathbf{i}} = \sum_{j=0}^{p+1} (-1)^j \mathrm{res}(\delta_j|\mathbf{i})(s_{\delta_j \mathbf{i}}).$$

It is immediately checked that $d^p \circ d^{p-1} = 0$ hence $\mathcal{C}(\mathcal{F}, \mathcal{P})$ is indeed a complex.

(5.4.41) The cohomology groups of the complex $\{\mathcal{C}^p(\mathcal{F}, \mathcal{P}), d^p\}_{p \in \mathbb{N}}$ are the Čech cohomology groups

$$\check{H}^p_{[X'/X]}(\mathcal{F}, \mathcal{P})$$

of the presheaf $\mathcal{P}$ on $[X'/X]$ with respect to the filter $\mathcal{F}$.

If $\mathcal{F}$ is subordinate to the covering $\mathcal{U}/U$ we sometimes write

$$\check{H}^p_{[X'/X]}(\mathcal{F} \backslash \mathcal{U}/U, \mathcal{P})$$

for the cohomology group $\check{H}^p_{[X'/X]}(\mathcal{F}, \mathcal{P})$.

(5.4.42) Let $\mathcal{A}$ and $\mathcal{B}$ be full subcategories of $C(I)$ as in (5.4.39). Let $\mathcal{F} : \mathcal{A} \to [X'/X]$ and $\mathcal{G} : \mathcal{B} \to [X'/X]$ be filters with respect to the subcategories $\mathcal{A}$ and $\mathcal{B}$ respectively. Suppose that $\mathcal{F}$ is subordinate to $\mathcal{G}$ and so that $\mathcal{A}$ is a full subcategory of $\mathcal{B}$. Then we have a natural transformation of functors $\tau : \mathcal{F} \to \mathcal{G}|_{\mathcal{A}}$. The morphisms of schemes $\tau(\mathbf{i}) : \mathcal{F}(\mathbf{i}) \to \mathcal{G}(\mathbf{i})$ induce homomorphisms of groups of sections

$$\begin{aligned} \mathcal{C}^p(\mathcal{G}, \mathcal{P}) &\to \mathcal{C}^p(\mathcal{F}, \mathcal{P}) \\ (s_{\mathbf{i}})_{\mathbf{i} \in \mathcal{B}_{p+1}} &\mapsto (\tau s_{\mathbf{i}})_{\mathbf{i} \in \mathcal{A}_{p+1}} \end{aligned}$$

These homomorphisms are composites of the form

$$\mathcal{C}^p(\mathcal{G}, \mathcal{P}) = \prod_{\mathbf{i} \in \mathcal{B}_{p+1}} \Gamma(\mathcal{G}(\mathbf{i}), \mathcal{P}) \to \prod_{\mathbf{i} \in \mathcal{A}_{p+1}} \Gamma(\mathcal{G}(\mathbf{i}), \mathcal{P}) \to$$

$$\prod_{\mathbf{i} \in \mathcal{A}_{p+1}} \Gamma(\mathcal{F}(\mathbf{i}), \mathcal{P}) = \mathcal{C}^p(\mathcal{F}, \mathcal{P})$$

and these homomorphisms are compatible with the differentials d^p.

These homomorphisms then provide a homomorphism of complexes

$$\{\mathcal{C}^p(\mathcal{G}, \mathcal{P}), d^p\}_{p \in \mathbb{N}} \to \{\mathcal{C}^p(\mathcal{F}, \mathcal{P}), d^p\}_{p \in \mathbb{N}}.$$

Then we obtain the natural homomorphisms of cohomology for all $p \geq 0$

$$\pi^p : \check{H}^p_{[X'/X]}(\mathcal{G}, \mathcal{P}) \to \check{H}^p_{[X'/X]}(\mathcal{F}, \mathcal{P}).$$

5.4.43. Remark. The functors

$$\mathcal{P} \mapsto \check{H}^p_{[X'/X]}(\mathcal{F}, \mathcal{P})$$

for $p \geq 1$ are not in general the derived functors of the functor $\mathcal{P} \mapsto \check{H}^0_{[X'/X]}(\mathcal{F}, \mathcal{P})$ on the category of presheaves $\mathrm{Prsh}[X'/X]$ (see (5.4.24) and the proof of proposition 5.4.23).

Alternating Čech cochains

(5.4.44) Let I be a set. Fix a well ordering $<$ of the set I. Let $C(I)^{\mathrm{alt}}$ be the full sub-category of $C(I)$ defined in the following way.

(a) For each integer $p \geq 0$, let $C(I)^{\mathrm{alt}}_{p+1}$ be the set of $p+1$-tuples $(i_0, i_1, \ldots, i_p)$, where $i_0 < i_1 < \ldots < i_p$ and $i_k \in I$ for all k.

(b) The set of objects of the category $C(I)^{\mathrm{alt}}$ is

$$\bigcup_{p \geq 0} C(I)^{\mathrm{alt}}_{p+1}.$$

(c) For $\mathbf{i} \in C(I)^{\mathrm{alt}}_{p+1}$ and $\mathbf{j} \in C(I)^{\mathrm{alt}}_{q+1}$, the set of morphisms $\mathrm{Morph}(\mathbf{i}, \mathbf{j})$ from $\mathbf{i}$ to $\mathbf{j}$ is a set of deletion maps

$$\mathrm{Morph}(\mathbf{i}, \mathbf{j}) = \{\delta_S \mid \delta_S(\mathbf{i}) = \mathbf{j},\ |S| = p - q,\ S \subseteq \{0, 1, 2, \ldots, p\}\}.$$

If $\mathbf{j}$ is a subsequence of $\mathbf{i}$ then $\mathrm{Morph}(\mathbf{i}, \mathbf{j})$ contains only one element denoted $\delta(\mathbf{i}, \mathbf{j})$ which is the unique "deletion map" from $\mathbf{i}$ to $\mathbf{j}$; if $\mathbf{j}$ is not a subsequence of $\mathbf{i}$ then $\mathrm{Morph}(\mathbf{i}, \mathbf{j})$ is the empty set.

The category $C(I)^{\mathrm{alt}}$ evidently satisfies the condition that for all integers $0 \leq k \leq p$ we have

$$\delta_k C(I)^{\mathrm{alt}}_{p+1} \subseteq C(I)^{\mathrm{alt}}_p.$$

The category $C(I)^{\mathrm{alt}}$ is the opposite category of the category of finite subsets of I with morphisms given by inclusion of subsets.

(5.4.45) Let $\mathcal{U} = \{f_i : U_i \to U\}_{i \in I}$ be a covering of U in $[X'/X]$. Fix a well ordering $<$ of the set I.

Let

$$\mathcal{S}^{\mathrm{alt}} : C(I)^{\mathrm{alt}} \to [X'/X]$$

be the filter subordinate to the covering $\mathcal{U}/U$ given by $\mathbf{i} \mapsto U(\mathbf{i})$. The complex associated to $\mathcal{S}^{\mathrm{alt}}$ is the complex of alternating cochains.

More precisely, let $\mathcal{P}$ be a presheaf of abelian groups on the site $[X'/X]$. The cohomology of the complex $\{\mathcal{C}^p(\mathcal{S}^{\mathrm{alt}} \backslash \mathcal{U}/U, \mathcal{P}), d^p\}_{p \in \mathbb{N}}$ is then the alternating Čech cohomology groups

$$\check{H}^p_{[X'/X]}(\mathcal{S}^{\mathrm{alt}} \backslash \mathcal{U}/U, \mathcal{P})$$

of the presheaf $\mathcal{P}$ on $[X'/X]$ with respect to the covering $\mathcal{U}$ of U.

(5.4.46) Let $\mathcal{C}^p_\sharp(\mathcal{U}/U, \mathcal{P})$ be the subgroup of alternating cochains of the Čech group of cochains $\mathcal{C}^p(\mathcal{U}/U, \mathcal{P})$ defined in the following way. If $(i_0, \ldots, i_p)$ is a $p+1$-tuple of distinct indices in I^{p+1} and σ is the permutation of the set $\{i_0, \ldots, i_p\}$ such that $\sigma i_0 < \sigma i_1 < \ldots < \sigma i_p$ then we fix an isomorphism

$$f_\sigma : \Gamma(U(\mathbf{i}), \mathcal{P}) \xrightarrow{\cong} \Gamma(U(\sigma \mathbf{i}), \mathcal{P}).$$

Then $\mathcal{C}^p_\sharp(\mathcal{U}/U, \mathcal{P})$ is the subgroup of cochains

$$s = (s_{\mathbf{i}})_{\mathbf{i}\in I^{p+1}} \in \mathcal{C}^p(\mathcal{U}/U, \mathcal{P})$$

such that if there is a repeated index in the set $\{i_0, \ldots, i_p\}$ then

$$s_{i_0 \ldots i_p} = 0$$

and if the indices are distinct then

$$f_\sigma(s_{i_0 \ldots i_p}) = \mathrm{sgn}(\sigma) s_{\sigma i_0, \sigma i_1, \ldots, \sigma i_p}$$

where σ is the permutation of the set $\{i_0, \ldots, i_p\}$ such that $\sigma i_0 < \sigma i_1 < \ldots < \sigma i_p$ and $\mathrm{sgn}(\sigma)$ denotes the signature $+1, -1$ of σ.

Define a differential

$$d^p_\sharp : \mathcal{C}^p_\sharp(\mathcal{U}/U, \mathcal{P}) \to \mathcal{C}^{p+1}_\sharp(\mathcal{U}/U, \mathcal{P})$$

via the formula

$$(d^p_\sharp s)_{\mathbf{i}} = \begin{cases} 0, & \text{if } \mathbf{i} \text{ contains repeated indices} \\ \sum_{j=0}^{p+1} (-1)^j \mathrm{res}(\delta_j|\mathbf{i})(s_{\delta_j \mathbf{i}}), & \text{if not.} \end{cases}$$

Then we have $d^p_\sharp \circ d^{p-1}_\sharp = 0$ for all p and hence $\{\mathcal{C}^p_\sharp(\mathcal{U}/U, \mathcal{P}), d^p_\sharp\}_{p\in\mathbb{N}}$ is a complex. The projection homomorphism

$$\mathcal{C}^p_\sharp(\mathcal{U}/U, \mathcal{P}) \to \mathcal{C}^p(\mathcal{S}^{\mathrm{alt}}\backslash\mathcal{U}/U, \mathcal{P})$$

given by

$$s = (s_{\mathbf{i}})_{\mathbf{i}\in I^{p+1}} \mapsto (s_{\mathbf{i}})_{\mathbf{i}\in C(I)^{\mathrm{alt}}_{p+1}}$$

induces an isomorphism on cohomology

$$H^p(\{\mathcal{C}^p_\sharp(\mathcal{U}/U, \mathcal{P}), d^p\}_{p\in\mathbb{N}}) \cong \check{H}^p_{[X'/X]}(\mathcal{S}^{\mathrm{alt}}\backslash\mathcal{U}/U, \mathcal{P}).$$

(5.4.47) Let $\mathcal{S}^{\mathrm{alt}}$ be the alternating filter subordinate to the covering $\mathcal{U}/U$ (see (5.4.45)). Let $\mathcal{P}$ be a presheaf on $[X'/X]$. Then there are natural homomorphisms for all $p \geq 0$

$$\pi^p : \check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{P}) \to \check{H}^p_{[X'/X]}(\mathcal{S}^{\mathrm{alt}}\backslash\mathcal{U}/U, \mathcal{P})$$

because $\mathcal{S}^{\mathrm{alt}}\backslash\mathcal{U}/U$ is subordinate to the standard filter associated to the covering $\mathcal{U}/U$ (see (5.4.42)).

(5.4.48) Let $\mathcal{F} : C(I)^{\mathrm{alt}} \to [X'/X]$ be a filter on $C(I)^{\mathrm{alt}}$ which is subordinate to the alternating filter $\mathcal{S}^{\mathrm{alt}}\backslash\mathcal{U}/U$ of the covering $\mathcal{U}/U$. Then we have natural homomorphisms for all $p \geq 0$ (see (5.4.42))

$$\check{H}^p_{[X'/X]}(\mathcal{S}^{\mathrm{alt}}\backslash\mathcal{U}/U, \mathcal{P}) \to \check{H}^p_{[X'/X]}(\mathcal{F}, \mathcal{P}).$$

Composing this with π^p (see (5.4.47)), we obtain natural homomorphisms for all $p \geq 0$

$$\rho^p : \check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{P}) \to \check{H}^p_{[X'/X]}(\mathcal{F}, \mathcal{P}).$$

5.4.49. Remark. The alternating Čech cohomology groups

$$\check{H}^p_{[X'/X]}(\mathcal{S}^{\mathrm{alt}} \backslash \mathcal{U}/U, \mathcal{P})$$

do not in general coincide with the Čech cohomology groups

$$\check{H}^p_{[X'/X]}(\mathcal{U}/U, \mathcal{P}).$$

For example, if I is a finite set with n elements then $\check{H}^p_{[X'/X]}(\mathcal{S}^{\mathrm{alt}} \backslash \mathcal{U}/U, \mathcal{P}) = 0$ for all $p > n$. [See also [M2, Chap. III, Remark 2.2(d)]].

5.5 Group rings and Čech cohomology

For this section, we shall write finite groups multiplicatively. All modules over the group algebra $\mathbb{Z}[G]$ of a finite group G will be *left* modules.

In this section we apply Čech cohomology of a filter (see §5.4) to group rings. The main result that is applied to the Heegner module is corollary 5.5.30. This corollary is a special case of a more general result proposition 5.5.19 on the vanishing of Čech cohomology and Čech homology for group algebras relative to *admissible* families of subgroups (definition 5.5.18).

Explicit form of Čech galois cohomology

(5.5.1) Let

G be a finite group;
$H_0, \ldots, H_{n-1}$ be normal subgroups of G;
X be a connected quasi-compact locally noetherian scheme;
$\overline{x} \to X$ be a geometric point of X;
X' be a connected finite galois covering of X with galois group G;
$[X'/X]$ be the site defined in (5.4.5) and (5.4.10);
I be the finite set of integers $\{0, 1, \ldots, n-1\}$ with its usual well-ordering $<$ of the elements;
U_i be the scheme in $[X'/X]$ for all i such that $\mathrm{Gal}(X'/U_i) = H_i$ for all i;
R be a commutative ring.

As G is the galois group of the finite galois connected covering X'/X then G is a quotient of the Grothendieck fundamental group $\pi_1(X, \overline{x})$ by an open subgroup. Hence under the equivalence of categories between $\mathbf{FEt}/X$ and $\pi_1(X, \overline{x}) - \mathbf{sets}$ (see (5.4.3) and [M2, Chap. 1, §5]), the category $[X'/X]$ is equivalent to the category of all finite sets equipped with an action by the group G. Hence it is clear that the schemes U_i in $[X'/X]$ exist such that $U_i \to X$ is galois with galois group $\mathrm{Gal}(U_i/X) = G/H_i$.

(5.5.2) We have that

$$\mathcal{U} = \{U_i \to X\}_{i \in I}$$

is a covering of X in the site $[X'/X]$, for each morphism $U_i \to X$ is finite étale and surjective.

For $\mathbf{i} = (i_0, \ldots, i_p) \in I^{p+1}$, we have, with the notation of §5.4,

$$U(\mathbf{i}) \ = U_{i_0} \times_X \ldots \times_X U_{i_p}.$$

Furthermore, $U(\mathbf{i})$ is galois scheme over X with galois group

$$\mathrm{Gal}(U(\mathbf{i})/X) = \prod_{r=0}^{p} \mathrm{Gal}(U_{i_r}/X)$$

which is the direct product of the groups G/H_{i_r}.

(5.5.3) For all $\mathbf{i} = (i_0, \ldots, i_p) \in I^{p+1}$ let $H(\mathbf{i})$ be the normal subgroup $\bigcap_{j=0}^{p} H_{i_j}$ of G. Then under the equivalence of categories between $\mathbf{FEt}/X$ and $\pi_1(X, \overline{x}) - \mathbf{sets}$, it is clear that there is a scheme $E(\mathbf{i})$ in $[X'/X]$ such that $E(\mathbf{i})/X$ is galois with galois group

$$\mathrm{Gal}(E(\mathbf{i})/X) = \frac{G}{\bigcap_{j=0}^{p} H_{i_j}}.$$

The scheme $U(\mathbf{i})$ is a disjoint union of copies of the scheme $E(\mathbf{i})$. We may then choose for all $\mathbf{i}$ a morphism of X-schemes

$$f_{\mathbf{i}} : E(\mathbf{i}) \to U(\mathbf{i}).$$

(5.5.4) Let $C(I)^{\mathrm{alt}}$ be the alternating subcategory of $C(I)$ (see (5.4.44)). Let

$$\mathcal{F} : C(I)^{\mathrm{alt}} \to [X'/X]$$

be the filter given on objects by

$$\mathbf{i} \mapsto E(\mathbf{i}).$$

and where the morphisms of $C(I)^{\mathrm{alt}}$ are transformed by $\mathcal{F}$ to the morphisms of X-schemes $E(\mathbf{i}) \to E(\mathbf{j})$ if $\mathbf{j}$ is a subsequence of $\mathbf{i}$ (see (5.4.44) and (5.4.45)).

The filter $\mathcal{F}$ is subordinate to the standard alternating filter $\mathcal{S}^{\mathrm{alt}}$ with respect to the covering $\mathcal{U}/X$. The natural transformation $\tau : \mathcal{F} \to \mathcal{S}^{\mathrm{alt}}$ is given by the morphisms $f_{\mathbf{i}} : E(\mathbf{i}) \to U(\mathbf{i})$ for all objects $\mathbf{i}$ of $C(I)^{\mathrm{alt}}$.

(5.5.5) Let M be a $\mathbb{Z}[G]$-module. Then M defines a sheaf $\mathcal{M}$ of abelian groups on the site $[X'/X]$ (proposition 5.4.12).

In particular, we have for $\mathbf{i} = (i_0, i_1, \ldots, i_p) \in I^{p+1}, i_0 < i_1 < \ldots < i_p$,

$$\Gamma(E(\mathbf{i}), \mathcal{M}) = M^{\mathrm{Gal}(X'/E(\mathbf{i}))} = M^{\bigcap_{j=0}^{p} H_{i_j}}.$$

(5.5.6) The Čech complex with coefficients in $\mathcal{M}$ of the filter $\mathcal{F} : C(I)^{\mathrm{alt}} \to [X'/X]$ takes the form

$$\mathcal{C}^p(\mathcal{F}, \mathcal{M}) = \prod_{\substack{\mathbf{i} \in I^{p+1} \\ i_0 < i_1 < \ldots < i_p}} \Gamma(E(\mathbf{i}), \mathcal{M}) = \prod_{\substack{\mathbf{i} \in I^{p+1} \\ i_0 < i_1 < \ldots < i_p}} M^{\bigcap_{j=0}^{p} H_{i_j}}$$

and

$$d^p : \mathcal{C}^p(\mathcal{F}, \mathcal{M}) \to \mathcal{C}^{p+1}(\mathcal{F}, \mathcal{M})$$

is the coboundary homomorphism defined by

$$s = (s_{\mathbf{i}})_{\mathbf{i} \in C(I)^{\mathrm{alt}}_{p+1}} \in \mathcal{C}^p(\mathcal{F}, \mathcal{M})$$

$$(d^p s)_{\mathbf{i}} = \sum_{j=0}^{p+1} (-1)^j s_{\delta_j \mathbf{i}}$$

as the restriction maps $\mathrm{res}(\delta_k|\mathbf{i})$ (see (5.4.40)) are here injections arising from the inclusions

$$M^{\mathrm{Gal}(X'/E(\delta_j \mathbf{i}))} \subseteq M^{\mathrm{Gal}(X'/E(\mathbf{i}))}.$$

Put for all $i = 0, \ldots, n-1$

$$G_i = \bigcap_{\substack{0 \le j \le n-1 \\ j \ne i}} H_j.$$

The groups G_i are normal subgroups of G.

5.5.7. Proposition. *For any $R[G]$-module M with corresponding sheaf $\mathcal{M}$ on $[X'/X]$, we have:*
(i) $\check{H}^0_{[X'/X]}(\mathcal{F},\mathcal{M}) \cong M^{H_0H_1\dots H_{n-1}}$.
(ii) $\check{H}^{n-2}_{[X'/X]}(\mathcal{F},\mathcal{M}) = 0$ *if and only if the following sequence of R-modules is exact*

$$\prod_{\substack{\mathbf{i}\in I^{n-2}\\ i_0<i_1<\dots<i_{n-3}}} M^{\bigcap_{j=0}^{n-3} H_{i_j}} \overset{d^{n-3}}{\to} \prod_{i=0}^{n-1} M^{G_i} \overset{d^{n-2}}{\to} M^{\bigcap_{j=0}^{n-1} H_j}.$$

(iii) $\check{H}^{n-1}_{[X'/X]}(\mathcal{F},\mathcal{M}) \cong M^{\bigcap_{j=0}^{n-1} H_j} / \sum_{i=0}^{n-1} M^{G_i}$.

Proof. (i) The Čech complex $\{\mathcal{C}^p(\mathcal{F},\mathcal{M}), d^p\}_{p\geq 0}$ begins with the terms for $p = 0, 1$ where we have explicitly

$$\mathcal{C}^0(\mathcal{F},\mathcal{M}) = \prod_{i_0\in I} M^{H_{i_0}} \quad \text{and} \quad \mathcal{C}^1(\mathcal{F},\mathcal{M}) = \prod_{\substack{(i_0,i_1)\in I^2\\ i_0<i_1}} M^{H_{i_0}\cap H_{i_1}}.$$

The differential $d^0 : \mathcal{C}^0(\mathcal{F},\mathcal{M}) \to \mathcal{C}^1(\mathcal{F},\mathcal{M})$ is given by

$$(d^0 s)_{i_0,i_1} = s_{i_1} - s_{i_0}.$$

Let $s = (s_i)_{i\in I} \in \mathcal{C}^0(\mathcal{F},\mathcal{M}) = \prod_{i\in I} M^{H_i}$; then $d^0 s = 0$ if and only if $s_{i_0} = s_{i_1}$ for all $i_0, i_1 \in I$. Hence the kernel of d^0 is the submodule $M^{H_0H_1\dots H_{n-1}}$ embedded diagonally in $\prod_{i\in I} M^{H_i}$, as required.
(ii) and (iii). The Čech complex $\{\mathcal{C}^p(\mathcal{F},\mathcal{M}), d^p\}_{p\geq 0}$ ends with the terms

$$\dots \quad \mathcal{C}^{n-3}(\mathcal{F},\mathcal{M}) \overset{d^{n-3}}{\to} \mathcal{C}^{n-2}(\mathcal{F},\mathcal{M}) \overset{d^{n-2}}{\to} \mathcal{C}^{n-1}(\mathcal{F},\mathcal{M}) \overset{d^{n-1}}{\to} \mathcal{C}^n(\mathcal{F},\mathcal{M}) = 0.$$

We have explicitly

$$\mathcal{C}^{n-3}(\mathcal{F},\mathcal{M}) = \prod_{\substack{\mathbf{i}\in I^{n-2}\\ i_0<i_1<\dots<i_{n-3}}} M^{\bigcap_{j=0}^{n-3} H_{i_j}}, \qquad \mathcal{C}^{n-2}(\mathcal{F},\mathcal{M}) = \prod_{i=0}^{n-1} M^{G_i}$$

$$\mathcal{C}^{n-1}(\mathcal{F},\mathcal{M}) = M^{\bigcap_{j=0}^{n-1} H_j}, \qquad \mathcal{C}^n(\mathcal{F},\mathcal{M}) = 0.$$

The stated results follow from this. □

Vanishing of the group $\check{H}^{n-1}_{[X'/X]}(\mathcal{F},\mathcal{M})$ when G is abelian

(5.5.8) Put

$$H_\infty = \bigcap_{j=0}^{n-1} H_j$$

and

$$G_i = \bigcap_{\substack{0 \le j \le n-1 \\ j \ne i}} H_j \quad \text{for all } i.$$

5.5.9. Proposition. *Suppose the group G is abelian. Let $\mathcal{M}$ be the sheaf on $[X'/X]$ associated to the group algebra $R[G]$. Then we have*

$$\check{H}^{n-1}_{[X'/X]}(\mathcal{F}, \mathcal{M}) = 0$$

if and only if for every residue field characteristic $p \ge 0$ of a maximal ideal of R and every subgroup J of G such that $J \supseteq H_\infty$ and G/J is cyclic of order prime to p there is i such that $G_i \subseteq J$ and $|G_i/H_\infty|$ is prime to p.

Proof. We have by proposition 5.5.7(iii) that

$$\check{H}^{n-1}_{[X'/X]}(\mathcal{F}, \mathcal{M}) = 0$$

if and only if

$$R[G]^{H_\infty} = \sum_{j=0}^{n-1} R[G]^{G_j}.$$

As $R[G]^{H_\infty} \cong R[G/H_\infty]$, we obtain that $\check{H}^{n-1}_{[X'/X]}(\mathcal{F}, \mathcal{M}) = 0$ if and only if

$$R[G/H_\infty] = \sum_{j=0}^{n-1} R[G/H_\infty]^{G_j/H_\infty}.$$

Hence we may reduce to the case where $H_\infty = \{1\}$.

The proof of the proposition is now the combination of the statements I,II,III below.

(I) If $\mathfrak{M}$ is a maximal ideal of $R[G]$ and H is the kernel of the induced group homomorphism $G \to \kappa(\mathfrak{M})^*$ then G/H is cyclic of order prime to the characteristic of $\kappa(\mathfrak{m})$ where $\mathfrak{m} = R \cap \mathfrak{M}$.

For the proof, let $\mathfrak{M}$ be a maximal ideal of $R[G]$. Then $\mathfrak{m} = \mathfrak{M} \cap R$ is a maximal ideal of R and the residue field $\kappa(\mathfrak{M})$ is a cyclotomic field extension of $\kappa(\mathfrak{m})$. Let p be the characteristic of $\kappa(\mathfrak{m})$. The images of the elements of G in $\kappa(\mathfrak{M})$ under the homomorphism $R[G] \to \kappa(\mathfrak{M})$ are roots of unity of order prime to p; furthermore, the image of G in $\kappa(\mathfrak{M})$ is a cyclic group of order prime to p. It follows that

$$H = \ker(G \to \kappa(\mathfrak{M})^*)$$

is a subgroup of G for which G/H is cyclic of order prime to p.

(II) Suppose that there is a maximal ideal $\mathfrak{m}$ of R and a subgroup H of G for which G/H is cyclic of order prime to the characteristic of the residue field $\kappa(\mathfrak{m})$. Then there is a maximal ideal $\mathfrak{M}$ of $R[G]$ such that $\mathfrak{M} \cap R = \mathfrak{m}$ and H is the kernel of the induced group homomorphism $G \to \kappa(\mathfrak{M})^*$.

Let n be the order of G/H. Then there is a primitive nth root of unity ζ in the separable closure of the field $\kappa(\mathfrak{m})$. Let L be the field $\kappa(\mathfrak{m})(\zeta)$. Let $g \in G$ be an element whose image in G/H generates the cyclic group G/H. Define a homomorphism of groups $f : G \to L^*$ via the recipe $g^r h \mapsto \zeta^r$, for all $r \in \mathbb{Z}$ and all $h \in H$. Then the kernel of f is equal to H and f extends to a homomorphism of R-algebras

$$f^\sharp : R[G] \to L, \quad g^r h \mapsto \zeta^r$$

which is a composite of the form $R[G] \to \kappa(\mathfrak{m})[G] \to L$. The kernel of $f^\sharp$ is a maximal ideal $\mathfrak{M}$ of $R[G]$ such that $\mathfrak{M} \cap R = \mathfrak{m}$ and $H = \ker(G \to \kappa(\mathfrak{M})^*)$.

(III) We have

$$\check{H}^{n-1}_{[X'/X]}(\mathcal{F}, \mathcal{M}) = 0$$

if and only if for every maximal ideal $\mathfrak{M}$ of $R[G]$ there is i such that $G_i \subseteq \ker(G \to \kappa(\mathfrak{M})^*)$ and the integer $|G_i|$ is not divisible by the characteristic of $\kappa(\mathfrak{M})$.

Put

$$e_i = \sum_{g \in G_i} g \quad \text{for all } i;$$

thus we have $e_i \in R[G]$ for all i and $e_i R[G] = R[G]^{G_i}$.

From the first part of the proof, we evidently have

$$\check{H}^{n-1}_{[X'/X]}(\mathcal{F}, \mathcal{M}) = 0$$

if and only if $\sum_{j=0}^{n-1} e_j R[G]$ is not contained in any maximal ideal of $R[G]$.

Let $\mathfrak{M}$ be a maximal ideal of $R[G]$ and H be the kernel of the induced group homomorphism $G \to \kappa(\mathfrak{M})^*$. Let p be the residue characteristic of $\mathfrak{M}$. We have $e_i \in \mathfrak{M}$ if and only if either that $G_i \not\subseteq H$ or that $G_i \subseteq H$ and $|G_i|$ is divisible by p. Hence we have

$$\mathfrak{M} + \sum_{i=0}^{n-1} e_i R[G] = \mathfrak{M} + \sum_{G_i \subseteq H} |G_i| R[G].$$

It follows that

$$\mathfrak{M} \supseteq \sum_{i=0}^{n-1} e_i R[G]$$

if and only if for all i the order $|G_i|$ is divisible by p whenever $G_i \subseteq H$, as required. □

Molecules and atoms

5.5.10. Definition. A finite family of subgroups $\{\Gamma_i\}_{i\in I}$ of G is a *molecule* if the subgroups

$$\Delta_i = \bigcap_{j\neq i} \Gamma_j, \quad \text{for all } i \in I,$$

satisfy the condition that for any finite subset S of I, where $S \neq I$, we have

$$< \{\Delta_i\}_{i\in I\setminus S} >= \bigcap_{j\in S} \Gamma_j$$

where $< \{\Delta_i\}_{i\in I\setminus S} >$ denotes the subgroup of G generated by Δ_i for all $i \in I \setminus S$.

The subgroups $\Delta_i, i \in I$, are the *atoms* of the molecule $\{\Gamma_i\}_{i\in I}$.

5.5.11. Examples. (i) If $\{\Gamma_i\}_{i\in I}$ is a molecule of G where the Γ_i are normal subgroups of G for all $i \in I$ then the atoms Δ_i of $\{\Gamma_i\}_{i\in I}$ are normal subgroups of G and we have

$$\prod_{i\in I\setminus S} \Delta_i = \bigcap_{j\in S} \Gamma_j$$

for any finite subset S of I, where $S \neq I$.

(ii) If the family of subgroups $\{\Gamma_i\}_{i\in I}$ of G satisfies $\Gamma_i = \Gamma_j$ for all i, j then $\{\Gamma_i\}_{i\in I}$ is a molecule whose atoms are equal to Γ_i for all i.

(iii) If $\{\Gamma_i\}_{i\in I}$ is a molecule of G and I' is a subset of I then $\{\Gamma_i\}_{i\in I'}$ is a molecule.

(iv) Suppose that G is vector space of dimension n over a field L and that $\{\Gamma_i\}_{i\in E}$ is a family of distinct codimension 1 subspaces of G where E is a finite set. Then the following conditions are equivalent, as may be checked,

(a) $\{\Gamma_i\}_{i\in E}$ is a molecule of G;
(b) $|E| \leq n$ and $\dim_L\big(\bigcap_{i\in S} \Gamma_i\big) = n - |S|$ for all finite subsets S of E;
(c) $|E| \leq n$ and $\dim_L\big(\bigcap_{i\in E} \Gamma_i\big) = n - |E|$;
(d) if $v_i \in \mathrm{Hom}_L(G, L)$ are elements of the dual space such that the kernel of v_i is equal to Γ_i for all $i \in E$, then the elements $\{v_i\}_{i\in E}$ are linearly independent.

(v) Let E be a finite set and $\Sigma(E)$ be the symmetric group of permutations of the elements of E. For $E' \subseteq E$ let $\Sigma(E')$ be the subgroup of $\Sigma(E)$ of permutations which fix all elements of $E \setminus E'$.

Fix an element $e \in E$ and let $I_0, \dots I_{n-1}$ be subsets of E such that

$$I_r \cap I_s = \{e\} \quad \text{for all } r \neq s, \quad \text{and} \quad |I_r| \geq 2 \quad \text{for all } r.$$

Put for all $r = 0, \dots, n-1$

$$J_r = \bigcup_{s \neq r} I_s.$$

Then $\{\Sigma(J_r)\}_{r=0,\dots,n-1}$ is a molecule of $\Sigma(E)$ whose atoms are the groups $\Sigma(I_r), r = 0, \dots, n-1$.

[For the proof, let S be a subset of $N = \{0, 1, \dots, n-1\}$ distinct from N. Put

$$\Sigma = \bigcap_{s \in S} \Sigma(J_s).$$

It is clear that

$$\bigcap_{s \in S} \Sigma(J_s) = \Sigma(\bigcap_{s \in S} J_s).$$

Furthermore, we have

$$\bigcap_{s \in S} J_s = \bigcup_{r \in N \setminus S} I_r.$$

Hence we obtain

$$\Sigma = \Sigma(\bigcup_{r \in N \setminus S} I_r).$$

The group $H =< \{\Sigma(I_r)\}_{r \in N \setminus S} >$ is a subgroup of Σ. The group H is generated by transpositions, as each group $\Sigma(I_r)$ is so generated, and H contains at least one transposition as $|\Sigma(I_r)| \geq 2$ for all r. Furthermore, the group H acts transitively on the set $\bigcup_{r \in N \setminus S} I_r$ as we have $I_r \cap I_s = \{e\}$ for all $r \neq s$. It follows that $H = \Sigma$ (by [S3, Lemma 1 p.139]); hence $\{\Sigma(J_r)\}_{r \in N}$ is a molecule of $\Sigma(E)$. As

$$\bigcap_{r \neq s} J_r = I_s, \quad \text{for all } s,$$

the atoms of $\{\Sigma(J_r)\}_{r \in N}$ are the groups $\Sigma(I_r), r \in N$, as required.]

The homology complex $\{C_j, d_j\}_{j\in\mathbb{N}}$

(5.5.12) Let I be the set of integers $\{0, 1, \ldots, n-1\}$. Let Γ be a finite group and $\Gamma_0, \ldots, \Gamma_{n-1}$ be normal subgroups of Γ. We write

$$\Gamma_{i_0 i_1 \ldots i_k}$$

for the normal subgroup of Γ given by the product

$$\Gamma_{i_0}\Gamma_{i_1}\ldots\Gamma_{i_k}.$$

(5.5.13) For any left $R[\Gamma]$-module N, and any integer j such that $0 \le j \le n-1$ let $C_j = C_j(\{\Gamma_i\}_{i\in I}, N)$ be the module

$$C_j(\{\Gamma_i\}_{i\in I}, N) = \prod_{\substack{0\le i_k<i_{k+1}\le n-1 \\ \text{for all } k}} N^{\Gamma_{i_0 i_1 \cdots i_j}}.$$

Put

$$C_j(\{\Gamma_i\}_{i\in I}, N) = 0 \quad \text{for all } j \ge n.$$

Put

$$C_{-1}(\{\Gamma_i\}_{i\in I}, N) = N^{\Gamma_0\cap\Gamma_1\cap\ldots\cap\Gamma_{n-1}}.$$

An element of C_j, for $0 \le j \le n-1$, is a family of elements $m = \{m^{(i_0\ldots i_j)}\}_{\substack{0\le i_k<i_{k+1}\le n-1 \\ \text{for all } k}}$ where for all $i_0 < \ldots < i_j$

$$m^{(i_0\ldots i_j)} \in N^{\Gamma_{i_0 i_1 \cdots i_j}}.$$

Define the *lower numbering* of the element $m = \{m^{(i_0\ldots i_j)}\}_{\substack{0\le i_k<i_{k+1}\le n-1 \\ \text{for all } k}}$ of C_j, for $0 \le j \le n-1$, by

$$m_{k_0\ldots k_{n-j-2}} = m^{I\setminus\{k_0\ldots k_{n-j-2}\}}$$

for all $0 \le k_0 < k_1 < \ldots < k_{n-j-2} \le n-1$, where $I \setminus \{k_0 \ldots k_{n-j-2}\}$ denotes the $j+1$-tuple of elements $i_0 < i_1 < \ldots < i_j$ of I such that $i_r \ne k_s$ for all r, s.

(5.5.14) Define a differential d_j for all $j \ge 0$

$$d_j : C_j \to C_{j-1}$$

in terms of the lower numbering by the formula

$$(d_j(m))_{\mathbf{i}} = \sum_{k=0}^{n-j-1} (-1)^k m_{\delta_k \mathbf{i}}.$$

We put $d_j = 0$ for all $j \geq n$ and $d_0 : C_0 \to C_{-1}$ is defined by the previous formula where the group C_{-1} is equal to

$$C_{-1} = N^{\Gamma_0 \cap \Gamma_1 \cap \ldots \cap \Gamma_{n-1}}.$$

In particular, if $n = 1$ then $d_{-1} : N^{\Gamma_0} \to N^{\Gamma_0}$ is the identity map. It is easily checked that $d_j \circ d_{j+1} = 0$ for all j and hence $\{C_j, d_j\}_{j \in \mathbb{N}}$ is a homology complex.

(5.5.15) Let $\check{H}_j(\{\Gamma_i\}_i, N)$ be the homology of this complex, that is to say

$$\check{H}_j(\{\Gamma_i\}_i, N) = \mathrm{Ker}(d_j)/\mathrm{Im}(d_{j+1}).$$

This is defined for all $j \in \mathbb{N}$.

We evidently have that

$$R[\Gamma] - \mathbf{mod} \quad \to \quad R - \mathbf{mod}$$

$$N \mapsto \check{H}_j(\{\Gamma_i\}_i, N)$$

is a covariant functor from the category of $R[\Gamma]$-modules to the category of R-modules.

5.5.16. Proposition. *For any $R[\Gamma]$-module N we have*

$$\check{H}_{n-2}(\{\Gamma_i\}_{i \in I}, N) \cong 0 \quad \textit{if} \ \ n \geq 2$$

and

$$\check{H}_{n-1}(\{\Gamma_i\}_{i \in I}, N) \cong 0 \quad \textit{if} \ \ n \geq 1.$$

Proof. That part of the homology complex $\{C_j\}_j$ for $j = n-1, n-2, n-3$ is the short complex

$$N^{\Gamma_{01\ldots n-1}} \overset{d_{n-1}}{\to} \prod_{\substack{0 \leq i_k < i_{k+1} \leq n-1 \\ \text{for all } k}} N^{\Gamma_{i_0 i_1 \ldots i_{n-2}}} \overset{d_{n-2}}{\to} \prod_{\substack{0 \leq i_k < i_{k+1} \leq n-1 \\ \text{for all } k}} N^{\Gamma_{i_0 i_1 \ldots i_{n-3}}}$$

where, if $n = 2$, the last term $\prod_{\substack{0 \leq i_k < i_{k+1} \leq n-1 \\ \text{for all } k}} N^{\Gamma_{i_0 i_1 \ldots i_{n-3}}}$ is understood to be equal to $N^{\Gamma_0 \cap \Gamma_1 \cap \ldots \cap \Gamma_{n-1}}$. It is easily checked that this complex is exact in the middle (this is similar to the proof of proposition 5.5.7(i) by taking $H_i = \prod_{j \neq i} \Gamma_j$). Furthermore, the first homomorphism of this complex is clearly an injection, whence the result.□

5.5.17. Proposition. *Suppose that $\{H_i\}_{i\in I}$ is a molecule of G with atoms $\{G_i\}_{i\in I}$. For any $R[G]$-module M with associated sheaf $\mathcal{M}$ on the site $[X'/X]$, we then have an isomorphism of complexes, where $\mathcal{F}$ is the filter associated to $\{H_i\}_{i\in I}$ (as in (5.5.4))*

$$\{C_j(\{G_i\}_{i\in I}, M), d_j\} \cong \{\mathcal{C}^{n-2-j}(\mathcal{F}, \mathcal{M}), d^{n-2-j}\} \quad \text{for } 0 \le j < n-2.$$

In particular we have isomorphisms for all $j = 0, \dots, n-3$

$$\check{H}_j(\{G_i\}_i, M) \cong \check{H}^{n-2-j}_{[X'/X]}(\mathcal{F}, \mathcal{M}).$$

Proof. As the family $\{H_j\}_{j=0,\dots,n-1}$ is a molecule, for any finite subset S of I, where $S \neq I = \{0, \dots, n-1\}$, we have

$$\prod_{i\in I\setminus S} G_i = \bigcap_{j\in S} H_j.$$

The Čech complex of the filter $\mathcal{F} : C(I)^{\mathrm{alt}} \to [X'/X]$, as in (5.5.4), takes the form

$$\mathcal{C}^p(\mathcal{F}, \mathcal{M}) = \prod_{\substack{\mathbf{i}\in I^{p+1}\\ i_0<i_1<\dots<i_p}} \Gamma(E(\mathbf{i}), \mathcal{M}) = \prod_{\substack{\mathbf{i}\in I^{p+1}\\ i_0<i_1<\dots<i_p}} M^{\bigcap_{j=0}^{p} H_{i_j}}.$$

Hence we have

$$\mathcal{C}^p(\mathcal{F}, \mathcal{M}) = \prod_{\substack{\mathbf{i}\in I^{p+1}\\ i_0<i_1<\dots<i_p}} M^{\prod_{i\in I\setminus\{i_0,i_1,\dots,i_p\}} G_i}.$$

Hence the complex $C_j(\{G_i\}_{i\in I}, M)$ defining the homology group $\check{H}_j(\{G_i\}_{i\in I}, M)$, for $0 \le j < n-2$, is isomorphic to the Čech cohomology complex

$$\mathcal{C}^{n-3-j}(\mathcal{F}, \mathcal{M}) \to \mathcal{C}^{n-2-j}(\mathcal{F}, \mathcal{M}) \to \mathcal{C}^{n-1-j}(\mathcal{F}, \mathcal{M}) \to \dots.$$

We have then for all $0 \le j < n-2$ the isomorphisms for any $R[G]$-module M with associated sheaf $\mathcal{M}$ on $[X'/X]$

$$\check{H}_j(\{G_i\}_{i\in I}, M) \cong \check{H}^{n-2-j}_{[X'/X]}(\mathcal{F}, \mathcal{M}). \quad \square$$

Vanishing of the group $\check{H}^k_{[X'/X]}(\mathcal{F}, \mathcal{M})$ *for* $1 \leq k \leq n-2$

5.5.18. Definition. A family $\{G_i\}_{i\in I}$ of subgroups G_i of the group G is *admissible*, with respect to the ring R, if it satisfies the two conditions:

(i) G_i, for all $i \in I$, are normal subgroups of G which are pairwise central (i.e. for all $g \in G_i, h \in G_j$ where $i \neq j$ we have $gh = hg$).

(ii) the order of the kernel of the homomorphism

$$f : G_0 \times G_1 \times \ldots \times G_{n-1} \to G, \quad (g_0, \ldots, g_{n-1}) \mapsto g_0 g_1 \ldots g_{n-1}$$

is a unit in the ring R.

5.5.19. Proposition. *Suppose that the family* $\{G_i\}_{i\in I}$ *of subgroups of* G *is* R*-admissible. Then we have*

$$\check{H}_k(\{G_i\}_{i\in I}, R[G]) = 0 \quad \textit{for all} \quad k \geq 0.$$

The next corollary follows from propositions 5.5.17 and 5.5.19.

5.5.20. Corollary. *Suppose that*
(i) $\{H_j\}_{j\in I}$ *is a molecule of normal subgroups of* G *with atoms* $\{G_i\}_{i\in I}$*;*
(ii) *the family of subgroups* $\{G_i\}_{i\in I}$ *of* G *is* R*-admissible.*
Let $\mathcal{M}$ *be the sheaf on the site* $[X'/X]$ *corresponding to the module* $R[G]$*. Then we have*

$$\check{H}^k_{[X'/X]}(\mathcal{F}, \mathcal{M}) = 0 \quad \textit{for all} \quad 1 \leq k \leq n-2. \quad \square$$

Proof of proposition 5.5.19. Let G' be the subgroup of G generated by the atoms $G_0, \ldots, G_{n-1}$. Then G' is a normal subgroup of G and $\{G_i\}_{i\in I}$ is also an R-admissible family of subgroups of G'. As $R[G]$ is a finite free $R[G']$-module we then have

$$\check{H}_j(\{G_i\}_{i\in I}, R[G]) = 0$$

if and only if

$$\check{H}_j(\{G_i\}_{i\in I}, R[G']) = 0.$$

Hence we may reduce to the case where $G' = G$.

Put

$$G(n) = G_0 \times G_1 \times \ldots \times G_{n-1}.$$

Let K be the kernel of the group homomorphism $G(n) \to G$ given by

$$(g_0, \ldots, g_{n-1}) \mapsto g_0 g_1 \ldots g_{n-1}.$$

Put

$$e_K = \sum_{g \in K} g \ \in \ R[G(n)].$$

As $|K|$ is a unit of R (by (5.5.18)), the element $e_K/|K|$ belongs to $R[G(n)]$. Furthermore, $e_K/|K|$ is an idempotent of $R[G(n)]$ and we have an isomorphism of left $R[G(n)]$-modules

$$\frac{e_K}{|K|} R[G(n)] \cong R[G].$$

As $e_K/|K|$ is an idempotent, the module $R[G]$ is a direct factor of $R[G(n)]$ as a $R[G(n)]$-module.
We write M for $R[G(n)]$ as an $R[G(n)]$-module. As $\{G_i\}_{i \in I}$ is an R-admissible family of subgroups of $G(n)$ and as the module $R[G]$ is a direct summand of the $R[G(n)]$-module M, to prove the proposition it suffices to show that we have

$$\check{H}_j(\{G_i\}_{i \in I}, M) = 0 \ \text{ for all } j \geq 0.$$

Put for all $i \in I$

$$e_i = \sum_{g \in G_i} g;$$

then e_i is an element of $R[G(n)]$. Put

$$G(n-1) = G_1 \times G_2 \times \ldots \times G_{n-1}.$$

If $n = 1$ then the homology complex $C_j(\{G_i\}_{i \in I}, M)$ takes the form

$$\ldots 0 \ \overset{d_2}{\to} \ 0 \ \overset{d_1}{\to} \ M^{G_0} \ \overset{d_0}{\to} \ M^{G_0}$$

where d_0 is the identity (see (5.5.14)). Hence we have if $n = 1$ then

$$\check{H}_j(\{G_i\}_{i \in I}, M) \cong 0 \ \text{ for all } j \geq 0.$$

Hence the result is true for $n = 1$. We now prove the proposition by induction on n; the induction hypothesis is that for

$$J = \{1, 2, \ldots, n-1\} = I \setminus \{0\}$$

we have

$$\check{H}_j(\{G_i\}_{i \in J}, R[G(n-1)]) = 0 \ \text{ for all } j \geq 0.$$

As M is a finite free left $R[G(n-1)]$-module, this induction hypothesis is equivalent to

$$\check{H}_j(\{G_i\}_{i \in J}, M) = 0 \ \text{ for all } j \geq 0.$$

By proposition 5.5.16, we have

$$\check{H}_j(\{G_i\}_{i\in I}, M) = 0 \text{ for } j = n-1 \text{ and } n-2.$$

We now consider the group $\check{H}_j(\{G_i\}_{i\in I}, M)$ where $j \leq n-3$.

Let $\gamma : M \to M$ be the projection homomorphism of $R[G(n-1)]$-modules given by, where $g_i \in G_i$ for all i,

$$\begin{array}{rcll} \gamma : M & \to & M & \\ (g_0, \ldots, g_{n-1}) & \mapsto & e_0(g_0, g_2 \ldots, g_{n-1}) & \text{if } g_0 = 1 \\ (g_0, \ldots, g_{n-1}) & \mapsto & 0 & \text{if } g_0 \neq 1. \end{array}$$

Then the image of γ is the submodule $e_0 M$. Note that γ is *not* a homomorphism of $R[G(n)]$-modules. The homomorphism of $R[G(n-1)]$-modules

$$f = \mathrm{id} - \gamma : M \to M$$

has kernel equal to $e_0 M$.

As in (5.4.44), let $C(I)^{\mathrm{alt}}_{p+1}$ be the set of $p+1$-tuples $(i_0, \ldots, i_p)$ of elements of I such that $i_0 < i_1 < \ldots < i_p$; define similarly $C(J)^{\mathrm{alt}}_{p+1}$. A cycle in $\check{H}_j(\{G_i\}_{i\in I}, M)$ is given by an element of the kernel of

$$d_j : C_j(\{G_i\}_{i\in I}, M) \to C_{j-1}(\{G_i\}_{i\in I}, M).$$

Thus a homology class in $\check{H}_j(\{G_i\}_{i\in I}, M)$ is given by an element

$$m = (m_{\mathbf{i}})_{\mathbf{i}\in C(I)^{\mathrm{alt}}_{n-1-j}} \in C_j(\{G_i\}_{i\in I}, M)$$

such that for all $\mathbf{i} \in C(I)^{\mathrm{alt}}_{n-j}$

$$\sum_{k=0}^{n-1-j} (-1)^k m_{\delta_k \mathbf{i}} = 0.$$

We write

$$e(i_1, i_2, \ldots, i_m) = \prod_{k \neq i_1, i_2, \ldots, i_m} e_k.$$

We then have, for $\mathbf{i} \in C(I)^{\mathrm{alt}}_{n-1-j}$

$$m_{\mathbf{i}} \in e(\mathbf{i}) M.$$

as

$$m_{\mathbf{i}} \in N^{\Gamma_{I\setminus\{i_0 i_1 \ldots i_{n-2-j}\}}}.$$

We may write

$$m_{\mathbf{i}} = e(\mathbf{i}) y_{\mathbf{i}}$$

for all $\mathbf{i}$ where $y_{\mathbf{i}} \in M$. Then we have for all $\mathbf{i} \in C(I)^{\mathrm{alt}}_{n-j}$

$$\sum_{k=0}^{n-1-j} (-1)^k e(\delta_k \mathbf{i}) y_{\delta_k \mathbf{i}} = 0.$$

The map $f : M \to M$ has kernel $e_0 M$. In particular, we have

$$f(e(\mathbf{i})M) = 0$$

whenever $\mathbf{i} = (i_0, \ldots, i_m)$ satisfies $i_k \neq 0$ for all k. Under f, this system of equations becomes: for all $\mathbf{i} \in C(I)^{\mathrm{alt}}_{n-j}$

$$\sum_{k=0}^{n-1-j} (-1)^k f(e(\delta_k \mathbf{i}) y_{\delta_k \mathbf{i}}) = 0.$$

But $f(e(\delta_k \mathbf{i}) y_{\delta_k \mathbf{i}}) = 0$ unless $\delta_k \mathbf{i}$ contains 0. That is to say the only terms contributing to this sum $\sum_{k=0}^{n-1-j} (-1)^k f(e(\delta_k \mathbf{i}) y_{\delta_k \mathbf{i}})$ are those for which $\mathbf{i} = (0, i_1, i_2, \ldots, i_{n-1-j})$ and for which $k > 0$. That is to say the system becomes for all $\mathbf{i} = (0, \mathbf{j}) \in C(I)^{\mathrm{alt}}_{n-j}$, where $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-j-1}$, as f is $R[G(n-1)]$-linear

$$\sum_{k=1}^{n-1-j} (-1)^k e(\delta_k \mathbf{i}) f(y_{\delta_k \mathbf{i}}) = 0.$$

But this is a cycle $c = \{e(0, \mathbf{j}) f(y_{0,\mathbf{j}})\}_{\mathbf{j}}$ in $C_j(\{G_i\}_{i \in J}, M)$. By induction we assume that

$$\check{H}_j(\{G_i\}_{i \in J}, M) = 0.$$

Hence c is in the image of the map

$$d_{j+1} : C_{j+1}(\{G_i\}_{i \in J}, M) \to C_j(\{G_i\}_{i \in J}, M).$$

That is to say for all $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-2-j}$

$$c_{\mathbf{j}} = \sum_{k=0}^{n-3-j} (-1)^k g_{\delta_k \mathbf{j}}.$$

Hence we have for all $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-2-j}$

$$e(0, \mathbf{j}) f(y_{0,\mathbf{j}}) = \sum_{k=0}^{n-3-j} (-1)^k g_{\delta_k \mathbf{j}}$$

where

$$g_{\delta_k \mathbf{j}} \in e(0, \delta_k \mathbf{j}) M.$$

We may then write

$$g_{\delta_k \mathbf{j}} = e(0, \delta_k \mathbf{j}) p_{\delta_k \mathbf{j}}$$

for elements $p_{\delta_k \mathbf{j}} \in M$ and hence

$$e(0, \mathbf{j}) f(y_{0,\mathbf{j}}) = \sum_{k=0}^{n-3-j} (-1)^k e(0, \delta_k \mathbf{j}) p_{\delta_k \mathbf{j}}$$

But by definition of f we have

$$f(y_{\mathbf{i}}) = y_{\mathbf{i}} - e_0 x_{\mathbf{i}}$$

for all $\mathbf{i}$ where $x_{\mathbf{i}} \in M$. Hence we have for all $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-2-j}$

$$e(0, \mathbf{j}) y_{0,\mathbf{j}} = e_0 e(0, \mathbf{j}) x_{0,\mathbf{j}} + \sum_{k=0}^{n-3-j} (-1)^k e(0, \delta_k \mathbf{j}) p_{\delta_k \mathbf{j}}.$$

Put for all $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-2-j}$

$$n_{0,\mathbf{j}} = x_{0,\mathbf{j}}$$

and put for $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-1-j}$

$$n_{\mathbf{j}} = -p_{\mathbf{j}}.$$

This defines an element $\{e(\mathbf{i}) n_{\mathbf{i}}\}_{\mathbf{i}} \in C_j(\{G_i\}_{i \in I}, M)$. Then we have for all $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-2-j}$

$$e(0, \mathbf{j}) y_{0,\mathbf{j}} = \sum_{k=0}^{n-2-j} (-1)^k e(\delta_k(0, \mathbf{j})) n_{\delta_k(0,\mathbf{j})}.$$

That is to say for all $\mathbf{i} = (0, \mathbf{j}) \in C(I)^{\mathrm{alt}}_{n-1-j}$, where $\mathbf{j} \in C(J)^{\mathrm{alt}}_{n-2-j}$, we have

$$e(\mathbf{i}) y_{\mathbf{i}} = \sum_{k=0}^{n-2-j} (-1)^k e(\delta_k \mathbf{i}) n_{\delta_k \mathbf{i}}.$$

Suppose that $\mathbf{i} \in C(I)^{\mathrm{alt}}_{n-1-j}$ where $\mathbf{i} = (i_0, i_1, \ldots, i_{n-2-j})$. If $i_0 = 0$ then we have shown that $e(\mathbf{i}) y_{\mathbf{i}} = \sum_{k=0}^{n-2-j} (-1)^k e(\delta_k \mathbf{i}) n_{\delta_k \mathbf{i}}$. Suppose then that $i_0 > 0$. We put

$$\mathbf{h} = (0, \mathbf{j}) \in C(I)^{\mathrm{alt}}_{n-j} \quad \text{where} \quad \mathbf{j} = \mathbf{i} \in C(J)^{\mathrm{alt}}_{n-1-j}.$$

Then we have from this system of equations

$$\sum_{k=0}^{n-1-j} (-1)^k e(\delta_k \mathbf{l}) y_{\delta_k \mathbf{l}} = 0, \quad \text{for all } \mathbf{l} \in C(I)^{\mathrm{alt}}_{n-j},$$

that

$$e(\mathbf{j})y_{\mathbf{j}} + \sum_{k=1}^{n-1-j} (-1)^k e(\delta_k \mathbf{h}) y_{\delta_k \mathbf{h}} = 0.$$

Hence we have

$$e(\mathbf{j})y_{\mathbf{j}} = - \sum_{k=1}^{n-1-j} (-1)^k e(\delta_k \mathbf{h}) y_{\delta_k \mathbf{h}}$$

$$= - \sum_{k=1}^{n-1-j} (-1)^k \sum_{l=0}^{n-2-j} (-1)^l e(\delta_l \delta_k \mathbf{h}) n_{\delta_l \delta_k \mathbf{h}}.$$

Here in the double sum there is a cancellation of terms with $l > 0$ and there only remains the terms with $l = 0$. Hence we have

$$e(\mathbf{j})y_{\mathbf{j}} = - \sum_{k=1}^{n-1-j} (-1)^k e(\delta_0 \delta_k \mathbf{h}) n_{\delta_0 \delta_k \mathbf{h}}$$

$$= - \sum_{k=0}^{n-2-j} (-1)^{k+1} e(\delta_k \mathbf{j}) n_{\delta_k \mathbf{j}}.$$

That is to say we have

$$e(\mathbf{j})y_{\mathbf{j}} = \sum_{k=0}^{n-2-j} (-1)^k e(\delta_k \mathbf{j}) n_{\delta_k \mathbf{j}}.$$

This shows that the element $m \in C_j(\{G_i\}_{i\in I}, M)$ lies in the image of

$$d_{j+1} : C_{j+1}(\{G_i\}_{i\in I}, M) \to C_j(\{G_i\}_{i\in I}, M).$$

Hence we have

$$\check{H}_j(\{G_i\}_{i\in I}, M) = 0$$

as required. □

Universal exact sequences, universal submodules

5.5.21. Definition. (i) A submodule N of an R-module M is a *universal submodule* if for any R-algebra S the induced homomorphism of S-modules $N \otimes_R S \to M \otimes_R S$ is an injection.

(ii) Let

$$\ldots \quad A_3 \xrightarrow{f_3} A_2 \xrightarrow{f_2} A_1 \xrightarrow{f_1} A_0$$

be an exact sequence of R-modules. Then this sequence is *universally exact* if for any R-algebra S the sequence

$$\ldots \quad A_3 \otimes_R S \xrightarrow{f_3 \otimes 1} A_2 \otimes_R S \xrightarrow{f_2 \otimes 1} A_1 \otimes_R S \xrightarrow{f_1 \otimes 1} A_0 \otimes_R S$$

is exact.

5.5.22. Remarks. (i) Let N be an R-submodule of M. For N to be a universal submodule of M it is sufficient that M/N be a flat R-module or that N be a direct summand of M. The module N is a universal submodule of M if and only if for any R-algebra S the induced homomorphism

$$\mathrm{Tor}_1(M/N, S) \to N \otimes_R S$$

is zero.

The zero submodule and M are both universal submodules of M.

(ii) Let

$$\ldots \quad A_3 \xrightarrow{f_3} A_2 \xrightarrow{f_2} A_1 \xrightarrow{f_1} A_0$$

be an exact sequence of R-modules. Then this sequence is universally exact if and only if $A_i/f_{i+1}(A_{i+1})$ is a universal submodule of A_{i-1} for all $i \geq 1$.

(iii) Let

$$\ldots \xrightarrow{f_4} M_3 \xrightarrow{f_3} M_2 \xrightarrow{f_2} M_1$$

be a universally exact sequence of R-modules. Let M_0 be the cokernel of $f_2 : M_2 \to M_1$ and let $f_1 : M_1 \to M_0$ be the natural surjection. Then

$$\ldots \xrightarrow{f_4} M_3 \xrightarrow{f_3} M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_0 \to 0 \tag{5.5.23}$$

is a universally exact sequence of R-modules.

[For the proof, let S be an R-algebra. By remark (ii) above, to show that the augmented sequence

$$\ldots \xrightarrow{f_4} M_3 \xrightarrow{f_3} M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_0 \xrightarrow{f_0} 0$$

is universally exact it suffices to show that $M_1/f_2(M_2) = M_0$ is a universal submodule of M_0 and that $f_0(M_0) = 0$ is a universal submodule of 0. But this is the case by remark (i) above.]

Corollaries of proposition 5.5.19

5.5.24. Corollary. *Suppose that $\{G_i\}_{i\in I}$ is an R-admissible family of subgroups of G. Put*

$$G_\infty = \bigcap_{j=0}^{n-1} G_j.$$

Then we have the universal exact sequence

(5.5.25)

$$0 \to R[G]^{G_0G_1\dots G_{n-1}} \to \prod_{i_0\in I} R[G]^{\prod_{j\neq i_0} G_j} \to \prod_{\substack{(i_0,i_1)\in I^2\\ i_0<i_1}} R[G]^{\prod_{j\neq i_0,i_1} G_j} \to \dots$$

$$\dots \prod_{\substack{(i_0,\dots,i_p)\in I^{p+1}\\ i_0<i_1<\dots<i_p}} R[G]^{\prod_{j\neq i_0,i_1,\dots,i_p} G_j} \dots \to \prod_{i\in I} R[G]^{G_i} \to$$

$$R[G]^{G_\infty} \to \frac{R[G]^{G_\infty}}{\sum_{i\in I} R[G]^{G_i}} \to 0.$$

Furthermore, $\sum_{i\in I} R[G]^{G_i}$ is a flat R-module.

Proof. Write $\mathcal{G}$ for $\{G_i\}_{i\in I}$. Let S be an R-algebra. For any $\mathbb{Z}[G]$-module M, let $C_k(\mathcal{G}, M)$ be the homology complex defined in (5.5.13).

For any normal subgroup H of G, we have natural isomorphisms of $S[G]$-modules

$$(R[G]^H) \otimes_R S \cong S[G]^H.$$

All chain groups $C_k(\mathcal{G}, R[G])$ are direct products of modules of the form $R[G]^H$ where H runs over a set of subgroups of G. Hence we have isomorphisms of complexes

$$\{C_j(\mathcal{G}, R[G]), d_j\}_{j\geq -1} \otimes_R S \cong \{C_j(\mathcal{G}, S[G]), d_j\}_{j\geq -1}.$$

As $\{G_i\}_{i\in I}$ is an R-admissible family of subgroups of G, it follows that the family $\{G_i\}_{i\in I}$ is S-admissible. By proposition 5.5.19, the homology of the complex $C_k(\mathcal{G}, S[G])$ satisfies $\check{H}_k(\mathcal{G}, S[G]) = 0$ for all $k \geq 0$. Hence the complex $\{C_k(\mathcal{G}, S[G]), d_k\}_{k\in\mathbb{N}}$ for $k \geq 0$ and where $C_p(\mathcal{G}, S[G]) = 0$ for all $p > n-1$, becomes an exact sequence of S-modules

$$0 \to C_{n-1}(\mathcal{G}, S[G]) \to C_{n-2}(\mathcal{G}, S[G]) \to C_{n-3}(\mathcal{G}, S[G]) \to \dots$$

$$\dots \to C_0(\mathcal{G}, S[G]) \to \check{H}_{-1}(\mathcal{G}, S[G]) \to 0.$$

This exact sequence is isomorphic to

$$0 \to C_{n-1}(\mathcal{G}, R[G]) \otimes_R S \to C_{n-2}(\mathcal{G}, R[G]) \otimes_R S \to C_{n-3}(\mathcal{G}, R[G]) \otimes_R S \to \dots$$

$$\dots \to C_0(\mathcal{G}, R[G]) \otimes_R S \to \check{H}_{-1}(\mathcal{G}, S[G]) \to 0.$$

Hence the sequence of R-modules

$$0 \to C_{n-1}(\mathcal{G}, R[G]) \to C_{n-2}(\mathcal{G}, R[G]) \to C_{n-3}(\mathcal{G}, R[G]) \to \dots$$

$$\dots \to C_1(\mathcal{G}, R[G]) \stackrel{d_1}{\to} C_0(\mathcal{G}, R[G])$$

is universally exact. The cokernel of the homomorphism d_1 here is (see (5.5.15))

$$\check{H}_{-1}(\mathcal{G}, R[G]) = R[G]^{G_\infty} / \sum_{i \in I} R[G]^{G_i}.$$

It follows from remark 5.5.22(iii) that the sequence of R-modules

$$0 \to C_{n-1}(\mathcal{G}, R[G]) \to C_{n-2}(\mathcal{G}, R[G]) \to C_{n-3}(\mathcal{G}, R[G]) \to \dots \tag{5.5.26}$$

$$\dots \to C_0(\mathcal{G}, R[G]) \to \check{H}_{-1}(\mathcal{G}, R[G]) \to 0$$

is universally exact and furthermore that there is an isomorphism of S-modules

$$\check{H}_{-1}(\mathcal{G}, R[G]) \otimes_R S \cong \check{H}_{-1}(\mathcal{G}, S[G]).$$

The definition of the chain groups $C_j(\mathcal{G}, R[G])$ as direct products of modules of the form $R[G]^H$ where H runs over a set of subgroups of G (see (5.5.13)) combined with the exact sequence (5.5.26) gives the exact sequence (5.5.25), as required.

The image of the homomorphism $\prod_{i \in I} R[G]^{G_i} \to R[G]^{G_\infty}$ from the exact sequence (5.5.25) is precisely the submodule $\sum_{i \in I} R[G]^{G_i}$. Hence we may shorten this universally exact sequence to the universally exact sequence of R-modules, by remark 5.5.22(iii),

(5.5.27)

$$0 \to R[G]^{G_0 G_1 \dots G_{n-1}} \to \prod_{i_0 \in I} R[G]^{\prod_{j \neq i_0} G_j} \to \prod_{\substack{(i_0, i_1) \in I^2 \\ i_0 < i_1}} R[G]^{\prod_{j \neq i_0, i_1} G_j} \to \dots$$

$$\dots \to \prod_{i \in I} R[G]^{G_i} \to \sum_{i \in I} R[G]^{G_i} \to 0.$$

This is a resolution of $\sum_{i \in I} R[G]^{G_i}$ by finite free R-modules; hence tensoring this universally exact free resolution (5.5.27) with $- \otimes_R S$ for any R-algebra S we obtain that

$$\mathrm{Tor}_j^R(\sum_{i \in I} R[G]^{G_i}, S) = 0 \quad \text{for all } j \geq 1.$$

Hence $\sum_{i \in I} R[G]^{G_i}$ is a flat R-module. □

5.5.28. Corollary. *Suppose that*
(i) $\{H_j\}_{j\in I}$ *is a molecule of normal subgroups of* G *with atoms* $\{G_i\}_{i\in I}$;
(ii) *the family of subgroups* $\{G_i\}_{i\in I}$ *of* G *is* R*-admissible.*
Put

$$G_\infty = \bigcap_{j=0}^{n-1} G_j.$$

Then we have the universal exact sequence of R*-modules*
(5.5.29)

$$0 \to R[G]^{H_0H_1\dots H_{n-1}} \to \prod_{i_0\in I} R[G]^{H_{i_0}} \to \prod_{\substack{(i_0,i_1)\in I^2\\ i_0<i_1}} R[G]^{H_{i_0}\cap H_{i_1}} \to \dots$$

$$\dots \to \prod_{i\in I} R[G]^{G_i} \to R[G]^{G_\infty} \to R[G]^{G_\infty}/\sum_{i\in I} R[G]^{G_i} \to 0.$$

Proof. This is an immediate consequence of the previous corollary 5.5.24 and that $\{H_j\}_{j\in I}$ is a molecule of normal subgroups of G with atoms $\{G_i\}_{i\in I}$. □

5.5.30. Corollary. *Assume that* $\{G_i\}_{i\in I}$ *is an* R*-admissible family of subgroups of* G. *Put for all* $i \neq j$

$$e_i = \sum_{h\in G_i} h \quad \text{and} \quad e_{ij} = \sum_{h\in G_iG_j} h.$$

Let $s_i \in R[G]^{G_i}$, *for* $i = 0, \dots, n-1$, *be elements such that*

$$\sum_{i=0}^{n-1} s_i = 0.$$

Then there are elements

$$\eta^{(i,j)} \in R[G], \quad \text{for all } 0 \le i,j \le n-1,\ i \neq j,$$

such that
(a) $\eta^{(i,j)} = -\eta^{(j,i)}$ *for all* $i \neq j$;
(b) $s_i = \sum_{j\neq i} e_{ij}\eta^{(i,j)}$ *for all* i.
Furthermore, let $f_i : G \to G/G_i$ *denote the canonical group homomorphism. Then we have* $s_i = e_ig_i$, *where* $g_i \in R[G]$, $e_{f_i(G_j)} = \sum_{h\in f_i(G_j)} h \in R[G/G_i]$, *and*

$$f_i(g_i) = \sum_{j\neq i} e_{f_i(G_j)} f_i(\eta^{(i,j)}) \quad \text{for all } i,j.$$

Proof. The result is trivial for $n = 1$. We may therefore assume that $n \geq 2$.

Write $\mathcal{G}$ for $\{G_i\}_{i\in I}$. From corollary 5.5.24, the homology complex $\{C_k(\mathcal{G}, R[G]), d_k\}_{k\in\mathbb{N}}$ becomes an exact sequence

$$0 \to C_{n-1}(\mathcal{G}, R[G]) \to C_{n-2}(\mathcal{G}, R[G]) \to C_{n-3}(\mathcal{G}, R[G]) \to \dots$$

$$\dots \to C_0(\mathcal{G}, R[G]) \to C_{-1}(\mathcal{G}, R[G]).$$

The terms for $k = -1, 0, 1$ give precisely the exact sequence, where $G_\infty = \cap_{i=0}^{n-1} G_i$,

$$\prod_{\substack{(i_0,i_1)\in I^2 \\ i_0<i_1}} R[G]^{G_{i_0}G_{i_1}} \xrightarrow{d_1} \prod_{i\in I} R[G]^{G_i} \xrightarrow{d_0} R[G]^{G_\infty}. \tag{5.5.31}$$

By definition the chain group $C_0(\mathcal{G}, R[G])$ is given by

$$C_0(\mathcal{G}, R[G]) = \prod_{i\in I} R[G]^{G_i}.$$

Define an isomorphism

$$\begin{aligned} \pi : \quad \prod_{j=0}^{n-1} R[G]^{G_j} \quad &\to \quad C_0(\mathcal{G}, R[G]) \\ (s_0, \dots, s_{n-1}) \quad &\mapsto \quad (s_0, -s_1, s_2, \dots, (-1)^i s_i, \dots, (-1)^{n-1} s_{n-1}). \end{aligned}$$

Then we have that $\pi(s_0, \dots, s_{n-1})$ is a cycle of $C_0(\mathcal{G}, R[G])$ if and only if $\sum_{i=0}^{n-1} s_i = 0$

Suppose then the elements $s_i \in R[G]^{G_i}$ satisfy $\sum_i s_i = 0$. We write

$$\mathrm{Ann}(e) = \{x \in R[G] \mid xe = 0\}$$

for the annihilator ideal of an element e of $R[G]$. The G-module $R[G]$ is cohomologically trivial hence we have

$$e_i R[G] = R[G]^{H_i} \quad \text{for all } i.$$

By the exact sequence (5.5.31), there are elements $t^{(i,j)} \in R[G]^{G_iG_j}$, for all $i \neq j$, such that

$$s_i = \sum_{j\neq i} t^{(i,j)}$$

and

$$t^{(i,j)} = -t^{(j,i)} \quad \text{for all } i \neq j.$$

As we have

$$R[G]^{G_iG_j} = e_{ij} R[G] \quad \text{for all } i \neq j$$

there are elements $\zeta^{(i,j)} \in R[G]$ such that

$$t^{(i,j)} = e_{ij}\zeta^{(i,j)} \quad \text{for all } i \neq j.$$

As $t^{(i,j)}$ is antisymmetric in i, j, we obtain

$$\zeta^{(i,j)} + \zeta^{(j,i)} \in \mathrm{Ann}(e_{ij}).$$

Put

$$\theta^{(i,j)} = \zeta^{(i,j)} + \zeta^{(j,i)} \in \mathrm{Ann}(e_{ij})$$

and put

$$\eta^{(i,j)} = \begin{cases} \zeta^{(i,j)} - \theta^{(i,j)}, & \text{if } i < j; \\ \zeta^{(i,j)}, & \text{if } i > j. \end{cases}$$

Then we have

$$s_i = \sum_{j \neq i} e_{ij}\eta^{(i,j)} \quad \text{for all } i$$

and

$$\eta^{(i,j)} = -\eta^{(j,i)} \quad \text{for all } i \neq j.$$

This proves the first part of the corollary.

For the last part, we have

$$e_{ij} = \sum_{g \in G_i} \sum_{h \in G_j/G_i \cap G_j} gh = e_i \sum_{h \in G_j/G_i \cap G_j} h;$$

hence we obtain

$$e_i g_i = e_i \big[\sum_{j \neq i} \sum_{h \in G_j/G_i \cap G_j} h\eta^{(i,j)} \big]$$

therefore we have

$$g_i - \big[\sum_{j \neq i} \sum_{h \in G_j/G_i \cap G_j} h\eta^{(i,j)} \big] \in \mathrm{Ann}(e_i).$$

As $\mathrm{Ann}(e_i)$ is just the augmentation ideal of G_i (see remark 5.5.32(i) below) we obtain

$$f_i(g_i) = f_i\Big(\sum_{j \neq i} \sum_{h \in G_j/G_i \cap G_j} h\eta^{(i,j)}\Big)$$

$$= \sum_{j \neq i} \sum_{h \in G_j/G_i \cap G_j} f_i(h) f_i(\eta^{(i,j)}) = \sum_{j \neq i} e_{f_i(G_j)} f_i(\eta^{(i,j)}). \quad \square$$

5.5.32. Remarks. (i) Let I_H be the augmentation ideal of a normal subgroup H of G in $R[G]$

$$I_H = \sum_{h \in H} (h-1)R[G].$$

The cohomological triviality of $R[G]$ implies that the annihilator ideal of $e_H = \sum_{h \in H} g$ in $R[G]$ is equal to I_H.

(ii) With the notation of corollary 5.5.30, let

$$\eta^{(i,j)} \in R[G], \quad \text{for all } 0 \leq i, j \leq n-1, \ i \neq j,$$

be any elements such that $\eta^{(i,j)} = -\eta^{(j,i)}$ for all i, j. Then the elements $h_i \in R[G]$ given by

$$h_i = \sum_{j \neq i} e_{ij} \eta^{(i,j)}, \quad \text{for all } i,$$

obviously satisfy

$$\sum_{i=0}^{n-1} h_i = 0.$$

and

$$h_i \in e_i R[G] \quad \text{for all } i.$$

Thus the corollary 5.5.30 gives the general solution of the equation $\sum_i e_i g_i = 0$ in the group algebra $R[G]$ under the hypothesis that $\{G_i\}_{i \in I}$ be R-admissible.

(iii) If R is a field whose characteristic does not divide $|G|$ and $G_1, \ldots, G_n$ are normal subgroups (not necessarily pairwise central) of the finite group G then representation theory shows that the conclusion of corollary 5.5.30 still holds for $R[G]$ that is to say if $s_i \in R[G]^{G_i}$ are elements such that $\sum_i s_i = 0$ then there are elements $\eta^{(i,j)} \in R[G]^{G_i G_j}$, antisymmetric in i, j, such that $s_i = \sum_{j \neq i} \eta^{(i,j)}$ for all i. .

[For the proof, let M be a simple left $R[G]$-module. Then for all i the R-submodule M^{G_i} is an $R[G]$-submodule of M, as the groups G_i are normal in G. Hence for all i we have either $M^{G_i} = M$ or $M^{G_i} = 0$. It follows that the conclusion of corollary 5.5.30 holds for the simple $R[G]$-module M, that is to say if $s_i \in M^{G_i}$ are elements such that $\sum_i s_i = 0$ then there are elements $\eta^{(i,j)} \in M^{G_i G_j}$, antisymmetric in i, j, such that $s_i = \sum_{j \neq i} \eta^{(i,j)}$ for all i. As the characteristic of the field R does not divide $|G|$, the group algebra $R[G]$ is a semi-simple $R[G]$-module. Hence the conclusion of this corollary also holds for $R[G]$ itself.]

(iv) If G is an abelian group, we give an example where the corollary 5.5.30 would become false without the hypothesis that the order of the kernel of the homomorphism $\prod_i G_i \to G$ be a unit of the ring R.

Let G be the group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ where p is a prime number ≥ 3. Let x_1, x_2 be generators of G. Let G_i, $i = 1, 2, 3$, be the cyclic subgroups of order p of G given by

$$G_1 =< x_1 >, \quad G_2 =< x_2 >, \quad G_3 =< x_1 x_2 > .$$

Let R be a field of characteristic p and in the group algebra $R[G]$ we put

$$e_i = \sum_{h \in G_i} h, \quad \text{for } i = 1, 2, 3.$$

Then there are elements $g_1, g_2, g_3 \in R[G]$ such that

$$\sum_{i=1}^{3} e_i g_i = 0$$

but $e_1 g_1$ is not an element of $R[G]^{G_1 G_2} + R[G]^{G_1 G_3}$.

[Put

$$\eta_1 = x_1 - 1, \eta_2 = x_2 - 1$$

and put

$$g_1 = (x_2 - 1)^{p-2} + (x_2 - 1)^{p-1},\ g_2 = -(x_1 - 1)^{p-2},\ g_3 = (x_1 - 1)^{p-2}.$$

The group algebra $R[G]$ is R-isomorphic to

$$R[\eta_1, \eta_2]/ < \eta_1^p, \eta_2^p > .$$

In particular, it is an artin local ring with residue field R. We have

$$e_1 = \eta_1^{p-1},\ e_2 = \eta_2^{p-1},\ e_3 = (\eta_1 \eta_2 + \eta_1 + \eta_2)^{p-1}.$$

The elements g_i are given by

$$g_1 = \eta_2^{p-2} + \eta_2^{p-1}, \quad g_2 = -g_3 = -\eta_1^{p-2}.$$

Hence we have

$$\sum_{i=1}^{3} e_i g_i = \eta_1^{p-1}(\eta_2^{p-2} + \eta_2^{p-1}) - \eta_2^{p-1}\eta_1^{p-2} + (\eta_1 \eta_2 + \eta_1 + \eta_2)^{p-1}\eta_1^{p-2}$$

$$= \eta_1^{p-1}(\eta_2^{p-2} + \eta_2^{p-1}) - \eta_2^{p-1}\eta_1^{p-2} + \left\{ \sum_{i=0}^{p-1} C_i^{p-1} \big(\eta_1(1 + \eta_2)\big)^i \eta_2^{p-1-i} \right\} \eta_1^{p-2}$$

$$= \eta_1^{p-1}(\eta_2^{p-2} + \eta_2^{p-1}) - \eta_2^{p-1}\eta_1^{p-2} + \eta_2^{p-1}\eta_1^{p-2} - \big(\eta_1(1 + \eta_2)\big)\eta_2^{p-2}\eta_1^{p-2} = 0.$$

We have $G_1G_2 = G_1G_3 = G$ hence we obtain

$$R[G]^{G_1G_2} + R[G]^{G_1G_3} = R[G]^G = R\eta_1^{p-1}\eta_2^{p-1}.$$

Furthermore, we have

$$e_1g_1 = \eta_1^{p-1}(\eta_2^{p-2} + \eta_2^{p-1}).$$

If e_1g_1 were an element of $R[G]^{G_1G_2} + R[G]^{G_1G_3}$ we would have for some $r \in R$ that

$$\eta_1^{p-1}\eta_2^{p-2} = r\eta_1^{p-1}\eta_2^{p-1}$$

which is impossible. Hence $e_1g_1 \notin R[G]^{G_1G_2} + R[G]^{G_1G_3}$ as required.]

5.6 Group cohomology; Kolyvagin elements

Let $R[G]$ be a group algebra where R is a commutative ring and G is a finite group. In this section we first consider sets of submodules of $R[G]$ which are the invariants under familes of subgroups of G. The set of relations of the Heegner module are closely related to such submodules; in particular, example 5.6.3(5) is later applied to the Heegner module.

Second, we define Kolyvagin elements attached to cochains in the cohomology of the group G. Kolyvagin [K] considered special cases of our general construction of Kolyvagin elements. Stickelberger elements [R] in the theory of cyclotomic fields are also examples of Kolyvagin elements attached to 1-cochains.

The final part of this section on the cohomology of cocycles collects some technical results on group cohomology that are required principally for the computation of the cohomology of the Heegner module in chapter 6. The reading of this final part from proposition 5.6.14 onwards may be omitted until the relevant results are required for a reading of chapter 6.

(5.6.1) Let G be a finite group and R be a commutative ring.

Sieves of submodules

5.6.2. Definition. A *sieve* is a partially ordered set E in which every pair of elements a, b of E has a least upper bound, written $\mathrm{lub}(a, b)$, and a greatest lower bound, written $\mathrm{glb}(a, b)$.

[The usual terminology for such a partially ordered set is a *lattice*, but the word lattice is used differently in this text; see [C, Chapters I and II] for more details.]

5.6.3. Examples. (1) Let M be an R-module. The set of all R-submodules of M is a sieve $L(M)$ which is partially ordered by set-theoretic inclusion of submodules. Let $\mathcal{S}$ be a set of R-submodules of M which is partially ordered by set-theoretic inclusion of submodules. Then $\mathcal{S}$ is a subsieve of $L(M)$ if and only if it satisfies:

(a) the intersection of any finite set of submodules in $\mathcal{S}$ belongs to $\mathcal{S}$;

(b) the sum in M of any finite set of submodules in $\mathcal{S}$ also lies in $\mathcal{S}$.

We call such a set $\mathcal{S}$ of submodules satisfying the conditions (a) and (b) a *sieve of submodules* of M.

(2) Let M be an R-module. The intersection of any collection of sieves of submodules of M, as in (1), is also a sieve of submodules of M.

(3) Let M be an R-module. Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a family of submodules M_λ of M. Then, by (2) above, there is a smallest sieve of submodules $\sigma\{M_\lambda\}_{\lambda\in\Lambda}$ of M containing all elements of the family $\{M_\lambda\}_{\lambda\in\Lambda}$.

(4) Let $\Lambda(G)$ be the set of all finite sets $\{H_1,\ldots,H_n\}$ of distinct subgroups H_i of the finite group G such that $H_i \not\subseteq H_j$ for all $i \neq j$. Define a partial order $\leq$ on $\Lambda(G)$ as follows. If $S_1, S_2 \in \Lambda(G)$ then $S_1 \leq S_2$ if and only if for all $G_1 \in S_1$ there is $G_2 \in S_2$ with $G_1 \supseteq G_2$.

For any finite set of subgroups $S = \{G_1,\ldots,G_m\}$ of G let $\min\{G_1,\ldots,G_m\}$ denote the set of minimal elements of S with respect to the inclusion order; then we have $\min(S) \in \Lambda(G)$ and any subgroup contained in S contains at least one element of $\min(S)$.

The partially ordered set $\Lambda(G)$ is a sieve. More precisely, for elements $S_1, S_2 \in \Lambda(G)$ where

$$S_1 = \{H_1,\ldots,H_n\} \quad \text{and} \quad S_2 = \{G_1,\ldots,G_m\}$$

with $H_1,\ldots,H_n,G_1,\ldots,G_m$ subgroups of G, we have that $\mathrm{lub}(S_1,S_2)$ is equal to the set of minimal elements of the union of S_1 and S_2

$$\mathrm{lub}(S_1,S_2) = \min(S_1 \cup S_2).$$

Furthermore, $\mathrm{glb}(S_1,S_2)$ is the set of minimal elements given by

$$\mathrm{glb}(S_1,S_2) = \min\big(\{< H_r, G_s > \ \mid \ \text{for all } r,s\}\big).$$

where $< H_r, G_s >$ denotes the subgroup of G generated by H_r and G_s.

(5) Suppose that $\{G_i\}_{i=0,\dots,n-1}$ is an R-admissible family of subgroups of the finite group G. Then we have for all integers $m = 0, 1, \dots, n-1$

$$\big(\sum_{i=0}^{m} R[G]^{G_i}\big) \cap \big(\sum_{j=m+1}^{n-1} R[G]^{G_j}\big) = \sum_{i=0}^{m} \sum_{j=m+1}^{n-1} R[G]^{G_i G_j}.$$

[For the proof, put

$$M_1 = \sum_{i=0}^{m} R[G]^{G_i} \quad \text{and} \quad M_2 = \sum_{j=m+1}^{n-1} R[G]^{G_j}.$$

Clearly we have the inclusion

$$M_1 \cap M_2 \supseteq \sum_{i=0}^{m} \sum_{j=m+1}^{n-1} R[G]^{G_i G_j}.$$

Let $x \in M_1 \cap M_2$. We put

$$e_i = \sum_{g \in G_i} g, \quad e_{ij} = \sum_{g \in G_i G_j} g.$$

We have

$$x = \sum_{i=0}^{m} e_i y_i = \sum_{j=m+1}^{n-1} -e_j y_j$$

where $y_i \in R[G]$ for all $i = 0, \dots, n-1$. Hence we have $\sum_{i=0}^{n-1} e_i y_i = 0$. By corollary 5.5.30, there are elements $\eta^{(i,j)} \in R[G]$ antisymmetric in i, j, where $0 \le i, j \le n-1$, such that

$$e_i y_i = \sum_{j \neq i} e_{ij} \eta^{(i,j)} \quad \text{for all } i.$$

Hence we have

$$x = \sum_{i=0}^{m} e_i y_i = \sum_{i=0}^{m} \sum_{\substack{j=0 \\ j \neq i}}^{n-1} e_{ij} \eta^{(i,j)}.$$

As $\eta^{(i,j)}$ is antisymmetric in i, j, this double sum for x reduces to

$$x = \sum_{i=0}^{m} \sum_{j=m+1}^{n-1} e_{ij} \eta^{(i,j)}.$$

Hence we have

$$x \in \sum_{i=0}^{m} \sum_{j=m+1}^{n-1} R[G]^{G_i G_j}.$$

We obtain the inclusion

$$M_1 \cap M_2 \subseteq \sum_{i=0}^{m} \sum_{j=m+1}^{n-1} R[G]^{G_i G_j}$$

whence the stated equality of submodules.]

(6) Let $\mathcal{S}$ be the set of $R[G]$-submodules of $R[G]$ of the form $\sum_i R[G]^{H_i}$ where H_i are subgroups of G for all i. Let $\Lambda(G)$ be the sieve of example 5.6.3(4). Let

$$f : \Lambda(G) \to \mathcal{S}$$

be the surjective map of *sets* given by

$$\{H_1, \ldots, H_n\} \mapsto \sum_{i=1}^{n} R[G]^{H_i}$$

where $H_1, \ldots, H_n$ are subgroups of G.

If the group G is abelian of order which is a unit in R then $\mathcal{S}$ is a *sieve* of $R[G]$-submodules of $R[G]$ and f is a surjective homomorphism of *sieves*.

[For the proof, to check that $\mathcal{S}$ is a sieve of submodules of M, we only need to verify the stability of $\mathcal{S}$ under finite intersections of submodules (example 5.6.3(1)).

Let S_1, S_2 be two elements of $\Lambda(G)$. Then we have

$$S_1 = \{H_1, \ldots, H_n\} \quad \text{and} \quad S_2 = \{J_1, \ldots, J_m\}$$

where $H_1, \ldots, H_n, J_1, \ldots, J_m$ are subgroups of G such that $H_i \not\subseteq H_j$ for all $i \neq j$ and $J_h \not\subseteq J_k$ for all $h \neq k$. Let

$$T = S_1 \cap S_2$$

that is to say, T is the set of subgroups common to both S_1 and S_2. Then we have $T \in \Lambda(G)$. Put $S_i' = S_i \setminus T$ for $i = 1, 2$. Then we have

$$f(S_1) \cap f(S_2) = (f(S_1') + f(T)) \cap (f(S_2') + f(T)).$$

As S_1', S_2', T are pairwise disjoint sets of subgroups and as any finite family of subgroups of G is R-admissible, it follows from example (5) above that

$$f(S_1) \cap f(S_2) = f(T) + f(\mathrm{glb}(S_1', S_2')).$$

We obtain that $f(S_1) \cap f(S_2)$ belongs to $\mathcal{S}$. It follows by induction that the set of submodules $\mathcal{S}$ is closed under finite intersections and hence is a sieve of $R[G]$-submodules.

The map of sets $f : \Lambda(G) \to \mathcal{S}$ is evidently surjective. It remains to show that it is a homomorphism of sieves.

Let $S_1 = \{H_1, \ldots, H_n\}$, $S_2 = \{J_1, \ldots, J_m\}$ be the two elements of $\Lambda(G)$ as above. Suppose that $S_1 \leq S_2$. Then for all $i = 1, \ldots, n$ there is an integer j, where $1 \leq j \leq m$, such that $H_i \supseteq J_j$. It follows that

$$f(S_1) = \sum_{i=1}^{n} R[G]^{H_i} \quad \subseteq \quad \sum_{j=1}^{m} R[G]^{J_j} = f(S_2).$$

Hence the map f preserves the partial order on $\Lambda(G)$ and on $\mathcal{S}$ and it may be checked that f preserves least upper bounds and greatest lower bounds of the sieves (using the formula above for $f(S_1) \cap f(S_2)$); hence f is a homomorphism of sieves.]

5.6.4. Remarks. (i) Suppose that G is a finite abelian group and R is the rational field $\mathbb{Q}$. Define an equivalence relation $\sim$ on $\Lambda(G)$ as follows. For $S_1 = \{H_1, \ldots, H_n\} \in \Lambda(G)$ and $S_2 = \{J_1, \ldots, J_m\} \in \Lambda(G)$ we write $S_1 \sim S_2$ if for every subgroup K of G such that G/K is cyclic then $\{K\} \leq S_1$ if and only if $\{K\} \leq S_2$.

Let $\mathcal{S}$ be the set of $\mathbb{Q}[G]$-submodules of $\mathbb{Q}[G]$ of the form $\sum_i \mathbb{Q}[G]^{H_i}$ where H_i are subgroups of G for all i. Let

$$f : \Lambda(G) \to \mathcal{S}$$

be the surjective homomorphism of sieves given by examples 5.6.3(6). Then f induces an isomorphism of sieves

$$\Lambda(G)/\sim \quad \cong \quad \mathcal{S}.$$

[To prove this, the algebra $\mathbb{Q}[G]$ is a direct product of fields. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{Q}[G]$. By proposition 5.1.5, the ideal $\mathfrak{m}$ corresponds to a subgroup J of G for which the quotient G/J is cyclic, namely, J is the kernel of the induced group homomorphism $G \to (\mathbb{Q}[G]/\mathfrak{m})^*$. Let $S \in \Lambda(G)$. There is a subgroup H_0 belonging to S which is contained in J if and only if $f(S) = \sum_{H \in S} \mathbb{Q}[G]^H$ is not contained in the ideal $\mathfrak{m}$. Hence $S_1 \sim S_2$ if and only if the maximal ideals of $\mathbb{Q}[G]$ containing $f(S_1)$ are the same as those containing $f(S_2)$. But every ideal of $\mathbb{Q}[G]$ is an intersection of maximal ideals; hence $S_1 \sim S_2$ if and only if $f(S_1) = f(S_2)$.]

(ii) The map $f : \Lambda(G) \to \mathcal{S}$ of remark (i) is not necessarily an isomorphism of sieves.

For example, suppose that G is a non-cyclic finite abelian group; let S be the finite set of all the distinct minimal subgroups of G different from the trivial subgroup 0. Let the ring R be the rational field $\mathbb{Q}$. Then we have that $S \in \Lambda(G)$ and $S \sim \{0\}$ by remark (i) above. Hence we have $f(S) = \mathbb{Q}[G] = f(\{0\})$ and the map $f : \Lambda(G) \to \mathcal{S}$ is not injective.

Notation for the cohomology of finite groups

We introduce some standard notation for the cohomology of finite groups. A module over a non-commutative ring is a *left* module, unless otherwise stated.

(5.6.5) For any subgroup J of G and any $R[G]$-module M, let $\mathrm{Coch}^n(J,M)$ denote the module of n-cochains on J with values in M; that is to say, we have

$$\mathrm{Coch}^n(J,M) = \bigoplus_{j\in J^n} M.$$

Then $\mathrm{Coch}^n(J,M)$ is a (left) $R[G]$-module isomorphic to a direct sum of a finite number of copies of M. The R-module homomorphism

$$\partial^n : \mathrm{Coch}^n(J,M) \to \mathrm{Coch}^{n+1}(J,M) \quad \text{for all } n$$

is given by the usual coboundary formula

$$(\partial^n(f))(g_1,\dots,g_n) = g_1 f(g_2,\dots,g_{n+1}) + \sum_{i=1}^{i=n} (-1)^i f(g_1,\dots,g_i g_{i+1},\dots,g_{n+1}) +$$

$$+(-1)^{n+1} f(g_1,\dots,g_n).$$

We have $\partial^n \circ \partial^{n-1} = 0$ for all n. Hence $\{\mathrm{Coch}^n(J,M), \partial^n\}_{n\in\mathbb{N}}$ is a complex whose cohomology is written $H^n(J,M)$.

(5.6.6) Write $\mathrm{Cocy}^n(J,M)$ for the R-module of n-cocycles on J with values in M; that is to say

$$\mathrm{Cocy}^n(J,M) = \ker\big(\partial^n : \mathrm{Coch}^n(J,M) \to \mathrm{Coch}^{n+1}(J,M)\big).$$

If the group G is abelian, the R-module $\mathrm{Cocy}^n(J,M)$ is also a $R[G]$-module.

(5.6.7) Write $\mathrm{Cob}^n(J,M)$ for the group of n-coboundaries on J with values in M; that is to say

$$\mathrm{Cob}^n(J,M) = \mathrm{Im}\big(\partial^{n-1} : \mathrm{Coch}^{n-1}(J,M) \to \mathrm{Coch}^n(J,M)\big).$$

If the group G is abelian, the R-module $\mathrm{Cob}^n(J,M)$ is also a $R[G]$-module.

(5.6.8) The $R[G]$-module M is *cohomologically trivial* if for any subgroup J of G we have

$$H^i(J,M) = 0 \quad \text{for all } i \geq 1.$$

The $R[G]$-module M is *universally cohomologically trivial* if for any R-module N equipped with a trivial action by the group G then the module $M \otimes_R N$ is cohomologically trivial.

For example, the module $R[G]$ over the group algebra $R[G]$ is universally cohomologically trivial.

Kolyvagin elements

(5.6.9) Let S be an R-algebra and G be a finite group. Let e_G be the element of the group algebra $S[G]$ given by

$$e_G = \sum_{g \in G} g.$$

(5.6.10) Let

$$\psi : G^m \to S$$

be an m-cochain in $\mathrm{Coch}^m(G, S)$ of G with values in S. Define the $m-1$-cochain $E_\psi : G^{m-1} \to S[G]$ by

$$E_\psi(g_2, \ldots, g_m) = \sum_{h \in G} h^{-1}\psi(h, g_2, \ldots, g_m) \quad \text{for all } (g_2, \ldots, g_m) \in G^{m-1}.$$

The map $\psi \to E_\psi$ is a homomorphism of S-modules

$$E : \mathrm{Coch}^m(G, S) \to \mathrm{Coch}^{m-1}(G, S[G]).$$

5.6.11. Definition. The element E_ψ of $\mathrm{Coch}^{m-1}(G, S[G])$ is a *Kolyvagin element* attached to the m-cochain $\psi \in \mathrm{Coch}^m(G, S)$.

5.6.12. Proposition. *Let $\psi \in \mathrm{Coch}^m(G, S)$. Then the Kolyvagin element E_ψ is the unique cochain in $\mathrm{Coch}^{m-1}(G, S[G])$, up to addition of an $m-1$-coboundary in $\mathrm{Cob}^{m-1}(G, S[G])$, such that*

$$(\partial^{m-1} E_\psi)(g) = \psi(g) e_G - \sum_{h \in G} h^{-1}(\partial^m \psi)(h, g) \quad \text{for all } g \in G^m.$$

In particular, if ψ is a cocycle in $\mathrm{Cocy}^m(G, S)$ then E_ψ is the unique cochain in $\mathrm{Coch}^{m-1}(G, S[G])$, up to addition of an $m-1$-coboundary, such that

$$(\partial^{m-1} E_\psi)(g) = \psi(g) e_G \quad \text{for all } g \in G^m.$$

5.6.13. Remarks. (i) Let G be a finite group and let $\psi : G \to S$ be a homomorphism into the additive group of the R-algebra S. The Kolyvagin element E_ψ in $S[G]$ is then given by

$$E_\psi = \sum_{h \in G} \psi(h) h^{-1}.$$

This element satisfies

$$(g-1)E_\psi = \psi(g) e_G \quad \text{for all } g \in G.$$

(ii) Kolyvagin [K] considered the following special case of a Kolyvagin element defined above. Let n be a positive integer divisible by a prime number p. Let $\mathbb{F}_p$ be the prime field of order p and let G be a cyclic group of order n generated by an element g. Let $\psi : G \to \mathbb{F}_p$ be the homomorphism

$$g^r \mapsto r \pmod{p}.$$

The Kolyvagin element E_ψ in $\mathbb{F}_p[G]$ is then given by

$$E_\psi = -\sum_{r=1}^{n-1} r g^r.$$

This element satisfies

$$(g^r - 1)E_\psi = r e_G. \quad \text{for all } r.$$

(iii) Suppose that G is a direct product of finite groups $G_1, \ldots, G_m$. Let

$$\psi_i : G_i \to S$$

be homomorphisms as in remark (i) above. Let $E_{\psi_i} \in S[G_i]$ be the Kolyvagin element attached to the 1-cocycle ψ_i for all i. The map

$$\begin{aligned} \psi : G = G_1 \times \ldots \times G_m &\to S \\ (g_1, g_2, \ldots, g_m) &\mapsto \textstyle\prod_i \psi_i(g_i) \end{aligned}$$

is a multilinear homomorphism, that is to say it is a homomorphism with respect to each factor G_i. The element E_ψ in $S[G]$ associated to the 1-cochain $\psi \in \mathrm{Coch}^1(G, S)$ is

$$E_\psi = \prod_{i=1}^{m} E_{\psi_i} = \sum_{h \in G} h^{-1} \psi(h).$$

As we have the identity, where $g = \prod_{i=1}^m g_i$ and $g_i \in G_i$ for all i,

$$g - 1 = (g_1 - 1) \prod_{i \geq 2} g_i + (g_2 - 1) \prod_{i \geq 3} g_i + \ldots + g_m - 1$$

the Kolyvagin element E_ψ attached to the 1-cochain ψ satisfies

$$(g-1)E_\psi \in \sum_{i=1}^{m} e_{G_i} S[G] \quad \text{for all } g \in G.$$

Kolyvagin [K] also considers these elements E_ψ when the G_i are cyclic groups and S is the prime field $\mathbb{F}_p$.
(iv) Let $m > 1$ be an integer and let $\mathbb{Q}(\mu_m)$ be the cylotomic field extension of the rational field generated by the mth roots of unity. Let $G = \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Then there is an isomorphism $(\mathbb{Z}/m\mathbb{Z})^* \cong G$ given by $c \mapsto \sigma_c$ and where σ_c acts on primitive mth roots of unity by raising them to the cth power. Let $< t >$ denote the smallest real number ≥ 0 in the residue class modulo $\mathbb{Z}$ of a real number t. Let p be a prime number which does not divide m. Let $\mathfrak{p}$ be a prime ideal above p in $\mathbb{Q}(\mu_m)$. Let k be an integer such that $k/(q-1)$ has order m in $\mathbb{Q}/\mathbb{Z}$. Let ψ be the 1-cochain

$$\psi : G \to \mathbb{Q}, \quad c \mapsto < \frac{kc}{q-1} > .$$

The Kolyvagin element $E_\psi \in \mathbb{Q}[G]$ where

$$E_\psi = \sum_{c \in (\mathbb{Z}/m\mathbb{Z})^*} < \frac{kc}{q-1} > \sigma_c^{-1}$$

is then a *Stickelberger element*. A fundamental result due to Stickelberger is that the ideal $\mathfrak{p}^{E_\psi}$, in a suitable extension field of $\mathbb{Q}(\mu_m)$, is principal and is generated by a Gauss sum [R1].

Proof of proposition 5.6.12. Let $\psi \in \mathrm{Coch}^m(G, S)$. By definition of the $m-1$-cochain $E_\psi : G^{m-1} \to S[G]$, we have for any element $(g_1, \ldots, g_m)$ of G^m

$$(\partial^{m-1} E_\psi)(g_1, \ldots, g_m) = g_1 E_\psi(g_2, \ldots, g_m) +$$

$$\sum_{j=1}^{m-1} (-1)^j E_\psi(g_1, \ldots, g_j g_{j+1}, \ldots, g_m) + (-1)^m E_\psi(g_1, \ldots, g_{m-1}).$$

This is equal to

$$g_1 \sum_{h \in G} h^{-1} \psi(h, g_2, \ldots, g_m) + \sum_{j=1}^{m-1} (-1)^j \sum_{h \in G} h^{-1} \psi(h, g_1, \ldots, g_j g_{j+1}, \ldots, g_m)$$

$$+ (-1)^m \sum_{h \in G} h^{-1} \psi(h, g_1, \ldots, g_{m-1}).$$

This expression equals, via a change of variables $h \mapsto hg_1$ in the first summation,

$$\sum_{h\in G} h^{-1}\psi(hg_1, g_2, \ldots, g_m)+$$

$$\sum_{h\in G}\left\{\sum_{j=1}^{m-1}(-1)^j h^{-1}\psi(h, g_1, \ldots, g_jg_{j+1}, \ldots, g_m) + (-1)^m\psi(h, g_1, \ldots, g_{m-1})\right\}$$

$$= \sum_{h\in G} h^{-1}\Big\{\psi(hg_1, g_2, \ldots, g_m)+$$

$$\sum_{j=1}^{m-1}(-1)^j\psi(h, g_1, \ldots, g_jg_{j+1}, \ldots, g_m) + (-1)^m\psi(h, g_1, \ldots, g_{m-1})\Big\}.$$

As ψ is an m-cochain of G with values in S, we have, putting $g_0 = h$,

$$\partial^m\psi(h, g_1, \ldots, g_m) = \psi(g_1, \ldots, g_m) + \sum_{j=0}^{m-1}(-1)^{j-1}\psi(h, g_1, \ldots, g_jg_{j+1}, \ldots, g_m)$$

$$+(-1)^{m+1}\psi(h, g_1, \ldots, g_{m-1}).$$

That is to say we have

$$\psi(g_1, \ldots, g_m) = \sum_{j=0}^{m-1}(-1)^j\psi(h, g_1, \ldots, g_jg_{j+1}, \ldots, g_m)+$$

$$(-1)^m\psi(h, g_1, \ldots, g_{m-1}) - \partial^m\psi(h, g_1, \ldots, g_m).$$

Hence we have

$$(\partial^{m-1}E_\psi)(g_1, \ldots, g_m) = \sum_{h\in G} h^{-1}\psi(g_1, \ldots, g_m) - \sum_{h\in G} h^{-1}\partial^m\psi(h, g_1, \ldots, g_m)$$

$$= e_G\psi(g_1, \ldots, g_m) - \sum_{h\in G} h^{-1}\partial^m\psi(h, g_1, \ldots, g_m)$$

as required.

Suppose there is cochain C in $\mathrm{Coch}^{m-1}(G, S[G])$ such that

$$(\partial^{m-1}C)(g) = \psi(g)e_G - \sum_{h\in G} h^{-1}\partial^m\psi(h, g) \quad \text{for all } g \in G^m.$$

Then the cochain $C - E_\psi$ satisfies $\partial^{m-1}(C - E_\psi) = 0$. Therefore $C - E_\psi$ is an $m-1$-cocycle and as $S[G]$ is a cohomologically trivial G-module, we obtain that $C - E_\psi$ is an $m-1$-coboundary in $\mathrm{Cob}^{m-1}(G, S[G])$ as required.

If ψ is an m-cocycle in $\mathrm{Cocy}^m(G, S)$, then $\partial^m\psi = 0$ and the last part of the proposition follows fom the first part. □

Cohomology of groups of cocycles

5.6.14. Proposition. *Suppose that G is a finite abelian group. Then for any subgroups J, K of G we have an isomorphism of $R[G]$-modules for all $p \geq 1$ and $q \geq 0$*

$$H^p(K, \mathrm{Cocy}^q(J, R[G])) \cong H^{p+q}(J \cap K, R) \otimes_R R[G/J].$$

Proof. Write $\mathrm{Cocy}^q(J)$ for $\mathrm{Cocy}^q(J, R[G])$. We write $\mathrm{Cob}^q(J)$ for the submodule $\mathrm{Cob}^q(J, R[G])$ of n-coboundaries of J with values in the module $R[G]$ (see the notation (5.6.5) et seq.). We have the exact sequence of $R[K]$-modules

$$0 \quad \to \quad \mathrm{Cocy}^q(J) \quad \to \quad R[G]^{|J|^q} \quad \overset{\partial^q}{\to} \quad \mathrm{Cob}^{q+1}(J) \quad \to \quad 0.$$

As $R[G]$ is a cohomologically trivial G-module, we have

$$\mathrm{Cocy}^q(J) = \mathrm{Cob}^q(J) \text{ for all } q \geq 1.$$

We then have the exact sequence of $R[K]$-modules

$$0 \to \mathrm{Cocy}^q(J) \to R[G]^{|J|^q} \to \mathrm{Cocy}^{q+1}(J) \to 0 \text{ for all } q \geq 0.$$

The long exact sequence of K-cohomology of this exact sequence is

$$0 \to H^0(K, \mathrm{Cocy}^q(J)) \to H^0(K, R[G]^{|J|^q}) \to H^0(K, \mathrm{Cocy}^{q+1}(J)) \to \dots$$

$$\to H^p(K, \mathrm{Cocy}^q(J)) \to H^p(K, R[G]^{|J|^q}) \to H^p(K, \mathrm{Cocy}^{q+1}(J)) \to \dots$$

As $R[G]$ is K-cohomologically trivial we obtain isomorphisms for all $p \geq 2$ and all $q \geq 0$

$$H^p(K, \mathrm{Cocy}^q(J)) \cong H^{p-1}(K, \mathrm{Cocy}^{q+1}(J)).$$

From this we have isomorphisms

(5.6.15)
$$H^p(K, \mathrm{Cocy}^q(J)) \cong H^1(K, \mathrm{Cocy}^{q+p-1}(J)) \text{ for all } p \geq 1 \text{ and } q \geq 0.$$

Furthermore, we have the short exact sequence, where $e_K = \sum_{g \in K} g$,

$$0 \to H^0(K, \mathrm{Cocy}^q(J)) \to e_K R[G]^{|J|^q} \to H^0(K, \mathrm{Cocy}^{q+1}(J)) \to$$

(5.6.16)
$$\to H^1(K, \mathrm{Cocy}^q(J)) \to 0.$$

An element f of $\mathrm{Cocy}^q(J)$ is a map $f : J^q \to R[G]$ such that $\partial^q f = 0$. We have that this cocycle f satisfies $f \in H^0(K, \mathrm{Cocy}^q(J))$ if and only if

$$f(\mathbf{g})h = f(\mathbf{g}) \text{ for all } h \in K \text{ and all } \mathbf{g} \in J^q.$$

Hence $f \in H^0(K, \mathrm{Cocy}^q(J))$ if and only if $f \in \mathrm{Cocy}^q(J, e_K R[G])$. We obtain the equality

$$H^0(K, \mathrm{Cocy}^q(J)) = \mathrm{Cocy}^q(J, e_K R[G]).$$

From (5.6.16), we then obtain the short exact sequence

$$0 \to \mathrm{Cocy}^q(J, e_K R[G]) \to e_K R[G]^{|J|^q} \xrightarrow{\partial^q} \mathrm{Cocy}^{q+1}(J, e_K R[G])$$
$$\to H^1(K, \mathrm{Cocy}^q(J)) \to 0.$$

But the cokernel of the homomorphism

$$\partial^q : e_K R[G]^{|J|^q} \to \mathrm{Cocy}^{q+1}(J, e_K R[G])$$

is by definition the R-module $H^{q+1}(J, e_K R[G])$. Hence we obtain an isomorphism of R-modules

$$H^{q+1}(J, e_K R[G]) \cong H^1(K, \mathrm{Cocy}^q(J)).$$

This with the isomorphism of (5.6.15) shows that there are isomorphisms for all $p \geq 1$ and $q \geq 0$

$$H^p(K, \mathrm{Cocy}^q(J)) \cong H^1(K, \mathrm{Cocy}^{p+q-1}(J)) \cong H^{p+q}(J, e_K R[G]). \tag{5.6.17}$$

As there is an isomorphism of $R[G]$-modules $e_K R[G] \cong R[G/K]$, we have the Hochschild-Serre spectral sequence

$$H^p(J/(J \cap K), H^q(J \cap K, R[G/K])) \Rightarrow H^{p+q}(J, e_K R[G]).$$

As $R[G/K]$ is a finite free R-module on which $J \cap K$ acts trivially, we have isomorphisms for all $q \geq 0$

$$H^q(J \cap K, R[G/K]) \cong H^q(J \cap K, R) \otimes_R R[G/K].$$

Hence we have isomorphisms of $R[G]$-modules for all $p, q \geq 0$

$$H^p(J/(J \cap K), H^q(J \cap K, R[G/K])) \cong H^p(J/(J \cap K), R[G/K]) \otimes_R H^q(J \cap K, R).$$

As $R[G/K]$ is G/K-cohomologically trivial we have $H^p(J/(J \cap K), R[G/K]) = 0$ for all $p \geq 1$; hence we have

$$H^p(J/(J \cap K), H^q(J \cap K, R[G/K])) = 0 \text{ for all } p \geq 1.$$

Hence the above spectral sequence degenerates and provides isomorphisms

$$H^{p+q}(J, e_K R[G]) \cong H^0(J/(J \cap K), H^{p+q}(J \cap K, R[G/K]))$$

$$\cong H^{p+q}(J \cap K, R) \otimes_R R[G/J].$$

The proposition now follows from this and the isomorphisms of (5.6.17). □

Cohomology of the submodule $\sum_i R[G]^{G_i}$ *of* $R[G]$

5.6.18. Lemma. *Let H be a normal subgroup of G. Let M be a universally cohomologically trivial $R[G/H]$-module which is also a flat R-module. Let J be a subgroup of G. We have isomorphisms of R-modules*

$$H^i(J, M) \cong \left(M \otimes_R H^i(J \cap H, R)\right)^J \quad \text{for all } i \geq 0.$$

Proof. As M is a flat R-module on which $J \cap H$ acts trivially, we have isomorphisms of R-modules

$$H^j(J \cap H, M) \cong M \otimes_R H^j(J \cap H, R) \text{ for all } j \geq 0.$$

The Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i(J/J \cap H, H^j(J \cap H, M)) \Rightarrow H^{i+j}(J, M)$$

then becomes the spectral sequence

$$H^i(J/J \cap H, M \otimes_R H^j(J \cap H, R)) \Rightarrow H^{i+j}(J, M).$$

The $R[G/H]$-module $M \otimes_R H^j(J \cap H, R)$ is cohomologically trivial; hence we have

$$H^i(J/J \cap H, M \otimes_R H^j(J \cap H, R))) = 0 \quad \text{for all } i > 0 \text{ and } j \geq 0.$$

Hence this spectral sequence degenerates and we obtain isomorphisms

$$H^0(J/J \cap H, M \otimes_R H^j(J \cap H, R)) \cong H^j(J, M) \quad \text{for all } j \geq 0$$

whence the result holds.□

5.6.19. Proposition. *Let $\{G_i\}_{i\in I}$, where $I = \{0,\dots,n-1\}$, be an R-admissible family of subgroups of the finite group G.*
(i) *Let $E \subset I$ and $t \in I \setminus E$. Then $\sum_{j\in E} R[G]^{G_j}$ is a cohomologically trivial $R[G_t]$-module.*
(ii) *If R is a field then for any integer $m \geq 0$ we have isomorphisms*

$$H^m(G, \sum_{i\in I} R[G]^{G_i}) \cong \bigoplus_{\substack{r_0\neq 0,\dots,r_{n-1}\neq 0 \\ r_0+r_1+\dots+r_{n-1}=n+m-1}} \bigotimes_{i\in I} H^{r_i}(G_i, R).$$

Proof. Let E be a subset of I. Then $\{G_i\}_{i\in E}$ is an R-admissible family of subgroups of G (see definition 5.5.18). Put

$$G_\infty = \bigcap_{j\in E} G_j.$$

As the family $\{G_i\}_{i\in E}$ is R-admissible, by the exact sequence (5.5.25) of corollary 5.5.24 we obtain the universal exact sequence

$$0 \to R[G]^{\prod_{i\in E} G_i} \to \prod_{i_0\in E} R[G]^{\prod_{\substack{j\neq i_0 \\ j\in E}} G_j} \to \prod_{\substack{(i_0,i_1)\in E^2 \\ i_0<i_1}} R[G]^{\prod_{\substack{j\neq i_0,i_1 \\ j\in E}} G_j} \to \dots$$

$$\dots \to \prod_{i\in E} R[G]^{G_i} \to \sum_{i\in E} R[G]^{G_i} \to 0$$

which is obtained from the exact sequence (5.5.25) by replacing the penultimate homomorphism $\prod_{i\in E} R[G]^{G_i} \to R[G]^{G_\infty}$ by its image which is the submodule $\sum_{i\in E} R[G]^{G_i}$. This sequence is universally exact by remark 5.5.22(iii).

This previous exact sequence is precisely the exact sequence (see (5.5.12) and (5.5.13)) where we write $\mathcal{G}_E = \{G_i\}_{i\in E}$ and $m = |E|$

$$0 \to C_{m-1}(\mathcal{G}_E, R[G]) \to C_{m-2}(\mathcal{G}_E, R[G]) \dots C_0(\mathcal{G}_E, R[G]) \to \sum_{i\in E} R[G]^{G_i} \to 0$$

where

$$C_k(\mathcal{G}_E, R[G]) = \prod_{E'\subseteq E,\ |E'|=k+1} R[G]^{\prod_{j\in E'} G_j};$$

here the first product runs over all subsets E' of E with precisely $k+1$ elements.

Let J be a subgroup of G. As

$$R[G]^{\prod_{i\in E} G_i} \ \cong\ R[G/\prod_{i\in E} G_i]$$

is a universally cohomologically trivial $R[G/\prod_{i\in E} G_i]$-module, by the previous lemma 5.6.18 we have that for all $p \geq 0$

$$H^p(J, R[G]^{\prod_{i\in E} G_i}) \cong \big(R[G]^{\prod_{i\in E} G_i} \otimes_R H^p(J \cap \prod_{i\in E} G_i, R)\big)^J \tag{5.6.20}$$

$$\cong R[G]^{J\prod_{i\in E} G_i} \otimes_R H^p(J \cap \prod_{i\in E} G_i, R).$$

We obtain isomorphisms of R-modules for all $p \geq 0$

$$H^p(J, C_k(\mathcal{G}_E, R[G])) \cong H^p(J, \prod_{E'\subseteq E,\ |E'|=k+1} R[G]^{\prod_{j\in E'} G_j}) \tag{5.6.21}$$

$$\cong \bigoplus_{E'\subseteq E,\ |E'|=k+1} \Big\{ R[G]^{J\prod_{j\in E'} G_j} \otimes_R H^p(J \cap \prod_{j\in E'} G_j, R) \Big\}.$$

We now prove the two parts of the proposition separately.

(i) As $\mathcal{G}_E = \{G_i\}_{i\in E}$ is R-admissible, we have that for any subset E' of E

$$G_t \cap \prod_{j\in E'} G_j$$

is a subgroup of G of order which is a unit of R. Hence we have for any subset E' of E and any subgroup J of G_t

$$H^s(J \cap \prod_{j\in E'} G_j, R) = 0 \ \text{ for all } s \geq 1.$$

Hence we obtain from the isomorphism of (5.6.21) that for any subgroup J of G_t

$$H^p(J, C_k(\mathcal{G}_E, R[G])) \cong 0 \ \text{ for all } p \geq 1 \text{ and } k \geq 0.$$

That is to say, $C_k(\mathcal{G}_E, R[G])$ is a cohomologically trivial G_t-module.

Put for all r

$$K_r = \ker\big(C_r(\mathcal{G}_E, R[G]) \ \stackrel{d_r}{\to}\ C_{r-1}(\mathcal{G}_E, R[G])\big)$$

where K_0, K_{-1} are defined to be

$$K_0 = \ker\big(C_0(\mathcal{G}_E, R[G]) \to \sum_{i\in E} R[G]^{G_i}\big)$$

$$K_{-1} = \sum_{i\in E} R[G]^{G_i}.$$

Then we have the exact sequence for all $r \geq 0$

$$0 \to K_r \to C_r(\mathcal{G}_E, R[G]) \to K_{r-1} \to 0.$$

We obtain the long exact sequence of cohomology for any subgroup J of G_t (5.6.22)

$$0 \to H^0(J, K_r) \to H^0(J, C_r(\mathcal{G}_E, R[G])) \to H^0(J, K_{r-1}) \to H^1(J, K_r) \to$$

$$H^1(J, C_r(\mathcal{G}_E, R[G])) \to \dots$$

As $C_k(\mathcal{G}_E, R[G])$ is a cohomologically trivial G_t-module, this long exact sequence (5.6.22) provides isomorphisms, where $m = |E|$,

$$H^s(J, K_{r-1}) \cong H^{s+1}(J, K_r) \cong H^{s+m-r}(J, K_{m-1}) \text{ for all } s \geq 1,\ m-1 \geq r \geq 0.$$

But $K_{m-1} = 0$ hence we have for any subgroup J of G_t

$$H^s(J, K_r) = 0 \text{ for all } s \geq 1 \text{ and } r \geq -1.$$

But $K_{-1} = \sum_{i \in E} R[G]^{G_i}$; hence $\sum_{i \in E} R[G]^{G_i}$ is a cohomologically trivial $R[G_t]$-module.

(ii) Assume that R is a field. As $\{G_i\}_{i \in I}$ is R-admissible, the Hochschild-Serre spectral sequence (or the Künneth formula) shows that for any subset E of I and for all $m \geq 0$

$$H^m(\prod_{i \in E} G_i, R) \cong \bigoplus_{\sum_{i \in E} r_i = m} \bigotimes_{i \in E} H^{r_i}(G_i, R).$$

Hence we have an isomorphism of R-modules (by the isomorphism (5.6.20)),

$$H^m(G, R[G]^{\prod_{i \in E} G_i}) \cong \bigoplus_{\sum_{i \in E} r_i = m} \bigotimes_{i \in E} H^{r_i}(G_i, R).$$

For any subset E of I, we shall write

$$H(\mathbf{r}) = \bigotimes_{i \in E} H^{r_i}(G_i, R)$$

where $\mathbf{r} = (r_{e_1}, \dots, r_{e_t}) \in \mathbb{N}^t$, where $t = |E|$ and $e_1 < e_2 < \dots < e_t$ are the elements of E arranged in ascending order. For $\mathbf{r} = (r_{e_1}, \dots, r_{e_t}) \in \mathbb{N}^t$ we write

$$\sigma(\mathbf{r}) = \sum_{i=1}^{t} r_{e_i}.$$

If $E' \subseteq E$ the inclusion

$$R[G]^{\prod_{i \in E} G_i} \subseteq R[G]^{\prod_{i \in E'} G_i}$$

induces a commutative diagram of homomorphisms of R-modules for all $m \geq 0$

$$\begin{array}{ccc} H^m(G, R[G]^{\prod_{i\in E} G_i}) & \cong & \bigoplus_{\mathbf{r}\in\mathbb{N}^E, \sigma(\mathbf{r})=m} H(\mathbf{r}) \\ \downarrow & & \downarrow \\ H^m(G, R[G]^{\prod_{i\in E'} G_i}) & \cong & \bigoplus_{\mathbf{r}\in\mathbb{N}^{E'}, \sigma(\mathbf{r})=m} H(\mathbf{r}) \end{array}$$

where the right hand vertical arrow is the surjective projection homomorphism onto the submodule $\bigoplus_{\mathbf{r}\in\mathbb{N}^{E'}, \sigma(\mathbf{r})=m} H(\mathbf{r})$ of $\bigoplus_{\mathbf{r}\in\mathbb{N}^{E}, \sigma(\mathbf{r})=m} H(\mathbf{r})$.

We prove the result by induction on n. The result is obvious if $n = 1$. Assume then that $n \geq 2$. Put $J = I \setminus \{n-1\}$ and

$$\Sigma = \sum_{i\in J} R[G/G_{n-1}]^{G_i/(G_i\cap G_{n-1})} \subseteq R[G/G_{n-1}].$$

Then we have the exact sequence of $R[G]$-modules (by example 5.6.3(5) and as $\{G_i\}_{i\in I}$ is R-admissible)

$$0 \to \Sigma \to \left\{ \sum_{i\in J} R[G]^{G_i} \right\} \oplus R[G]^{G_{n-1}} \to \sum_{i\in I} R[G]^{G_i} \to 0.$$

The long exact sequence of cohomology of this sequence is

$$\text{(5.6.23)} \qquad \ldots \to H^m(G, \Sigma) \to H^m(G, \sum_{i\in J} R[G]^{G_i}) \oplus H^m(G, R[G]^{G_{n-1}})$$

$$\to H^m(G, \sum_{i\in I} R[G]^{G_i}) \to H^{m+1}(G, \Sigma) \to \ldots$$

We have the Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i(G/G_{n-1}, H^j(G_{n-1}, \Sigma)) \Rightarrow E^{i+j} = H^{i+j}(G, \Sigma)$$

and an isomorphism of $R[G/G_{n-1}]$-modules (as Σ is flat over R by corollary 5.5.24)

$$H^j(G_{n-1}, \Sigma) \cong H^j(G_{n-1}, R) \otimes_R \Sigma.$$

We obtain the isomorphisms of R-modules

$$E_2^{i,j} \cong H^i(G/G_{n-1}, \Sigma) \otimes_R H^j(G_{n-1}, R).$$

The differentials

$$d_2^{i,j} : E_2^{i,j} \to E_2^{i+2,j-1}$$

of the spectral sequence are then zero for all i, j. We obtain that

$$E_2^{i,j} = E_3^{i,j} = \ldots = E_\infty^{i,j} \text{ for all } i, j.$$

Hence this spectral sequence becomes an isomorphism

$$H^m(G, \Sigma) \cong \bigoplus_{i+j=m} E_2^{i,j} \cong \bigoplus_{i+j=m} H^i(G/G_{n-1}, \Sigma) \otimes_R H^j(G_{n-1}, R).$$

It follows from the definition 5.5.18 that $\{G_i/(G_i \cap G_{n-1})\}_{i\in J}$ is an R-admissible family of subgroups of G/G_{n-1}, as $\{G_i\}_{i\in I}$ is an R-admissible family of subgroups of G. Hence the equality $\Sigma = \sum_{i\in J} R[G/G_{n-1}]^{G_i/(G_i\cap G_{n-1})}$ and the induction hypothesis provides an isomorphism

$$H^i(G/G_{n-1}, \Sigma) \cong \bigoplus_{\substack{r_0\neq 0,\ldots,r_{n-1}\neq 0 \\ \sigma(\mathbf{r})=n+i-2}} \bigotimes_{i\in J} H^{r_i}(G_i/(G_i \cap G_{n-1}), R).$$

As the order of the group $G_i \cap G_{n-1}$ is a unit of R for all $i \neq n-1$, we have isomorphisms for all $i \neq n-1$ and all m, via the Hochschild-Serre spectral sequence,

$$H^m(G_i/(G_i \cap G_{n-1}), R) \cong H^m(G_i, R).$$

Hence we have an isomorphism, where $\mathbf{r} = (r_0, \ldots, r_{n-1})$,

$$H^i(G/G_{n-1}, \Sigma) \cong \bigoplus_{\substack{\mathbf{r}\neq 0 \\ \sigma(\mathbf{r})=n+i-2}} H(\mathbf{r}).$$

Hence we obtain the isomorphism

$$H^m(G, \Sigma) \cong \left\{ \bigoplus_{i+j=m} \bigoplus_{\substack{\mathbf{r}\neq 0 \\ \sigma(\mathbf{r})=n+i-2}} H(\mathbf{r}) \right\} \otimes_R H^j(G_{n-1}, R).$$

We obtain from the induction hypothesis that we have an isomorphism

$$H^m(G, \sum_{i\in J} R[G]^{G_i}) \cong \bigoplus_{\substack{\mathbf{r}\neq 0 \\ \sigma(\mathbf{r})=n+m-2}} H(\mathbf{r}).$$

In the case where $m = 0$, the right hand side of this formula must be interpreted as R. Furthermore, we have an isomorphism

$$H^m(G, R[G]^{G_{n-1}}) \cong H^m(G_{n-1}, R).$$

The long exact sequence of cohomology (5.6.23) then becomes

$$\ldots \to H^m(G,\Sigma) \to \Big\{ \bigoplus_{\substack{\mathbf{r}\neq 0\\ \sigma(\mathbf{r})=n+m-2}} H(\mathbf{r}) \Big\} \ \oplus \ H^m(G_{n-1},R)$$

$$\to H^m(G,\sum_{i\in I} R[G]^{G_i}) \to H^{m+1}(G,\Sigma) \to \ldots$$

This then becomes

$$\ldots \to \bigoplus_{i+j=m} \bigoplus_{\substack{\mathbf{r}\neq 0\\ \sigma(\mathbf{r})=n+i-2}} H(\mathbf{r})\otimes_R H^j(G_{n-1},R) \to \bigoplus_{\substack{\mathbf{r}\neq 0\\ \sigma(\mathbf{r})=n+m-2}} H(\mathbf{r})\oplus H^m(G_{n-1},R)$$

$$\to H^m(G,\sum_{i\in I} R[G]^{G_i}) \to \bigoplus_{i+j=m+1} \bigoplus_{\substack{\mathbf{r}\neq 0\\ \sigma(\mathbf{r})=n+i-2}} H(\mathbf{r}) \otimes_R H^j(G_{n-1},R) \to \ldots$$

The first arrow here

$$H^m(G,\Sigma) \to \Big\{ \bigoplus_{\substack{\mathbf{r}\neq 0\\ \sigma(\mathbf{r})=n+m-2}} H(\mathbf{r}) \Big\} \ \oplus \ H^m(G_{n-1},R)$$

is surjective for all $m \geq 1$ for it corresponds to the projection homomorphism

$$H^m(G,\Sigma) \to E_2^{m,0} \oplus E_2^{0,m}$$

arising from the Hochshild-Serre spectral sequence $E_2^{i,j} \Rightarrow E^{i+j} = H^{i+j}(G,\Sigma)$ given above.

We obtain from the exact sequence (5.6.23) that $H^m(G,\sum_{i\in I} R[G]^{G_i})$ is isomorphic to the kernel of the homomorphism

$$E^{m+1} = H^{m+1}(G,\Sigma) \to \bigoplus_{\substack{\mathbf{r}\neq 0\\ \sigma(\mathbf{r})=n+m-1}} H(\mathbf{r})\oplus H^{m+1}(G_{n-1},R) \cong E_2^{m+1,0}\oplus E_2^{0,m+1}.$$

This kernel is isomorphic to $\bigoplus_{i+j=m,i>0,j>0} E_2^{i,j}$ that is to say isomorphic to

$$\bigoplus_{\substack{i+j=m\\ i>0,\ j>0}} E_2^{i,j} \ \cong \ \bigoplus_{\substack{r_0\neq 0,\ldots,r_{n-1}\neq 0\\ r_0+r_1+\ldots+r_{n-1}=n+m-1}} H(\mathbf{r}).$$

Hence we have an isomorphism of R-modules

$$H^m(G,\sum_{i\in I} R[G]^{G_i}) \cong \bigoplus_{\substack{r_0\neq 0,\ldots,r_{n-1}\neq 0\\ \sigma(\mathbf{r})=n+m-1}} \bigotimes_{i\in I} H^{r_i}(G_i,R)$$

as required.□

5.6.24. Lemma. *Let G be a finite group and let G_0 be a subgroup of G. Suppose that M is an $R[G]$-module and that N, P are $R[G]$-submodules of M. Assume that N is a cohomologically trivial $R[G_0]$-submodule and that $P^{G_0} = P$. Suppose that $P, N \cap P$ and $P/(N \cap P)$ are flat R-modules. Then the inclusion of submodules $P \subseteq P + N$ gives rise to short exact sequences of R-modules for all $m \geq 1$*

$$0 \to (N \cap P) \otimes_R H^m(G_0, R) \to H^m(G_0, P) \to H^m(G_0, P + N) \to 0.$$

Proof. We have the short exact sequence of $R[G]$-modules

$$0 \to P \cap N \to N \oplus P \to N + P \to 0.$$

Taking G_0-cohomology of the last short exact sequence, we obtain the long exact sequence as N is a cohomologically trivial $R[G_0]$-module

(5.6.25)

$$\begin{array}{ccccccc} 0 & \to & N \cap P & \to & N^{G_0} \oplus P & \to & (N+P)^{G_0} \quad \to \\ & & H^1(G_0, N \cap P) & \xrightarrow{f_1} & H^1(G_0, P) & \to & H^1(G_0, N+P) \quad \to \\ & & H^2(G_0, N \cap P) & \xrightarrow{f_2} & H^2(G_0, P) & \to & H^2(G_0, N+P) \quad \dots \end{array}$$

Here, G_0 acts trivially on the module $N \cap P$. The homomorphisms f_i of this exact sequence are induced by the inclusion of flat R-modules $N \cap P \to P$ on which the group G_0 acts trivially and whose cokernel is also a flat R-module, in particular this inclusion is a universal injection. Hence we obtain the commutative diagram of R-modules for all $i \geq 1$

(5.6.26)

$$\begin{array}{ccc} H^i(G_0, N \cap P) & \xrightarrow{f_i} & H^i(G_0, P) \\ \cong\downarrow & & \downarrow\cong \\ (N \cap P) \otimes_R H^i(G_0, R) & \to & P \otimes_R H^i(G_0, R) \end{array}$$

The bottom homomorphism here is an injection hence the maps f_i are injections for all $i \geq 1$.

The long exact sequence (5.6.25) then decomposes into the short exact sequences stated in the lemma. □

5.6.27. Lemma. *Suppose that $\{G_i\}_{i \in I}$, where $I = \{0, \dots, n-1\}$, is an R-admissible family of subgroups of the finite group G. Put*

$$N = \sum_{i=1}^{n-1} R[G]^{G_i}.$$

Then the modules

$$N, \quad R[G]^{G_0}, \quad N \cap R[G]^{G_0}, \quad R[G]^{G_0}/N \cap R[G]^{G_0}$$

are finite flat R-modules.

Proof. Put

$$e_i = \sum_{g \in G_i} g.$$

Then we have $R[G]^{G_i} = e_i R[G]$. Hence $R[G]^{G_i}$ is a finite free R-module for all i.

The module N is a finite flat R-module as $\{G_i\}_{i=1,\dots,n-1}$ is R-admissible (corollary 5.5.24). We have (by example 5.6.3(5))

$$e_0 R[G] \cap N = \sum_{i=1}^{n-1} e_0 e_i R[G].$$

We obtain the isomorphism of $R[G]$-modules

$$e_0 R[G] \cap N \cong \sum_{i=1}^{n-1} e_i R[G/G_0].$$

But $\{G_i G_0/G_0\}_{i=1,\dots,n-1}$ is an R-admissible family of subgroups of G/G_0, as $\{G_i\}_{i\in I}$ is R-admissible; hence $\sum_{i=1}^{n-1} e_i R[G/G_0]$ is a finite flat R-module (corollary 5.5.24) and hence $e_0 R[G] \cap N$ is a finite flat R-module.

By corollary 5.5.24 we have the universal exact sequence of R-modules for the R-admissible family $\{G_i\}_{i=0,\dots,n-1}$, where $G_\infty = \bigcap_{i=0}^{n-1} G_i$,

$$0 \to R[G]^{\prod_{i\in I} G_i} \to \prod_{i_0 \in I} R[G]^{\prod_{j\neq i_0} G_j} \to \prod_{\substack{(i_0,i_1)\in I^2 \\ i_0<i_1}} R[G]^{\prod_{j\neq i_0,i_1} G_j} \to \dots$$

$$\to \prod_{\substack{i_0<i_1 \\ i_0,i_1\in I}} R[G]^{G_{i_0}G_{i_1}} \to \prod_{i\in I} R[G]^{G_i} \to R[G]^{G_\infty} \to R[G]^{G_\infty}/\sum_{i\in I} R[G]^{G_i} \to 0.$$

This is a resolution of $R[G]^{G_\infty}/\sum_{i\in I} R[G]^{G_i}$ by finite free R-modules; hence tensoring this universally exact free resolution with $- \otimes_R S$ for any R-algebra S we obtain that

$$\mathrm{Tor}_j^R(R[G]^{G_\infty}/\sum_{i\in I} R[G]^{G_i}, S) = 0 \quad \text{for all } j \geq 1.$$

Hence $R[G]^{G_\infty}/\sum_{i\in I} R[G]^{G_i}$ is a finite flat R-module. We have the exact sequence of R-modules

$$0 \to R[G]^{G_\infty}/\sum_{i\in I} R[G]^{G_i} \to R[G]/\sum_{i\in I} R[G]^{G_i} \to R[G]/R[G^\infty] \to 0.$$

But the two outer terms of this sequence are finite flat R-modules; hence the middle term $R[G]/\sum_{i\in I} R[G]^{G_i}$ is also a finite flat R-module. Applying this to the R-admissible family of subgroups $\{G_i G_0/G_0\}_{i=1,\dots,n-1}$ of G/G_0

it follows that

$$e_0 R[G]/(e_0 R[G] \cap N)$$

is a finite flat R-module. □

5.6.28. Proposition. *Suppose that* $\{G_i\}_{i\in I}$, *where* $I = \{0, \ldots, n-1\}$, *is an* R*-admissible family of subgroups of the finite group* G. *Put*

$$e_i = \sum_{g\in G_i} g, \quad e_{ij} = \sum_{g\in G_i G_j} g.$$

Suppose also we have the equation in $\mathrm{Coch}^m(G_0, R[G])$

$$\delta = \sum_{i\in I} e_i \eta_i$$

where $\delta \in \mathrm{Cocy}^m(G_0, R[G])$ *and* $e_i\eta_i \in \mathrm{Coch}^m(G_0, e_i R[G])$ *and* $m \geq 1$. *Then there are cochains*

$$u^{(i,j)} \in \mathrm{Coch}^m(G_0, R[G]) \quad \text{for all } i \neq j \text{ and } 0 \leq i, j \leq n-1$$

such that

$$u^{(i,j)} = -u^{(j,i)}, \quad \text{for all } i \neq j \text{ and } 0 \leq i, j \leq n-1,$$

and cochains $\delta_i \in \mathrm{Coch}^m(G_0, R[G])$ *for all* $i \geq 0$ *where we have*

$$e_i\eta_i = e_i\delta_i + \sum_{j\neq i} e_{ij} u^{(i,j)} \quad \text{for all } i \geq 0, \quad \delta = \sum_{i\in I} e_i\delta_i,$$

where $e_i\delta_i \in \mathrm{Cob}^m(G_0, e_i R[G])$ *is an* m*-coboundary for all* $i \geq 1$ *and is an* m*-cocycle for* $i = 0$.

Proof. The case where $n = 1$. We have the equation

$$\delta(g) = e_0\eta_0(g) \text{ for all } g \in G_0^m.$$

In this case there is nothing further to prove.

The general case where $n \geq 2$. We put, in the notation of lemma 5.6.24,

$$N = e_1 R[G] + \ldots + e_{n-1} R[G], \quad M = R[G], \quad P = e_0 R[G].$$

By the previous lemma 5.6.27, we have that $N, P, N \cap P$, and $P/(N \cap P)$ are finite flat R-modules; by proposition 5.6.19(i), N is a cohomologically trivial $R[G_0]$-module.

From lemma 5.6.24 we then obtain exact sequences for all $m \geq 1$

$$0 \to (e_0 R[G] \cap N) \otimes_R H^m(G_0, R) \to H^m(G_0, e_0 R[G]) \to$$

$$H^m(G_0, e_0 R[G] + N) \to 0.$$

The m-cocycle δ of the proposition has cohomology class in $H^m(G_0, e_0 R[G] + N)$. From this exact sequence, it follows that there is an m-cocycle

$$\epsilon \in \mathrm{Cocy}^m(G_0, e_0 R[G])$$

and a coboundary

$$\zeta_1 \in \mathrm{Cob}^m(G_0, e_0 R[G] + N)$$

such that

$$\delta = \epsilon + \zeta_1.$$

Therefore there is a $m-1$-cochain

$$\zeta_2 \in \mathrm{Coch}^{m-1}(G_0, e_0 R[G] + N)$$

such that

$$\zeta_1 = \partial^{m-1} \zeta_2.$$

We may write

$$\zeta_2 = \sum_{i \geq 0} e_i \theta_i$$

where

$$\theta_i \in \mathrm{Coch}^{m-1}(G_0, R[G]) \text{ for all } i.$$

Hence we have

$$\zeta_1 = \partial^{m-1}(\zeta_2) = \sum_{i \geq 0} e_i \partial^{m-1}(\theta_i).$$

We may write

$$\delta = \epsilon + \zeta_1 = \epsilon + \sum_{i \geq 0} e_i \partial^{m-1}(\theta_i).$$

As we also have $\delta = \sum_{i \geq 0} e_i \eta_i$ this gives for all $g \in G_0^m$

$$-\epsilon(g) + e_0(\eta_0(g) - \partial^{m-1}(\theta_0)(g)) + \sum_{i \geq 1} e_i(\eta_i(g) - \partial^{m-1}(\theta_i)(g)) = 0.$$

For each $g \in G_0^m$ this is an equation of the form $\sum_{i \geq 0} e_i x_i = 0$ where $x_i \in R[G]$ for all i; by corollary 5.5.30, there are cochains

$$u^{(i,j)} \in \mathrm{Coch}^m(G_0, R[G]) \text{ for all } i \neq j$$

such that

$$u^{(i,j)} = -u^{(j,i)} \text{ for all } i \neq j$$

and where

$$e_i(\eta_i - \partial^{m-1}(\theta_i)) = \sum_{j \neq i} e_{ij} u^{(i,j)} \quad \text{for all } i \geq 1.$$

and

$$-\epsilon + e_0(\eta_0 - \partial^{m-1}(\theta_0)) = \sum_{j \neq 0} u^{(0,j)}.$$

Putting

$$e_i \delta_i = \begin{cases} e_i \partial^{m-1}(\theta_i) & \text{for } i \geq 1 \\ \epsilon + e_0 \partial^{m-1}(\theta_0) & \text{for } i = 0 \end{cases}$$

we obtain the result as $\epsilon \in \mathrm{Cocy}^m(G_0, e_0 R[G])$. □

5.6.29. Proposition. *Let $\{G_i\}_{i \in I}$, where $I = \{0, \ldots, n-1\}$, be an R-admissible family of subgroups of the finite group G. Let e_i, e_{ij} be the elements of $R[G]$ as in proposition 5.6.28. Suppose also we have the equation in $\mathrm{Coch}^m(G_0, R[G])$, where $m \geq 1$,*

$$e_0 \eta_0 = \sum_{i \in I} \partial^{m-1}(e_i \zeta_i)$$

where $e_0\eta_0$ is an m-cocycle in $\mathrm{Cocy}^m(G_0, e_0 R[G])$ and

$$e_i \zeta_i \in \mathrm{Coch}^{m-1}(G_0, e_i R[G])$$

are $m-1$-cochains for all $i = 0, \ldots, n-1$. Then there are cochains

$$u^{(i,j)} \in \mathrm{Coch}^{m-1}(G_0, R[G]) \quad \text{for all } i \neq j \text{ and } 0 \leq i, j \leq n-1$$

such that

$$u^{(i,j)} = -u^{(j,i)}, \quad \text{for all } i \neq j \text{ and } 0 \leq i, j \leq n-1,$$

and a finite set M and cocycles $f_{ik} \in \mathrm{Cocy}^m(G_0, R)$, for all $i \geq 1$ and all $k \in M$, and elements $\theta_{ik} \in e_{0i} R[G]$, for all $i \geq 1$ and all $k \in M$, and a coboundary $\epsilon \in \mathrm{Cob}^m(G_0, e_0 R[G])$ such that

$$\partial^{m-1}(e_i \zeta_i) = \sum_{k \in M} f_{ik} \otimes \theta_{ik} + \sum_{\substack{j \neq i \\ 0 \leq j \leq n-1}} e_{ij} \partial^{m-1} u^{(i,j)} \quad \text{for all } i \geq 1$$

$$\partial^{m-1}(e_0 \zeta_0) = \epsilon + \sum_{j \neq 0} e_{0i} \partial^{m-1} u^{(0,j)}.$$

Proof. For $n = 1$ there is nothing to prove so we may assume that $n \geq 2$. Put, with the notation of lemma 5.6.24,

$$N = e_1 R[G] + \ldots + e_{n-1} R[G], \quad M = R[G], \quad P = e_0 R[G].$$

By lemma 5.6.27, we have that $N, P, N \cap P$, and $P/(N \cap P)$ are finite flat R-modules; by proposition 5.6.19(i), N is a cohomologically trivial $R[G_0]$-module.

From lemma 5.6.24 we then obtain exact sequences for all $m \geq 1$, where $P = e_0 R[G]$,

$$0 \to (P \cap N) \otimes_R H^m(G_0, R) \to H^m(G_0, P) \to H^m(G_0, P + N) \to 0.$$

The equation

$$e_0\eta_0 = \sum_{i \in I} \partial^{m-1}(e_i\zeta_i)$$

shows that the cocycle $e_0\eta_0$ induces a cohomology class in $H^m(G_0, e_0R[G])$ which lies in the kernel of the homomorphism

$$H^m(G_0, e_0R[G]) \to H^m(G_0, e_0R[G] + N).$$

By the above exact sequence, the cohomology class of $e_0\eta_0$ therefore lies in

$$(e_0R[G] \cap N) \otimes_R H^m(G_0, R).$$

By example 5.6.3(5) we have

$$N \cap e_0R[G] = \sum_{i=1}^{n-1} \big(e_0R[G] \cap e_iR[G]\big) = \sum_{i=1}^{n-1} e_{0i}R[G].$$

Hence the cohomology class of $e_0\eta_0$ lies in

$$(\sum_{i=1}^{n-1} e_{0i}R[G]) \otimes_R H^m(G_0, R).$$

We obtain that there are cocycles $f_{ik} \in \mathrm{Cocy}^m(G_0, R)$ for all $i = 1, \ldots, n-1$ and for all $k \in M$ where M is a finite set, elements $\theta_{ik} \in e_{0i}R[G]$ for all $i \geq 1$ and all $k \in M$, and a coboundary $\epsilon \in \mathrm{Cob}^m(G_0, e_0R[G])$ such that

$$e_0\eta_0 = \epsilon + \sum_{i \geq 1} \sum_{k \in M} f_{ik} \otimes \theta_{ik}.$$

We may write

$$\theta_{ik} = e_0 e_i \Theta_{ik}$$

for all $i \geq 1$ and $k \in M$ where $\Theta_{ik} \in R[G]$. We then have

$$e_0\eta_0 = \sum_{i \in I} \partial^{m-1}(e_i\zeta_i)$$

$$= \epsilon + \sum_{i \geq 1} \sum_{k \in M} f_{ik} \otimes e_0 e_i \Theta_{ik}.$$

Let $E_{f_{ik}} \in \mathrm{Coch}^{m-1}(G_0, R[G])$ be the Kolyvagin element attached to the cocycle $f_{ik} \in \mathrm{Cocy}^m(G_0, R)$ (definition 5.6.11). As $\partial^{m-1} E_{f_{ik}} = e_0 f_{ik}$, we then have the equation

$$e_0\eta_0 = \sum_{i\in I} \partial^{m-1}(e_i\zeta_i)$$

$$= \epsilon + \sum_{i\geq 1}\sum_{k\in M} \partial^{m-1} E_{f_{ik}} \otimes e_i\Theta_{ik}.$$

As $\epsilon \in \mathrm{Cob}^m(G_0, e_0R[G])$ there is $\mu \in \mathrm{Coch}^{m-1}(G_0, R[G])$ such that

$$\epsilon = \partial^{m-1}(e_0\mu).$$

We then have the equation

$$\sum_{i\in I} \partial^{m-1}(e_i\zeta_i)$$

$$= e_0\partial^{m-1}\mu + \sum_{i\geq 1}\sum_{k\in M} e_i\big(\partial^{m-1} E_{f_{ik}} \otimes \Theta_{ik}\big).$$

We obtain

$$e_0\partial^{m-1}(\zeta_0 - \mu) + \partial^{m-1}\sum_{i=1}^{n-1} e_i(\zeta_i - \sum_{k\in M} E_{f_{ik}} \otimes \Theta_{ik}) = 0.$$

Hence we have that

$$h = e_0(\zeta_0 - \mu) + \sum_{i=1}^{n-1} e_i(\zeta_i - \sum_{k\in M} E_{f_{ik}} \otimes \Theta_{ik})$$

is a cocycle in $\mathrm{Cocy}^{m-1}(G_0, R[G])$; as $R[G]$ is cohomologically trivial, there is a cochain $c \in \mathrm{Coch}^{m-2}(G_0, R[G])$ such that $h = \partial^{m-2}c$. We then obtain the equality of cochains in $\mathrm{Coch}^{m-1}(G_0, R[G])$

$$\partial^{m-2}c = e_0(\zeta_0 - \mu) + \sum_{i=1}^{n-1} e_i(\zeta_i - \sum_{k\in M} E_{f_{ik}} \otimes \Theta_{ik}).$$

We may now apply proposition 5.6.28 to this equation. We obtain that there are cochains

$$u^{(i,j)} \in \mathrm{Coch}^{m-1}(G_0, R[G]), \quad \text{for all } i \neq j \text{ and } 0 \leq i, j \leq n-1,$$

such that

$$u^{(i,j)} = -u^{(j,i)}, \quad \text{for all } i \neq j \text{ and } 0 \leq i, j \leq n-1,$$

and cochains $\delta_i \in \mathrm{Coch}^m(G_0, R[G])$ for all $i \geq 0$ where we have

$$e_0(\zeta_0 - \mu) = e_0\delta_0 + \sum_{j\neq 0} e_{0j}u^{(0,j)}$$

$$e_i(\zeta_i - \sum_{k\in M} E_{f_{ik}} \otimes \Theta_{ik}) = e_i\delta_i + \sum_{j\neq i} e_{ij}u^{(i,j)}, \quad \text{for all } i \geq 1,$$

where $e_i\delta_i \in \mathrm{Cob}^{m-1}(G_0, e_iR[G])$ is an $(m-1)$-coboundary for all $i \geq 1$ and is an $(m-1)$-cocycle for $i = 0$.

We obtain

$$\partial^{m-1}(e_0\zeta_0) = \partial^{m-1}e_0\mu + \sum_{j\neq 0} e_{0j}\partial^{m-1}u^{(0,j)}$$

$$\partial^{m-1}(e_i\zeta_i) = \partial^{m-1}(\sum_{k\in M} E_{f_{ik}} \otimes e_i\Theta_{ik}) + \sum_{j\neq i} e_{ij}\partial^{m-1}u^{(i,j)} \quad \text{for all } i \geq 1.$$

That is to say we have

$$\partial^{m-1}(e_i\zeta_i) = \sum_{k\in M} f_{ik} \otimes \theta_{ik} + \sum_{j\neq i} e_{ij}\partial^{m-1}u^{(i,j)} \quad \text{for } i \geq 1$$

$$\partial^{m-1}(e_0\zeta_0) = \epsilon + \sum_{j\neq 0} e_{0j}\partial^{m-1}u^{(0,j)}$$

where $\epsilon \in \mathrm{Cob}^m(G_0, e_0R[G])$ as required.□

5.7 Basic properties of the Heegner module

This section contains no proofs; the assertions of this section are proved in §5.8.

(5.7.1) The notation we use is that of the two sections §§5.2,5.3; in résumé we have:

K/F is an imaginary quadratic extension field of F, with respect to ∞;
B is the integral closure of A in K;
$\tilde{I}$ is a finite subset of Σ_F;
R is a commutative ring;
$\rho : \Sigma_F \setminus \tilde{I} \quad \to \quad R$, $v \mapsto a_v$, is a map with values in R from the set of places $\Sigma_F \setminus \tilde{I}$ of the global field F;
$c \in \mathrm{Div}_+(A)$;
Δ_c is the integral group algebra $\mathbb{Z}[\mathrm{Pic}(O_c)]$ where $c \in \mathrm{Div}_+(A)$;
$\Delta_{\leq c} = \bigoplus_{c'\in \mathrm{Div}_+(A), c'\leq c} \Delta_{c'}$;

$\Delta = \bigoplus_{c\in \mathrm{Div}_+(A)} \Delta_c$;

$t^{\Delta}_{c,c-z} : \Delta \to \Delta$ is a transition homomorphism where $c \in \mathrm{Div}_+(A)$ and z is a prime divisor in the support of c; it is induced by the natural surjective group homomorphism $t_{c,c-z} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c-z})$ (see (5.2.2));

$e_{c,c-z} = \sum_{x\in \ker(t_{c,c-z})} x \in \Delta_c$ (see (5.3.3));

$K_{c,c-z}$ and $\tilde{K}_{c,c-z}$ are the homomorphisms $\Delta \otimes_{\mathbb{Z}} R \to \Delta \otimes_{\mathbb{Z}} R$ defined in (5.3.4) and (5.3.6);

$\mathcal{H}(\rho) = \varinjlim_{c\in \mathrm{Div}_+(A)} \mathcal{H}_c$ is the Heegner module of ρ and K/F with coefficients in R defined in (5.3.8)-(5.3.11).

We sometimes write $\Delta_{c,R}$ in place of the tensor product $\Delta_c \otimes_{\mathbb{Z}} R$.

(5.7.2) We recall that the homomorphism $t^{\Delta}_{c,c-z} : \Delta \to \Delta$ is the extension by zero of the transition homomorphism (see (5.2.2))

$$t^{\Delta}_{c,c-z} : \Delta_c \to \Delta_{c-z}.$$

Similarly, the homomorphisms

$$\tilde{K}_{c,c-z}, K_{c,c-z} \quad : \Delta \otimes_{\mathbb{Z}} R \to \Delta \otimes_{\mathbb{Z}} R$$

are the extensions by zero of the homomorphisms (see (5.3.4), (5.3.6))

$$\tilde{K}_{c,c-z}, K_{c,c-z} \quad : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\le c} \otimes_{\mathbb{Z}} R.$$

5.7.3. Proposition. *The Heegner module $\mathcal{H}(\rho)$ is isomorphic to the quotient of discrete* $\mathrm{Gal}(K^{\mathrm{sep}}/K)$*-modules*

$$\mathcal{H}(\rho) \;\cong\; \frac{\Delta \otimes_{\mathbb{Z}} R}{< K_{c,c-z}(\Delta_c \otimes_{\mathbb{Z}} R),\ \textit{for all } c \in \mathrm{Div}_+(A),\ z \in \mathrm{Supp}(c) \setminus \tilde{I} >}.$$

(5.7.4) We put

$$\mathcal{H}'_c = \mathrm{coker}\Big(\bigoplus_{0\le d<c} \Delta_d \otimes_{\mathbb{Z}} R \quad \to \quad \mathcal{H}_c \Big).$$

That is to say, $\mathcal{H}'_c$ is the largest quotient of $\mathcal{H}_c$ through which factor the cokernels of the transition homomorphisms $\mathcal{H}_d \to \mathcal{H}_c$ for all $d < c$.

5.7.5. Proposition. *Let n denote the image in R of the integer $|B^*|/|A^*|$. Let c be a divisor in $\mathrm{Div}_+(A)$.*
(i) *If n is a unit of R then $\mathcal{H}'_c$ is a finite free R-module for all c.*
(ii) *If c is a prime divisor then we have isomorphisms of R-modules for some integers $s, t \geq 0$*

$$\mathcal{H}'_c \cong R^t \oplus \left(\frac{R}{nR}\right)^s.$$

5.7.6. Proposition. (i) *The module $\mathcal{H}_0$ is a finite free R-module.*
(ii) *If c is a prime divisor in $\mathrm{Div}_+(A)$ and if n is a unit in R then $\mathcal{H}_c$ is a finite free R-module.*

(5.7.7) We put

$$t_z^{\Delta} = \bigoplus_{c \in \mathrm{Div}_+(A),\ c \geq z} t_{c,c-z}^{\Delta} : \Delta \to \Delta.$$

That is to say t_z^{Δ} is the direct sum of all the transition morphisms $t_{c,c-z}^{\Delta} : \Delta \to \Delta$ for those effective divisors c with $c \geq z$.

5.7.8. Proposition. *Let z and w be two prime components in $\mathrm{Supp}(c) \setminus \tilde{I}$, where c is any divisor in $\mathrm{Div}_+(A)$.*
(i) *We have, where 1_c denotes the multiplicative identity of the ring Δ_c,*

$$t_{c,c-z}^{\Delta}(e_{c,c-w}) = \begin{cases} |\ker(t_{c,c-z})|.1_c, & \text{if } z = w; \\ \frac{|O^*_{c-z-w}|}{|A^*|} e_{c-z,c-z-w}, & \text{if } z \neq w. \end{cases}$$

(ii) *We have $t_w^{\Delta} \circ \epsilon(c, z) = \epsilon(c - w, z) \circ t_w^{\Delta}$ if $w \neq z$ (see (5.3.5)).*
(iii) *If $z \neq w$ then we have*

$$t_w^{\Delta} \circ K_{c,c-z} = K_{c-w,c-z-w} \circ t_w^{\Delta}.$$

5.8 Proofs of the propositions of §5.7

In this section we give some further technical results on the Heegner module as well as the proofs of the results of the preceding section.

(5.8.1) The notation is that of (5.7.1) with the following extra notation.

5.8.2. Notation. Let E be a finite subset of $\mathrm{Div}_+(A)$.
(1) We say that E is *saturated* if it satisfies this condition:

$$c \in \mathrm{Div}_+(A),\ d \in E,\ \text{ and } 0 \le c \le d \ \Rightarrow\ c \in E.$$

(2) Let $z_1, \dots, z_n$ be prime divisors of $\mathrm{Div}_+(A)$ such that $z_i \notin \tilde{I}$ for all i. We write

$$\Gamma(E|z_1, \dots, z_n)$$

for the subgroup of $\Delta \otimes_{\mathbb{Z}} R$ generated by $K_{c',c'-z_i}(\Delta_{c'} \otimes_{\mathbb{Z}} R)$, for $i = 1, \dots, n$ where c' runs over all elements of E for which $c' - z_i \ge 0$ for some i; that is to say

$$\Gamma(E|z_1, \dots, z_n) = \sum_{i=1}^{n} \sum_{\substack{c' \in E \\ \text{where } c' \ge z_i}} K_{c',c'-z_i}(\Delta_{c'} \otimes_{\mathbb{Z}} R).$$

(3) Put

$$\Delta(E) = \bigoplus_{c \in E} \Delta_c.$$

If E is saturated let P be the finite set of prime divisors of E which do not lie in $\tilde{I}$ and put

$$\mathcal{H}(E) = (\Delta(E) \otimes_{\mathbb{Z}} R)/\Gamma(E|P).$$

5.8.3. Remarks. (1) If E is a finite saturated subset of $\mathrm{Div}_+(A)$ of divisors, the primes $z_1, \dots, z_n$ in the module $\Gamma(E|z_1, \dots, z_n)$ are usually all prime divisors of E which do not belong to $\tilde{I}$ i.e. the primes z_i form the set $\mathrm{Supp}(E) \setminus \tilde{I}$. In this event we write $\Gamma(E)$ in place of $\Gamma(E|z_1, \dots, z_n)$. With this notation, for finite saturated subsets E, E' of $\mathrm{Div}_+(A)$ we then have the evident properties

$$\Gamma(E) \subseteq \Gamma(E') \quad \text{if} \quad E \subseteq E';$$

$$\Gamma(E) + \Gamma(E') = \Gamma(E \cup E').$$

(2) Note that if c is an element of $\mathrm{Div}_+(A)$ and

$$E = \{c' \in \mathrm{Div}_+(A) |\ c' \le c\}$$

then we have

$$\Gamma_{\le c} = \Gamma(E|\ \mathrm{Supp}(c) \setminus \tilde{I}) = \Gamma(E)$$

and also

$$\mathcal{H}_c = \mathcal{H}(E).$$

5.8.4. Proposition. *Let $c \in \mathrm{Div}_+(A)$ and $z_1, \ldots, z_n$ be distinct prime divisors in* $\mathrm{Supp}(c)$. *Put $c' = c - \sum_{i=1}^n z_i$. Then we have:*
(i) *The family of subgroups*

$$\{\ker(t_{c,c'+z_i})\}_{i=1,\ldots,n}$$

of $\mathrm{Pic}(O_c)$ *is a molecule with atoms* $\{\ker(t_{c,c-z_i})\}_{i=1,\ldots,n}$.
(ii) *The kernel of the group homomorphism (where $\prod$ denotes the direct product)*

$$\begin{array}{rcl} \prod_{i=1}^n \ker(t_{c,c-z_i}) & \to & \mathrm{Pic}(O_c) \\ (h_1, \ldots, h_n) & \mapsto & h_1 h_2 \ldots h_n \end{array}$$

has order which divides the integer $|B^*|/|A^*|$. If $c' > 0$ this homomorphism is injective.
(iii) *If the image in R of the integer $|B^*|/|A^*|$ is a unit then* $\{\ker(t_{c,c-z_i})\}_{i=1,\ldots,n}$ *is an R-admissible family of subgroups of* $\mathrm{Pic}(O_c)$.

Proof. For any effective divisors $c \geq d$ on $X = \mathrm{Spec}\ A$, we have morphisms of A-schemes

$$f : V = \mathrm{Spec}\ O_c \ \to \ X, \quad g : W = \mathrm{Spec}\ O_d \ \to \ X$$

obtained from the inclusions $A \subset O_c \subset O_d$. Similarly as in (2.2.13), we obtain an exact sequence of sheaves of abelian groups for the Zariski topology on X

$$0 \to f_* \mathcal{O}_V^* \to g_* \mathcal{O}_W^* \to \mathcal{K} \to 0$$

where $\mathcal{K}$ is a skyscraper sheaf on X with support contained in the finite set of points of X where c and d differ. The long exact sequence of cohomology then gives an exact sequence of abelian groups

$$0 \to O_c^* \to O_d^* \to H^0(X, \mathcal{K}) \to H^1(X, f_* \mathcal{O}_V^*) \to H^1(X, g_* \mathcal{O}_W^*) \to 0$$

where we evidently have $H^1(X, \mathcal{K}) = 0$. Furthermore we have

$$H^1(X, f_* \mathcal{O}_V^*) = \mathrm{Pic}(O_c)$$

$$H^1(X, g_* \mathcal{O}_W^*) = \mathrm{Pic}(O_d).$$

This gives the exact sequence of abelian groups

$$0 \to O_c^* \to O_d^* \to H^0(X, \mathcal{K}) \to \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_d) \to 0.$$

With the notation of the proposition, if $n = 1$ there is nothing to prove; hence we may assume that $n \geq 2$. We then have that $c' + z_i > 0$ for all i, where $c' = c - \sum_{i=1}^n z_i$. Hence the natural homomorphism $O_c^* \to O_{c'+z_i}^*$ is an isomorphism for all i. Putting $d = c' + z_i$, we define the sheaf $\mathcal{K}_i$ as the cokernel

$$0 \to f_* \mathcal{O}_V^* \to g_* \mathcal{O}_W^* \to \mathcal{K}_i \to 0.$$

The above exact sequence of abelian groups becomes an isomorphism for all i

$$H^0(X, \mathcal{K}_i) \cong \ker(t_{c,c'+z_i}).$$

In particular we have injections

$$H^0(X, \mathcal{K}_i) \hookrightarrow \mathrm{Pic}(O_c)$$

for all i.

For any closed point z of X, with corresponding prime ideal $\mathfrak{p}$ of A, we then have that the stalk $\mathcal{K}_{i,z}$ of $\mathcal{K}_i$ at z is given by (see (2.2.10) and (2.2.11))

$$\mathcal{K}_{i,z} = (O_{c'+z_i} \otimes_A A_\mathfrak{p})^* / (O_c \otimes_A A_\mathfrak{p})^*.$$

We have

$$H^0(\mathrm{Spec}\ A, \mathcal{K}_i) = \prod_z \mathcal{K}_{i,z}$$

where the product runs over all primes z of the form z_j for all $j \neq i$. Furthermore, we have isomorphisms of A-algebras

$$O_{c'+z_i} \otimes_A A_\mathfrak{p} \ \cong O_{c'+z_j} \otimes_A A_\mathfrak{p}$$

for all i, j such that $z \neq z_i$ and $z \neq z_j$. As the stalks $\mathcal{K}_{i,z}$ are subgroups of $\mathrm{Pic}(O_c)$, It follows that we have equalities of stalks as subgroups of $\mathrm{Pic}(O_c)$

$$\mathcal{K}_{i,z} = \mathcal{K}_{j,z}$$

for all i, j such that $z \neq z_i$ and $z \neq z_j$. Hence the groups $\mathcal{K}_i = \prod_z \mathcal{K}_{i,z}$, $i = 1, \ldots, n$, form a molecule of subgroups of $\mathrm{Pic}(O_c)$ whose atoms are the subgroups $\mathcal{K}_{i,z}$ for all i, z. That is to say the atoms are the subgroups $\ker(t_{c,c-z_i})$ for all i. This proves part (i).

Clearly part (iii) follows from part (ii). To prove part (ii), we obtain from the above an exact sequence of finite abelian groups

$$0 \to O_c^* \to O_{c'}^* \to \prod_{i=1}^n \ker(t_{c,c-z_i}) \to \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c'}) \to 0.$$

(This also follows from the computation of the groups $\ker(t_{c,c'})$ of (2.2.13) and (2.2.15).) It follows that the homomorphism $\prod_{i=1}^n \ker(t_{c,c-z_i}) \to \mathrm{Pic}(O_c)$ is injective if $c' > 0$ and its kernel is isomorphic to B^*/A^* if $c' = 0$. □

Proof of proposition 5.7.3. The groups $\mathcal{H}_c$ are defined by the exact sequence (see (5.3.8))

$$0 \to \Gamma_{\leq c} \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R \to \mathcal{H}_c \to 0.$$

Passing to the direct limit over all $c \in \mathrm{Div}_+(A)$, this sequence remains exact and we obtain the exact sequence

$$0 \to \varinjlim \Gamma_{\leq c} \to \Delta \otimes_{\mathbb{Z}} R = \varinjlim(\Delta_{\leq c} \otimes_{\mathbb{Z}} R) \to \mathcal{H}(\rho) \to 0.$$

As we have an evident isomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\varinjlim \Gamma_{\leq c} \quad \cong \quad < K_{c,c-z}(\Delta_c \otimes_{\mathbb{Z}} R), \text{ for all } c \in \mathrm{Div}_+(A),\ z \in \mathrm{Supp}(c) \setminus \tilde{I} >$$

the result holds.□

Proof of proposition 5.7.5. Put

$$\Delta_{<c} = \bigoplus_{c' < c,\ c' \in \mathrm{Div}_+(A)} \Delta_{c'}.$$

By (5.3.5) and (5.3.6) the reduction modulo $\Delta_{<c} \otimes_{\mathbb{Z}} R$ of $K_{c',c'-z}$ where $c' \leq c$ is the homomorphism $\Delta_c \otimes_{\mathbb{Z}} R \to \Delta_c \otimes_{\mathbb{Z}} R$ given by

$$K_{c',c'-z} \equiv \begin{cases} -\frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z} & (\mathrm{mod}\ \Delta_{<c} \otimes_{\mathbb{Z}} R) \\ 0 \end{cases} \quad \begin{cases} \text{if} \quad c = c' \\ \text{if} \quad c \neq c'. \end{cases}$$

The module $\mathcal{H}'_c$ is the quotient of $\mathcal{H}_c$ by the image in $\mathcal{H}_c$ of $\Delta_{<c} \otimes_{\mathbb{Z}} R$; hence $\mathcal{H}'_c$ is $\Delta_c \otimes_{\mathbb{Z}} R$-isomorphic to the quotient of $\Delta_c \otimes_{\mathbb{Z}} R$ by the submodule

$$\sum_z \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z}(\Delta_c \otimes_{\mathbb{Z}} R) \tag{5.8.5}$$

where the sum runs through all prime components z in the support of c for which $z \notin \tilde{I}$.

Let J_c be the quotient of Δ_c by the Δ_c-submodule

$$\sum_z \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z} \Delta_c$$

where the sum runs through all prime components z in the support of c for which $z \notin \tilde{I}$. We have the short exact sequence of finite $\mathbb{Z}$-modules

$$0 \to \sum_z \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z} \Delta_c \to \Delta_c \to J_c \to 0.$$

Tensoring this sequence with $- \otimes_{\mathbb{Z}} R$ we obtain an isomorphism of $\Delta_c \otimes_{\mathbb{Z}} R$-modules

$$\mathcal{H}'_c \cong J_c \otimes_{\mathbb{Z}} R. \tag{5.8.6}$$

We now distinguish the two cases of the proposition.

(i) Assume that n is a unit of the ring R. Let S be the multiplicative subset of $\mathbb{Z}$ generated by the integer $|B^*|/|A^*|$. Let $\mathbb{Z}^{(n)}$ be fraction ring $S^{-1}\mathbb{Z}$ which is the subring of $\mathbb{Q}$ of rational numbers with denominators which are elements of S. We then obtain the exact sequence of $\Delta_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)}$-modules

$$0 \to \sum_z e_{c,c-z}\Delta_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)} \to \Delta_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)} \to J_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)} \to 0 \tag{5.8.7}$$

where the sum runs through the set $E = \mathrm{Supp}(c) \setminus \tilde{I}$ of all prime components z in the support of c for which $z \notin \tilde{I}$.

By proposition 5.8.4, the family of subgroups $\{\ker(t_{c,c-z})\}_{z\in E}$ of $\mathrm{Pic}(O_c)$ is $\mathbb{Z}^{(n)}$-admissible, as the image of $|B^*|/|A^*|$ in $\mathbb{Z}^{(n)}$ is a unit of this ring $\mathbb{Z}^{(n)}$. Fix a total ordering $<$ of the finite set E and put

$$G = \mathrm{Pic}(O_c), \quad G_z = \ker(t_{c,c-z})$$

and

$$G_\infty = \bigcap_{z\in E} G_z.$$

We then obtain from corollary 5.5.24 the universal exact sequence of $\mathbb{Z}^{(n)}$-modules

$$0 \to \mathbb{Z}^{(n)}[G]^{\prod_{j\in E} G_j} \to \prod_{i_0\in E} \mathbb{Z}^{(n)}[G]^{\prod_{j\neq i_0} G_j} \to \prod_{\substack{(i_0,i_1)\in E^2 \\ i_0<i_1}} \mathbb{Z}^{(n)}[G]^{\prod_{j\neq i_0,i_1} G_j} \to$$

$$\ldots \to \prod_{j\in E} \mathbb{Z}^{(n)}[G]^{G_j} \to \mathbb{Z}^{(n)}[G]^{G_\infty} \to \mathbb{Z}^{(n)}[G]^{G_\infty} / \sum_{j\in E} \mathbb{Z}^{(n)}[G]^{G_j} \to 0. \tag{5.8.8}$$

This is a resolution of

$$M = \mathbb{Z}^{(n)}[G]^{G_\infty} / \sum_{j\in E} \mathbb{Z}^{(n)}[G]^{G_j}$$

by free $\mathbb{Z}^{(n)}$-modules and this sequence remains exact under tensoring by any $\mathbb{Z}^{(n)}$-algebra. It follows from this free resolution that $\mathrm{Tor}_1^{\mathbb{Z}^{(n)}}(M,T) = 0$ for any $\mathbb{Z}^{(n)}$-algebra T. Hence M is a finite flat $\mathbb{Z}^{(n)}$-module. As $\mathbb{Z}^{(n)}$ is a principal ideal domain it follows that M is a finite free $\mathbb{Z}^{(n)}$-module. We have

the short exact sequence of $\mathbb{Z}^{(n)}$-modules (from (5.8.7))

$$0 \to M \to J_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)} \to \mathbb{Z}^{(n)}[G]/\mathbb{Z}^{(n)}[G]^{G_\infty} \to 0. \tag{5.8.9}$$

As the two extremities of this sequence are finite free $\mathbb{Z}^{(n)}$-modules, this sequence splits and hence $J_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)}$ is a finite free $\mathbb{Z}^{(n)}$-module. Therefore $\mathcal{H}'_c$ is a finite free R-module by the isomorphism $\mathcal{H}'_c \cong (J_c \otimes_{\mathbb{Z}} \mathbb{Z}^{(n)}) \otimes_{\mathbb{Z}^{(n)}} R$ of (5.8.6).

(ii) Suppose now that c is a prime divisor. Then we have

$$J_c = \frac{\Delta_c}{me_{c,0}\Delta_c}$$

where m is the integer $\frac{|B^*|}{|A^*|}$. Put $\tilde{J}_c = \Delta_c/e_{c,0}\Delta_c$; we obtain the exact sequence of $\mathbb{Z}$-modules

$$0 \to \frac{e_{c,0}\Delta_c}{me_{c,0}\Delta_c} \to J_c \to \tilde{J}_c \to 0.$$

But $\tilde{J}_c$ is a finite free $\mathbb{Z}$-module. Therefore this exact sequence of abelian groups splits and hence we obtain an isomorphism of abelian groups

$$J_c \cong \tilde{J}_c \oplus \frac{e_{c,0}\Delta_c}{me_{c,0}\Delta_c}.$$

Now $\frac{e_{c,0}\Delta_c}{me_{c,0}\Delta_c}$ is isomorphic as a $\mathbb{Z}$-module to $(\mathbb{Z}/m\mathbb{Z})^s$ where the integer s is equal to $|\mathrm{Pic}(A)|$. Hence we obtain the isomorphism of Δ_c-modules

$$J_c = \tilde{J}_c \oplus (\mathbb{Z}/m\mathbb{Z})^s.$$

We then have the isomorphism of R-modules from (5.8.6)

$$\mathcal{H}'_c \cong R^t \oplus \left(\frac{R}{nR}\right)^s$$

as required. □

Proof of proposition 5.7.6. We write $\Delta_{c,R}$ in place of $\Delta_c \otimes_{\mathbb{Z}} R$. We have by definition that $\mathcal{H}_0 = \Delta_{0,R}$ and hence $\mathcal{H}_0$ is a finite free R-module. Suppose first that $z \in \tilde{I}$ is a prime divisor where $z \neq \infty$; then we have $\mathcal{H}_z = \Delta_{0,R} \oplus \Delta_{z,R}$ is a finite free R-module. Suppose now that z is a prime divisor of $\Sigma_F \setminus \tilde{I}$. Then we have

$$\mathcal{H}_z = \frac{\Delta_{0,R} \oplus \Delta_{z,R}}{< K_{z,0}(\Delta_{z,R}) >}$$

where

$$K_{z,0} = (a_z - \epsilon(z,z))t_{z,0}^{\Delta} - ne_{z,0}.$$

From the projection map onto the second factor

$$\Delta_0 \oplus \Delta_z \to \Delta_z$$

we obtain a surjective homomorphism of $\Delta_{z,R}$-modules

$$\mathcal{H}_z \to \frac{\Delta_{z,R}}{ne_{z,0}\Delta_{z,R}}.$$

Let $h \in \mathcal{H}_z$ be an element of the kernel of this homomorphism. Then h is represented by a pair of elements $(\delta_0, \delta_1) \in \Delta_{0,R} \oplus \Delta_{z,R}$ where $\delta_0 \in \Delta_{0,R}$ and $\delta_1 \in \Delta_{z,R}$. As h is in the kernel we have

$$\delta_1 \in ne_{z,0}\Delta_{z,R}.$$

Hence the kernel is equal to the image of $\Delta_{0,R}$ in $\mathcal{H}_z$. But the map

$$\Delta_{0,R} \to \mathcal{H}_z, \qquad \delta_0 \mapsto (\delta_0, 0)$$

is an injection; because if $\delta_0 \in K_{z,0}(\Delta_{z,R})$ then we have for some $\delta \in \Delta_{z,R}$

$$\delta_0 = (a_z - \epsilon(z,z))t_{z,0}(\delta) \text{ and } ne_{z,0}\delta = 0$$

hence we have $\delta_0 = 0$ as n is a unit. We obtain an exact sequence of R-modules

$$0 \to \Delta_{0,R} \to \mathcal{H}_z \to \frac{\Delta_{z,R}}{ne_{z,0}\Delta_{z,R}} \to 0.$$

As n is a unit in R the two extremeties of this sequence are free R-modules of finite rank. Hence $\mathcal{H}_z$ is a free R-module of finite rank. This completes the proof. □

Proof of proposition 5.7.8. (i) The case where $z = w$ is obvious so that we may suppose that $z \neq w$ are two distinct prime divisors in the support of c. We have a commutative diagram of surjective homomorphisms of finite groups

$$\begin{array}{ccccc} & & \overset{t_{c,c-z}}{\to} & & \\ & \mathrm{Pic}(O_c) & & \mathrm{Pic}(O_{c-z}) & \\ t_{c,c-w} & \downarrow & & \downarrow & t_{c-z,c-z-w} \\ & \mathrm{Pic}(O_{c-w}) & \underset{t_{c-w,c-z-w}}{\to} & \mathrm{Pic}(O_{c-z-w}) & \end{array}$$

By the computation of the kernels of the homomorphisms $t_{c,c-z}$ of (2.2.13) and (2.2.15) we may complete this diagram to a commutative diagram with exact rows and exact columns

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & 0 & \to & O^*_{c-z-w}/A^* & \to & E_{c,c-w} & \to & E_{c-z,c-z-w} & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
(5.8.10) & 0 & \to & E_{c,c-z} & \to & \mathrm{Pic}(O_c) & \to & \mathrm{Pic}(O_{c-z}) & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & 0 & \to & E_{c-w,c-z-w} & \to & \mathrm{Pic}(O_{c-w}) & \to & \mathrm{Pic}(O_{c-z-w}) & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & & 0 & &
\end{array}$$

where the groups E_{c_1,c_2} are the kernels of the homomorphisms t_{c_1,c_2}. In particular we have that the induced homomorphisms

$$E_{c,c-z} \to E_{c-w,c-z-w}, \quad E_{c,c-w} \to E_{c-z,c-z-w}$$

are surjective.

Let r be the integer given by

$$r = |O^*_{c-z-w}/A^*|.$$

We obtain

$$\begin{aligned} t^{\Delta}_{c,c-z}(e_{c,c-w}) &= \sum_{g \in E_{c,c-w}} t^{\Delta}_{c,c-z}(g) \\ &= r \sum_{h \in E_{c-z,c-z-w}} h = r e_{c-z,c-z-w}. \end{aligned}$$

This is the required formula.

(ii) We recall from (5.3.5) that

$$\epsilon(c,z) : \Delta_{c-z} \otimes_{\mathbb{Z}} R \to \Delta_{\leq c-z} \otimes_{\mathbb{Z}} R$$

is defined via the formula (where the notation $\mathfrak{m}'_z, \mathfrak{p}_1, \mathfrak{p}_2, [[\mathfrak{m}'_z]]$, etc, is that of table 4.6.9 and (5.3.5)):

$\epsilon(c,z) =$

(1) 0 — if z remains prime in K/F and is prime to $c-z$;

(2) $< [[\mathfrak{m}'_z]]^{-1}, c-z >$ — if z is ramified in K/F and is prime to $c-z$;

(3) $< [[\mathfrak{p}_1]]^{-1}, c-z > + < [[\mathfrak{p}_2]]^{-1}, c-z >$ if z is split completely in K/F and is prime to $c-z$;

(4) $t^{\Delta}_{c-z,c-2z}$ — if $z \in \mathrm{Supp}(c-z)$.

We obtain from these 4 cases that $\epsilon(c,z)$ is an element of the module $(\Delta_{c-z} \otimes_{\mathbb{Z}} R) \oplus (\Delta_{c-z} \otimes_{\mathbb{Z}} R)t^{\Delta}_{c-z,c-2z}$ of homomorphsims $\Delta_{c-z} \otimes_{\mathbb{Z}} R \to \Delta_{\leq c-z} \otimes_{\mathbb{Z}} R$ generated by the ring $\Delta_{c-z} \otimes_{\mathbb{Z}} R$ and the homomorphism $t^{\Delta}_{c-z,c-2z}$. The homomorphism t^{Δ}_{w} of $\Delta_{\leq c} \otimes_{\mathbb{Z}} R$ commutes with the ring $\Delta_{c-z} \otimes_{\mathbb{Z}} R$ but does not commute with $t^{\Delta}_{c-z,c-2z}$; in fact, for any effective divisor c' such that $z+w \leq c'$ we have the equation

$$t^{\Delta}_{w} \circ t^{\Delta}_{c',c'-z} = t^{\Delta}_{c'-w,c'-z-w} \circ t^{\Delta}_{w}.$$

Hence from the 4 cases above for $\epsilon(c,z)$ we have

$$t^{\Delta}_{w} \circ \epsilon(c,z) = \epsilon(c-w,z) \circ t^{\Delta}_{w}.$$

(iii) We briefly recall the definition of the homomorphisms $K_{c,c-z}$ (see (5.3.5) et (5.3.6) for more details). The homomorphism

$$\tilde{K}_{c,c-z} : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$$

is defined by

$$\tilde{K}_{c,c-z} = a_z t^{\Delta}_{c,c-z} - \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z} i_c$$

where $i_c : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$ is the natural injection and a_z, as in (5.7.1), is the value of ρ at z. We may extend $\tilde{K}_{c,c-z}$ by linearity (see (5.7.2)) to a homomorphism $\Delta \otimes_{\mathbb{Z}} R \to \Delta \otimes_{\mathbb{Z}} R$ by defining it to be zero on any component of $\Delta \otimes_{\mathbb{Z}} R$ different from $\Delta_c \otimes_{\mathbb{Z}} R$. For each divisor c in $\mathrm{Div}_+(A)$ and each prime divisor z in the support of c where $z \notin \tilde{I}$, the homomorphism

$$K_{c,c-z} : \Delta_c \otimes_{\mathbb{Z}} R \to \Delta_{\leq c} \otimes_{\mathbb{Z}} R$$

is defined as

$$K_{c,c-z} = \tilde{K}_{c,c-z} - \epsilon(c,z) \circ t^{\Delta}_{c,c-z}$$

where the homomorphism $\epsilon(c,z)$ is defined in (5.3.5).

Suppose that z and w are distinct prime divisors in the support of c where $z, w \notin \tilde{I}$. Then we have $c \geq z + w$ and hence

$$\frac{|O^*_{c-z}|}{|A^*|} = 1.$$

We then have

$$t^{\Delta}_w \circ \tilde{K}_{c,c-z} = t^{\Delta}_w \circ (a_z t^{\Delta}_{c,c-z} - e_{c,c-z} i_c).$$

By proposition 5.7.8(i) and the compatibility of the transition homomorphisms t^{Δ}, this gives

$$t^{\Delta}_w \circ \tilde{K}_{c,c-z} = a_z t^{\Delta}_{c-w,c-z-w} \circ t^{\Delta}_w - \frac{|O^*_{c-z-w}|}{|A^*|} e_{c-w,c-z-w} \circ t^{\Delta}_w$$

$$= \tilde{K}_{c-w,c-z-w} \circ t^{\Delta}_w. \tag{5.8.11}$$

We have by part (ii) above

$$t^{\Delta}_w \circ \epsilon(c,z) = \epsilon(c-w,z) \circ t^{\Delta}_w.$$

By the preceding equation (5.8.11) and the equation $\epsilon(c,z) \circ t^{\Delta}_{c,c-z} = \tilde{K}_{c,c-z} - K_{c,c-z}$, we then obtain

$$t^{\Delta}_w \circ K_{c,c-z} = K_{c-w,c-z-w} \circ t^{\Delta}_w$$

as required. □

5.9 Faithful flatness of the Heegner module

This section contains no proofs. The results stated here are proved in §5.10.

(5.9.1) The notation of (5.2.1) and (5.3.1) holds in this section. Principally, we let

K/F be an imaginary quadratic extension of F with respect to ∞;
B be the integral closure of A in K;
$\tilde{I}$ be a finite subset of Σ_F;
R be a commutative ring;
$\rho : \Sigma_F \setminus \tilde{I} \rightarrow R, \ v \mapsto a_v,$ be a map of sets;
$\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$ be the Heegner module of ρ, K/F, and R;
E be a finite saturated subset of $\mathrm{Div}_+(A)$.

5.9.2. Proposition. *Let n be the image in R of the integer $\frac{|B^*|}{|A^*|}$. If n is a multiplicative unit of R then the R-modules $\mathcal{H}(E)$ (see notation 5.8.2) and $\mathcal{H}(\rho)$ are faithfully flat.*

5.9.3. Proposition. *Suppose that n is a multiplicative unit of R. Let $E' \subseteq E$ be finite saturated subsets of $\mathrm{Div}_+(A)$. The transition homomorphisms*

$$\mathcal{H}(E') \to \mathcal{H}(E)$$
$$\mathcal{H}(E) \to \mathcal{H}(\rho)$$

are injections and their cokernels are faithfully flat R-modules. In particular $\mathcal{H}(E)$ is a universal submodule of $\mathcal{H}(\rho)$ and $\mathcal{H}(E')$ is a universal submodule of $\mathcal{H}(E)$ (see 5.5.21(i)).

Identifying $\mathcal{H}_c$ with its image in $\mathcal{H}(\rho)$, by means of this proposition, we obtain the next corollary:

5.9.4. Corollary. *If S is an R-algebra and n is a multiplicative unit of R then we have*

$$\mathcal{H}(\rho) \otimes_R S \;=\; \bigcup_{c \in \mathrm{Div}_+(A)} \big(\mathcal{H}_c \otimes_R S\big).$$

5.9.5. Corollary. *Suppose that S is an R-algebra and n is a multiplicative unit of R. Let $\rho_S : \Sigma_F \setminus \tilde{I} \to S$ be the composite of $\rho : \Sigma_F \setminus \tilde{I} \to R$ with the structure map $R \to S$. Then we have isomorphisms of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules*

$$\mathcal{H}(\rho) \otimes_R S \cong \mathcal{H}(\rho_S, S), \quad \mathcal{H}(\rho, E) \otimes_R S \cong \mathcal{H}(\rho_S, S, E).$$

5.9.6. Corollary. *Suppose that n is a multiplicative unit of R. Then $\Gamma(E)$ is a flat R-module (see notation 5.8.2, remarks 5.8.3).*

5.10 Proofs of the results of §5.9

5.10.1. Lemma. *Assume that the image n in R of the integer $\frac{|B^*|}{|A^*|}$ is a multiplicative unit of R. Let $c \in \mathrm{Div}_+(A)$ be a non-zero divisor. Let $z_1, \ldots, z_s \in \mathrm{Div}_+(A)$ be prime divisors in $\mathrm{Supp}(c) \setminus \tilde{I}$, where $s \geq 1$. Suppose that*

$$\sum_{i=1}^{s} e_{c,c-z_i}\delta_i = 0$$

where $\delta_i \in \Delta_c \otimes_{\mathbb{Z}} R$ for all i. Then there are elements

$$\eta^{(i,j)} \in \Delta_c \otimes_{\mathbb{Z}} R, \quad i \neq j, \quad 1 \leq i, j \leq s,$$

such that

$$\eta^{(i,j)} = -\eta^{(j,i)} \quad \text{for all } i \neq j \tag{5.10.2}$$

and

$$e_{c,c-z_i}\delta_i = \sum_{j\neq i} e_{ij}\eta^{(i,j)}, \quad \text{for all } i, \tag{5.10.3}$$

where

$$e_{ij} = \sum_{h \in \ker(t_{c,c-z_i}) + \ker(t_{c,c-z_j})} h \quad \text{for all } i \neq j.$$

Furthermore, for any elements $\eta^{(i,j)} \in \Delta_c \otimes_{\mathbb{Z}} R$, antisymmetric in i, j and satisfying the equations (5.10.3), we have

$$N\sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) \;=\; -\sum_{i=1}^{s}\sum_{1\leq j\leq s, j\neq i} (a_{z_i} - \epsilon(c, z_i))K_{c-z_i,c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)}))$$

where

$$N = \frac{|O^*_{c-z_1-z_2}|}{|A^*|}$$

and where $N = 1$ unless $s = 2$ and $c = z_1 + z_2$.

Proof. For any element δ of Δ_c we shall also write δ for its image in $\Delta_c \otimes_{\mathbb{Z}} R$, as there will be no confusion for this proof. We have by definition

$$e_{c,c-z_i} = \sum_{h \in \ker(t_{c,c-z_i})} h \quad \text{for all } i.$$

Let

$$\epsilon(c, z_i) : \Delta_{c-z_i} \otimes_{\mathbb{Z}} R \;\to\; \Delta_{\leq c-z_i} \otimes_{\mathbb{Z}} R$$

be the homomorphisms defined in (5.3.5). By the definition of the homomorphisms K (see (5.3.6)), we then have

$$K_{c,c-z_i}(\delta_i) = (a_{z_i} - \epsilon(c,z_i))t^{\Delta}_{c,c-z_i}(\delta_i) - \frac{|O^*_{c-z_i}|}{|A^*|}e_{c,c-z_i}\delta_i. \tag{5.10.4}$$

Here the element $\epsilon(c,z_i)$ is either an element of Δ_{c-z_i} or is equal to $t^{\Delta}_{c-z_i,c-2z_i}$ as in case (4) of (5.3.5); in this case (4), we may therefore take $\epsilon(c,z_i)$ to be $t^{\Delta}_{z_i}$ (see (5.7.7)).

We have the equation

$$\sum_{i=1}^{s} e_{c,c-z_i}\delta_i = 0. \tag{5.10.5}$$

We now distinguish two cases in these equations.

The special case where $s = 1$.

We have from (5.10.5)

$$e_{c,c-z_1}\delta_1 = 0$$

that is to say the element δ_1 lies in the annihilator of $e_{c,c-z_1}$. But the annihilator of $e_{c,c-z_1}$ is simply the augmentation ideal of the subgroup $\ker(t_{c,c-z_1})$ in the group algebra $\Delta_c \otimes_{\mathbb{Z}} R$ of $\mathrm{Pic}(O_c)$ (see remark 5.5.32(i)). By the definition of the homomorphisms K (see (5.10.4)), we then have

$$K_{c,c-z_1}(\delta_1) = (a_{z_1} - \epsilon(c,z_1))t^{\Delta}_{c,c-z_1}(\delta_1) - \frac{|O^*_{c-z_1}|}{|A^*|}e_{c,c-z_1}\delta_1$$

$$= 0.$$

This proves the lemma for the case where $s = 1$.

The general case where $s \geq 2$.

By proposition 5.8.4, the family of subgroups $\{\ker(t_{c,c-z_r})\}_{r=1,\ldots,s}$ of $\mathrm{Pic}(O_c)$ is R-admissible. We may then apply corollary 5.5.30 to the equation $\sum_{i=1}^{s} e_{c,c-z_i}\delta_i = 0$ of (5.10.5); we conclude that there are elements

$$\eta^{(i,j)} \in \Delta_c \otimes_{\mathbb{Z}} R, \quad i \neq j, \quad 1 \leq i,j \leq s,$$

such that

$$\eta^{(i,j)} = -\eta^{(j,i)} \quad \text{for all } i \neq j$$

and

$$e_{c,c-z_i}\delta_i = \sum_{j \neq i} e_{ij}\eta^{(i,j)} \quad \text{for all } i. \tag{5.10.6}$$

where

$$e_{ij} = \sum_{h \in \ker(t_{c,c-z_i}) + \ker(t_{c,c-z_j})} h \quad \text{for all } i \neq j.$$

From corollary 5.5.30 we further obtain

$$t^{\Delta}_{c,c-z_i}(\delta_i) = \sum_{j \neq i} e_{c-z_i,c-z_i-z_j} t^{\Delta}_{c,c-z_i}(\eta^{(i,j)}) \quad \text{for all } i. \tag{5.10.7}$$

For the map

$$t_{c,c-z_i} : \ker(t_{c,c-z_j}) \to \ker(t_{c-z_i,c-z_i-z_j})$$

is surjective (see the diagram (5.8.10)).

Summing over i we obtain from (5.10.4), as $\sum_{i=1}^{s} e_{c,c-z_i}\delta_i = 0$ by hypothesis,

$$\sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) = \sum_{i=1}^{s} (a_{z_i} - \epsilon(c, z_i)) t^{\Delta}_{c,c-z_i}(\delta_i). \tag{5.10.8}$$

Replacing $t^{\Delta}_{c,c-z_i}(\delta_i)$ here with the expression given by (5.10.7) we obtain

$$\sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) = \sum_{i=1}^{s} (a_{z_i} - \epsilon(c, z_i)) \sum_{j \neq i} e_{c-z_i,c-z_i-z_j} t^{\Delta}_{c,c-z_i}(\eta^{(i,j)}). \tag{5.10.9}$$

The expression (5.10.9) may be written in terms of lower order K's as follows. We have by (5.10.4)

$$\frac{|O^*_{c-z_i-z_j}|}{|A^*|} e_{c-z_i,c-z_i-z_j} t^{\Delta}_{c,c-z_i}(\eta^{(i,j)}) =$$

$$(a_{z_j} - \epsilon(c - z_i, z_j)) t^{\Delta}_{c-z_i,c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})) - K_{c-z_i,c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})). \tag{5.10.10}$$

Put, as in the statement of the lemma,

$$N = \frac{|O^*_{c-z_1-z_2}|}{|A^*|}. \tag{5.10.11}$$

We have that $N = 1$ unless $s = 2$ and $c = z_1 + z_2$.

We obtain from (5.10.9) and (5.10.10)

$$N \sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) =$$

$$= N \sum_{i=1}^{s} (a_{z_i} - \epsilon(c, z_i)) \sum_{j \neq i} e_{c-z_i,c-z_i-z_j} t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})$$

$$= \sum_{i=1}^{s} (a_{z_i} - \epsilon(c, z_i)) \sum_{j \neq i} \big[(a_{z_j} - \epsilon(c - z_i, z_j)) t^{\Delta}_{c-z_i, c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})) - K_{c-z_i, c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})) \big].$$

This is equal to

$$N \sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) = S_1 + S_2 \tag{5.10.12}$$

where

(5.10.13)

$$S_1 = \sum_{i=1}^{s} \sum_{j \neq i} (a_{z_i} - \epsilon(c, z_i)) \big[(a_{z_j} - \epsilon(c - z_i, z_j)) t^{\Delta}_{c-z_i, c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})) \big]$$

$$S_2 = - \sum_{i=1}^{s} \sum_{j \neq i} (a_{z_i} - \epsilon(c, z_i)) K_{c-z_i, c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})). \tag{5.10.14}$$

Now the sum S_1 here is equal to

$$S_1 = \sum_{1 \leq i,j \leq s,\ i \neq j} (a_{z_i} - \epsilon(c, z_i))(a_{z_j} - \epsilon(c - z_i, z_j)) \big[t^{\Delta}_{c,c-z_i-z_j}(\eta^{(i,j)}) \big]. \tag{5.10.15}$$

In this expression the element

$$\big[t^{\Delta}_{c,c-z_i-z_j}(\eta^{(i,j)}) \big]$$

lies in $\Delta_{c-z_i-z_j} \otimes_{\mathbb{Z}} R$; furthermore the term

$$(a_{z_i} - \epsilon(c, z_i))(a_{z_j} - \epsilon(c - z_i, z_j))$$

acts on $\Delta_{c-z_i-z_j} \otimes_{\mathbb{Z}} R$ in exactly the same way as the term

$$(a_{z_i} - \epsilon(c, z_i))(a_{z_j} - \epsilon(c, z_j))$$

in view of the definition of $\epsilon(c, z_i)$ (see the discussion after (5.10.4)). Hence we have that the expression S_1 is equal to

$$S_1 = \sum_{1 \leq i,j \leq s,\ i \neq j} (a_{z_i} - \epsilon(c, z_i))(a_{z_j} - \epsilon(c, z_j)) \big[t^{\Delta}_{c,c-z_i-z_j}(\eta^{(i,j)}) \big]. \tag{5.10.16}$$

In the term

$$(a_{z_i} - \epsilon(c, z_i))(a_{z_j} - \epsilon(c, z_j)) \big[t^{\Delta}_{c,c-z_i-z_j}(\eta^{(i,j)}) \big] \tag{5.10.17}$$

of the sum in (5.10.16), all the components are symmetric in i, j except for $\eta^{(i,j)}$ which is antisymmetric; by the linearity of this term (5.10.17) in $\eta^{(i,j)}$

it follows that the sum over all i, j such that $i \neq j$ gives zero; that is to say, we have

$$S_1 = \sum_{1 \leq i,j \leq s,\ i \neq j} (a_{z_i} - \epsilon(c, z_i))(a_{z_j} - \epsilon(c, z_j))\big[t^{\Delta}_{c,c-z_i-z_j}(\eta^{(i,j)})\big] = 0. \tag{5.10.18}$$

We therefore have by (5.10.12) and (5.10.14)

$$N \sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) = S_2$$

$$= -\sum_{i=1}^{s} \sum_{j \neq i} (a_{z_i} - \epsilon(c, z_i)) K_{c-z_i, c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})). \tag{5.10.19}$$

This proves the lemma. □

5.10.20. Lemma. *Assume that the image n in R of the integer $\frac{|B^*|}{|A^*|}$ is a multiplicative unit of R. Let E be a finite saturated subset of $\mathrm{Div}_+(A)$; let $c \neq 0$ be a maximal element of E. Let $z_1, \ldots, z_s \in \mathrm{Div}_+(A)$ be prime divisors in $\mathrm{Supp}(c) \setminus \tilde{I}$, where $s \geq 1$. Then we have an equality of submodules of $\Delta(E) \otimes_{\mathbb{Z}} R$*

$$\Gamma(E|z_1, \ldots, z_s) \ \cap \ \big(\Delta(E \setminus \{c\}) \otimes_{\mathbb{Z}} R\big) \ = \ \Gamma(E \setminus \{c\}|z_1, \ldots, z_s).$$

Proof. It is clear that there is an inclusion

$$\Gamma(E|z_1, \ldots, z_s) \ \cap \ \big(\Delta(E \setminus \{c\}) \otimes_{\mathbb{Z}} R\big) \ \supseteq \ \Gamma(E \setminus \{c\}|z_1, \ldots, z_s).$$

where the notation is that of (5.8.2)(2).

Assume that

$$\gamma \ \in \ \Gamma(E|z_1, \ldots, z_s) \ \cap \ \big(\Delta(E \setminus \{c\}) \otimes_{\mathbb{Z}} R\big).$$

The element γ of $\Gamma(E|z_1, \ldots, z_s)$ is given by an expression of the form

$$\gamma = \sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) \ + \gamma'$$

where $\gamma' \in \Gamma(E \setminus \{c\}|z_1, \ldots, z_s)$ and where $\delta_i \in \Delta_c \otimes_{\mathbb{Z}} R$ for all i. By taking the difference $\gamma - \gamma'$ we may reduce to to the case where $\gamma' = 0$. By the definition of the homomorphisms K (see (5.3.6)), we have

$$K_{c,c-z_i}(\delta_i) = (a_{z_i} - \epsilon(c, z_i)) t^{\Delta}_{c,c-z_i}(\delta_i) - \frac{|O^*_{c-z_i}|}{|A^*|} e_{c,c-z_i} \delta_i. \tag{5.10.21}$$

Here the element $\epsilon(c, z_i)$ is either an element of Δ_{c-z_i} or is equal to $t^{\Delta}_{c-z_i,c-2z_i}$ as in case (4) of (5.3.5); in this case (4), we may therefore take $\epsilon(c, z_i)$ to be $t^{\Delta}_{z_i}$ (see (5.7.7)).

The integer $|O^*_{c-z_i}|/|A^*|$ in the formula (5.10.21) is equal to 1 unless $s = 1$ and $c = z_1$ in which case it is equal to $|B^*|/|A^*|$. Hence the component of γ in $\Delta_c \otimes_{\mathbb{Z}} R$ is equal to

$$-\sum_{i=1}^{s} \frac{|O^*_{c-z_i}|}{|A^*|} e_{c,c-z_i}\delta_i \tag{5.10.22}$$

where this component is assumed to be zero, as we have $\gamma \in \Delta(E \setminus \{c\}) \otimes_{\mathbb{Z}} R$. Hence the vanishing of the component of γ in $\Delta_c \otimes_{\mathbb{Z}} R$ is equivalent to one of the equations

$$\frac{|O^*_{c-z_1}|}{|A^*|} e_{c,c-z_1}\delta_1 = 0, \quad \text{if } s = 1, \tag{5.10.23}$$

$$\sum_{i=1}^{s} e_{c,c-z_i}\delta_i = 0, \quad \text{if } s \geq 2.$$

We now distinguish the two cases in these equations.

The special case where $s = 1$.

We have from (5.10.23)

$$\frac{|O^*_{c-z_1}|}{|A^*|} e_{c,c-z_1}\delta_1 = 0$$

that is to say the element $\frac{|O^*_{c-z_1}|}{|A^*|}\delta_1$ lies in the annihilator of $e_{c,c-z_1}$. But the annihilator of $e_{c,c-z_1}$ is simply the augmentation ideal of the subgroup $\ker(t_{c,c-z_1})$ in the group algebra $\Delta_c \otimes_{\mathbb{Z}} R$ of $\mathrm{Pic}(O_c)$ (see remark 5.5.32(i)). Hence we have from (5.10.21)

$$K_{c,c-z_1}(\delta_1) = (a_{z_1} - \epsilon(c, z_1))t^{\Delta}_{c,c-z_1}(\delta_1)$$

and where $\frac{|O^*_{c-z_1}|}{|A^*|}\delta_1$ lies in the augmentation ideal of the subgroup $\ker(t_{c,c-z_1})$. Hence we have

$$K_{c,c-z_1}(\frac{|O^*_{c-z_1}|}{|A^*|}\delta_1) = 0.$$

That is to say we have

$$\frac{|O^*_{c-z_1}|}{|A^*|}\gamma = 0.$$

As $\frac{|O^*_{c-z_1}|}{|A^*|}$ is a unit of R, we have $\gamma = 0$ which proves the lemma when $s = 1$.

The general case where $s \geq 2$.

We have from (5.10.23)

$$\sum_{i=1}^{s} e_{c,c-z_i}\delta_i = 0.$$

We may then apply the previous lemma 5.10.1; we conclude from this lemma that there are elements

$$\eta^{(i,j)} \in \Delta_c \otimes_{\mathbb{Z}} R, \quad i \neq j, \quad 1 \leq i, j \leq s,$$

such that

$$\eta^{(i,j)} = -\eta^{(j,i)} \quad \text{for all } i \neq j$$

and

$$e_{c,c-z_i}\delta_i = \sum_{j\neq i} e_{ij}\eta^{(i,j)} \quad \text{for all } i. \tag{5.10.24}$$

where

$$e_{ij} = \sum_{h\in \ker(t_{c,c-z_i})+\ker(t_{c,c-z_j})} h \quad \text{for all } i \neq j.$$

Put

$$N = \frac{|O^*_{c-z_1-z_2}|}{|A^*|}. \tag{5.10.25}$$

We have that $N = 1$ unless $s = 2$ and $c = z_1 + z_2$.

We furthermore obtain from lemma 5.10.1 the equation

(5.10.26)

$$N\sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) = -\sum_{i=1}^{s}\sum_{j\neq i}(a_{z_i} - \epsilon(c, z_i))K_{c-z_i,c-z_i-z_j}(t^{\Delta}_{c,c-z_i}(\eta^{(i,j)})).$$

Note that the element $\epsilon(c, z_i)$ here is either an element of Δ_{c-z_i} or is equal to $t^{\Delta}_{z_i}$ (see (5.3.5)). By the compatibility of the homomorphisms K with the transition homomorphisms $t^{\Delta}_{z_i}$ (proposition 5.7.8(iii)) and that the K are $\Delta_c \otimes_{\mathbb{Z}} R$-linear, the expression (5.10.26) shows that

$$N\gamma = N\sum_{i=1}^{s} K_{c,c-z_i}(\delta_i) \ \in \ \Gamma(E \setminus \{c\}|z_1, \ldots, z_s).$$

where $E \setminus \{c\}$ is the saturated subset of E obtained by removing c from E. As N is a unit of R, this proves the lemma. □

5.10.27. Lemma. *Assume that the image n in R of the integer $\frac{|B^*|}{|A^*|}$ is a multiplicative unit of R. Let E, E' be saturated finite subsets of $\mathrm{Div}_+(A)$ such that $E' \subseteq E$. Then the transition homomorphism $\mathcal{H}(E') \to \mathcal{H}(E)$ is an injection.*

Proof. The notation here is that of (5.8.2). Let

$$h \in \ker(\mathcal{H}(E') \to \mathcal{H}(E)).$$

Then there is an element $\delta \in \Delta(E') \otimes_{\mathbb{Z}} R$ whose image in $\mathcal{H}(E')$ is equal to h. As h is in the kernel of the transition homomorphism $\mathcal{H}(E') \to \mathcal{H}(E)$ we have

$$\delta \in (\Delta(E') \otimes_{\mathbb{Z}} R) \cap \Gamma(E|z_1, \ldots, z_s).$$

where $z_1, \ldots, z_s$ are all the prime divisors of E which do not lie in $\tilde{I}$. In particular, we have $\delta \in \Gamma(E|z_1, \ldots, z_s)$.

Amongst saturated subsets D of E such that $\delta \in \Gamma(D|z_1, \ldots, z_s)$ there is a *minimal* such saturated subset D_0 of E, with respect to the ordering of subsets by inclusion. The subset D_0 of E therefore verifies

$$\delta \in \Gamma(D_0|z_1, \ldots, z_s) \tag{5.10.28}$$

and no proper saturated subset D_1 of D_0 satisfies $\delta \in \Gamma(D_1)$, where it is understood here and for the rest of this proof that the finite set of prime divisors for each module Γ is $z_1, \ldots, z_s$.

Suppose first that

$$D_0 \not\subset E'.$$

The finite set D_0 has maximal elements with respect to the usual partial order $\leq$ on divisors, where $d \leq d'$ if and only if $d' - d$ is an effective divisor. Therefore there is $m \in D_0$ a maximal element of D_0 satisfying

$$m \notin E'. \tag{5.10.29}$$

As $\delta \in \Delta(E') \otimes_{\mathbb{Z}} R$, the component of δ in $\Delta_m \otimes_{\mathbb{Z}} R$ is zero.

Let S_m be the finite saturated subset of D_0 given by

$$S_m = \{c \mid 0 \leq c \leq m\}.$$

We have the decomposition (see remark 5.8.3(1))

$$\Gamma(D_0) = \Gamma(S_m) + \Gamma(D_0 \setminus \{m\}).$$

We may therefore express non-uniquely δ, which lies in $\Gamma(D_0)$, as a sum corresponding to this decomposition

$$\delta = \delta_1 + \delta_2$$

where

$$\delta_1 \in \Gamma(S_m) \tag{5.10.30}$$

$$\delta_2 \in \Gamma(D_0 \setminus \{m\}).$$

The component of δ_2 in $\Delta_m \otimes_{\mathbb{Z}} R$ is zero. Hence, as the component of δ in $\Delta_m \otimes_{\mathbb{Z}} R$ is zero, we have that the component of δ_1 in $\Delta_m \otimes_{\mathbb{Z}} R$ is zero. We may now apply lemma 5.10.20 to the element δ_1 in $\Gamma(S_m) \cap \Delta(S_m \setminus \{m\}) \otimes_{\mathbb{Z}} R$. We conclude that the element δ_1 satisfies

$$\delta_1 \in \Gamma(S_m \setminus \{m\})$$

where $S_m \setminus \{m\}$ is the saturated subset of S_m obtained by omitting m. We may replace this expression in (5.10.30) and obtain

$$\delta = \delta_1 + \delta_2 \in \Gamma(S_m \setminus \{m\}) + \Gamma(D_0 \setminus \{m\}) = \Gamma(D_0 \setminus \{m\})$$

(see remark 5.8.3(1)). We put

$$D_1 = D_0 \setminus \{m\} \subset D_0$$

and we have

$$\delta \in \Gamma(D_1) \tag{5.10.31}$$

and where we have $m \notin D_1$. Hence the proper subset D_1 of D_0 is saturated and $\delta \in \Gamma(D_1)$. But this contradicts the minimality of D_0 hence the hypothesis that $D_0 \not\subset E'$ is false; hence we have $D_0 \subseteq E'$.

We then have $\delta \in \Gamma(E')$ and hence that $h = 0$. We have therefore shown that $\ker(\mathcal{H}(E') \to \mathcal{H}(E))$ is zero.□

We now come to the proofs of the results of §5.9.

Proof of propositions 5.9.2, 5.9.3, and corollary 5.9.4. We prove simultaneously these three results. That the transition homomorphisms

$$\mathcal{H}(E') \to \mathcal{H}(E)$$

are injections, if n is a multiplicative unit of R, is a proved in lemma 5.10.27.

Furthermore, we have by definition (see (5.3.8))

$$\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$$

where the limit is over all $c \in \mathrm{Div}_+(A)$. The injectivity of the maps

$$\mathcal{H}(E) \to \mathcal{H}(\rho)$$

then follows from the injectivity of the homomorphisms

$$\mathcal{H}(E') \to \mathcal{H}(E)$$

for all finite saturated subsets $E' \subset E$ of $\mathrm{Div}_+(A)$.

We have these basic results on faithful flatness of modules:

(1) If M and M' are faithfully flat R-modules and N is an R-module situated in a short exact sequence of R-modules

$$0 \to M \to N \to M' \to 0$$

then N is a faithfully flat R-module.

[This immediately follows from the definition of faithful flatness.]

(2) The module $\mathcal{H}_0$ is a finite free R-module.

[This follows from proposition 5.7.6(i).]

(3) Let E be a finite saturated subset of $\mathrm{Div}_+(A)$. Let m be a maximal element of E for the usual ordering of divisors. Then $E \setminus \{m\}$ is a saturated subset of E and the cokernel of the transition homomorphism

$$f : \mathcal{H}(E \setminus \{m\}) \to \mathcal{H}(E)$$

is a finite free R-module.

[We have that $\mathrm{coker}(f)$ is isomorphic as an R-module to $\mathcal{H}'_m$ which is the cokernel of $\mathcal{H}_m$ by the homomorphism

$$\mathcal{H}(\{d|\ 0 \leq d < m\}) \to \mathcal{H}_m$$

(see (5.7.4) and proposition 5.7.5). But by this latter proposition 5.7.5, $\mathcal{H}'_m$ is a finite free R-module, as n is a unit of R.]

The two properties (1) and (3) imply that if $E' \subset E$ are finite saturated subsets of $\mathrm{Div}_+(A)$ then the cokernel of the transition homomorphism

$$f : \mathcal{H}(E') \to \mathcal{H}(E)$$

is a faithfully flat R-module. In particular, if we take $E' = \{0\}$ we conclude that the cokernel of

$$\mathcal{H}_0 \to \mathcal{H}(E)$$

is faithfully flat over R; but by property (2) above, $\mathcal{H}_0$ is a faithfully flat R-module hence, by property (1), $\mathcal{H}(E)$ is a faithfully flat R-module.

The module $\mathcal{H}(\rho)$ is a direct limit $\varinjlim \mathcal{H}_c$ of faithfully flat R-modules where the transition homomorphisms are injections with faithfully flat cokernels; hence the Heegner module $\mathcal{H}(\rho)$ is a faithfully flat R-module.

Furthermore, the cokernel of

$$\mathcal{H}(E) \to \mathcal{H}(\rho)$$

is isomorphic to the direct limit

$$\varinjlim \operatorname{coker}\big(\mathcal{H}(E) \to \mathcal{H}(D)\big)$$

where the limit runs over all finite saturated subsets D of $\mathrm{Div}_+(A)$ with $E \subset D$. Hence the cokernel of $\mathcal{H}(E) \to \mathcal{H}(\rho)$ is a direct limit, with injective transition homomophisms whose cokernels are faithfully flat modules; hence the cokernel of $\mathcal{H}(E) \to \mathcal{H}(\rho)$ is faithfully flat over R.

We have shown that the cokernel of

$$\mathcal{H}_{c'} \to \mathcal{H}_c$$

is a faithfully flat R-module and this map is an injection; applying the functor $- \otimes_R S$, where S is an R-algebra, to this injection we obtain that it remains an injection as $\mathrm{Tor}_1^R(\mathcal{H}_c/\mathcal{H}_{c'}, S) = 0$. Hence the transition homomorphisms

$$\mathcal{H}_c \otimes_R S \to \mathcal{H}(\rho) \otimes_R S = \varinjlim \big(\mathcal{H}_c \otimes_R S\big)$$

are also injections for all $c \in \mathrm{Div}_+(A)$. Identifying $\mathcal{H}_c \otimes_R S$ with its image in $\mathcal{H}(\rho) \otimes_R S$ we obtain that $\mathcal{H}(\rho) \otimes_R S$ is the union of the submodules $\mathcal{H}_c \otimes_R S$ as required. □

Proof of corollary 5.9.5. Let $c \in \mathrm{Div}_+(A)$ be a divisor prime to $\tilde{J}$. We have the exact sequence of R-modules

$$0 \to \mathit{\Gamma}_{\leq c} \to \mathit{\Delta}_{\leq c,R} \to \mathcal{H}_c \to 0.$$

Tensoring this with $- \otimes_R S$ this sequence remains exact, as $\mathcal{H}_c$ is a flat R-module (proposition 5.9.2), so we obtain the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \to & \mathit{\Gamma}_{\leq c} \otimes_R S & \to & (\mathit{\Delta}_{\leq c} \otimes_{\mathbb{Z}} R) \otimes_R S & \to & \mathcal{H}_c \otimes_R S & \to & 0 \\
 & & \downarrow & & \downarrow\cong & & \downarrow & & \\
0 & \to & \mathit{\Gamma}_{\leq c}(S) & \to & \mathit{\Delta}_{\leq c} \otimes_{\mathbb{Z}} S & \to & \mathcal{H}_c(\rho_S, S) & \to & 0
\end{array}$$

where the second row is the standard presentation of the component Heegner module $\mathcal{H}_c(\rho_S, S)$ of $\rho_S : \Sigma_F \setminus \tilde{I} \to S$ with coefficients in S and $\mathit{\Gamma}_{\leq c}(S)$ is its corresponding submodule of relations.

By definition we have

$$\Gamma_{\leq c}(S) = \sum_{z} \sum_{\substack{c' \leq c \\ \text{where } c' \geq z}} K_{c',c'-z}(\Delta_{c'} \otimes_{\mathbb{Z}} S)$$

the sums here run over all $c' \leq c$, where $c' \in \mathrm{Div}_+(A)$, and over all prime divisors z such that $z \in \mathrm{Supp}(c) \setminus \tilde{I}$. It follows from this and the above diagram that the homomorphism $\Gamma_{\leq c} \otimes_R S \to \Gamma_{\leq c}(S)$ is an isomorphism of $\Delta_{c,S}$-modules. Hence we obtain from the above diagram isomorphisms of $\Delta_{c,S}$-modules

$$\mathcal{H}_c \otimes_R S \cong \mathcal{H}_c(\rho_S, S)$$

for all c which are compatible with the transition homomorphisms $\mathcal{H}_{c'} \to \mathcal{H}_c$ for all $c' \leq c$.

Passing to the limit over all c, we obtain an isomorphism of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\rho) \otimes_R S \cong \mathcal{H}(\rho_S, S). \quad \square$$

Proof of corollary 5.9.6. Let E be a finite saturated subset of $\mathrm{Div}_+(A)$. Let $c \in \mathrm{Div}_+(A)$ be any divisor which is an upper bound of the elements of E. Then we have the exact sequence of $\Delta_c \otimes_{\mathbb{Z}} R$-modules.

$$0 \to \Gamma(E) \to \Delta(E) \to \mathcal{H}(E) \to 0.$$

For any R-algebra S we apply the functor $- \otimes_R S$ to this sequence and we obtain the long exact sequence

$$\ldots \mathrm{Tor}_2^R(\mathcal{H}(E), S) \to \mathrm{Tor}_1^R(\Gamma(E), S) \to \mathrm{Tor}_1^R(\Delta(E), S) \to \mathrm{Tor}_1^R(\mathcal{H}(E), S)$$

$$\to \Gamma(E) \otimes_R S \to \Delta(E) \otimes_R S \to \mathcal{H}(E) \otimes_R S \to 0.$$

But $\Delta(E)$ is a finite free R-module and $\mathcal{H}(E)$ is a faithfully flat R-module (proposition 5.9.2). Hence we have

$$\mathrm{Tor}_i^R(\Delta(E), S) \cong \mathrm{Tor}_i^R(\mathcal{H}(E), S) \cong 0 \quad \text{for all } i \geq 1.$$

It follows from this long exact sequence that

$$\mathrm{Tor}_i^R(\Gamma(E), S) \cong 0 \quad \text{for all } i \geq 1.$$

Hence $\Gamma(E)$ is a flat R-module. $\square$

5.11 The Heegner module as a Heegner sheaf

(5.11.1) Let I be a non-zero ideal of A and let $\mathbf{Y}_0^{\mathrm{Drin}}(I)/A$ be the corresponding Drinfeld modular curve (§2.4). Let $\mathcal{H}$ be the Heegner sheaf (defined in (4.9.3) et seq.) of sets on $X = \mathrm{Spec}\ A$ for the flat site corresponding to $\mathbf{Y}_0^{\mathrm{Drin}}(I)/A$; thus $\mathcal{H}$ is a subsheaf of the representable sheaf $\mathbf{Y}_0^{\mathrm{Drin}}(I)$ on X_{fl}.

(5.11.2) Let $\mathbb{Z}[\mathcal{H}]$ be the presheaf on X_{fl} given by: for any morphism $U \to \mathrm{Spec}\ A$ locally of finite type

$$\Gamma(U, \mathbb{Z}[\mathcal{H}]) = \quad \text{free abelian group with basis } \Gamma(U, \mathcal{H})$$

where the transition homomorphisms are induced from those of $\mathcal{H}$. Let $\mathcal{H}^{\mathrm{ab}}$ be the sheaf of abelian groups on the flat site X_{fl} associated to this presheaf $\mathbb{Z}[\mathcal{H}]$.

(5.11.3) Let

$$i : \mathrm{Spec}\ \ F \ \ \to \ \ \mathrm{Spec}\ \ A$$

be the inclusion of the generic point. Then $i^*\mathcal{H}$ and $i^*(\mathcal{H}^{\mathrm{ab}})$ are sheaves for the flat site over F.

Let F^{sep} be the separable closure of F and let $x : \mathrm{Spec}\ F^{\mathrm{sep}} \to \mathrm{Spec}\ F$ be the natural map. Let $i^*(\mathcal{H}^{\mathrm{ab}})_x$ be the stalk of the sheaf $i^*(\mathcal{H}^{\mathrm{ab}})$ at x. Then $i^*(\mathcal{H}^{\mathrm{ab}})_x$ is a discrete module over the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$. For any intermediate field $F^{\mathrm{sep}} \supseteq L \supseteq F$, we have

$$\Gamma(\mathrm{Spec}\ L, i^*(\mathcal{H}^{\mathrm{ab}})) = \left(i^*(\mathcal{H}^{\mathrm{ab}})_x\right)^{\mathrm{Gal}(F^{\mathrm{sep}}/L)}.$$

The sheaf $i^*(\mathcal{H}^{\mathrm{ab}})$ is the sheaf associated to the discrete $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-module $i^*(\mathcal{H}^{\mathrm{ab}})_x$. That is to say, it is the sheaf associated to the free abelian group on the set of Drinfeld-Heegner points with the natural galois action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ by permuting the generators.

(5.11.4) Let K/F be an imaginary quadratic extension with respect to ∞. As in (4.9.6), let $\mathcal{H}_K$ be the subsheaf of $\mathcal{H}$ on X_{fl} given by Drinfeld-Heegner points which have CM by the field K.

Let $\mathbb{Z}[\mathcal{H}_K]$ be the presheaf on X_{fl} given by: for any morphism $U \to \mathrm{Spec}\ A$ locally of finite type

$$\Gamma(U, \mathbb{Z}[\mathcal{H}_K]) = \quad \text{free abelian group with basis } \Gamma(U, \mathcal{H}_K).$$

Let $\mathcal{H}_K^{\mathrm{ab}}$ be the sheaf of abelian groups on X_{fl} associated to this presheaf $\mathbb{Z}[\mathcal{H}_K]$.

As in (5.11.3), $i^*\mathcal{H}_K$ and $i^*(\mathcal{H}_K^{\mathrm{ab}})$ are sheaves for the flat site over F. Let $x : \mathrm{Spec}\ F^{\mathrm{sep}} \to \mathrm{Spec}\ F$ be the natural map. Let $i^*(\mathcal{H}_K^{\mathrm{ab}})_x$ be the stalk of the sheaf $i^*(\mathcal{H}_K^{\mathrm{ab}})$ at x. Then $i^*(\mathcal{H}_K^{\mathrm{ab}})_x$ is a discrete module over the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$. For any intermediate field $F^{\mathrm{sep}} \supseteq L \supseteq F$, we have

$$\Gamma(\mathrm{Spec}\ L, i^*(\mathcal{H}_K^{\mathrm{ab}})) = \left(i^*(\mathcal{H}_K^{\mathrm{ab}})_x\right)^{\mathrm{Gal}(F^{\mathrm{sep}}/L)}.$$

The sheaf $i^*(\mathcal{H}_K^{\mathrm{ab}})$ is the sheaf associated to the discrete $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-module $i^*(\mathcal{H}_K^{\mathrm{ab}})_x$. That is to say, it is the sheaf associated to the free abelian group on the set of Drinfeld-Heegner points with CM by K and with the natural galois action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ by permuting the generators.

(5.11.5) Let

R be a commutative ring;
$\rho : \Sigma_F \setminus \tilde{I} \to R$ be a map of sets (as in (5.9.1));
$\mathcal{H}(\rho)^{(0)}$ be the component above 0 of the Heegner module $\mathcal{H}(\rho)$ of ρ, K/F, and with coefficients in R (see (5.3.8)).

As $\mathcal{H}(\rho)^{(0)}$ is a discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module, it may be considered as a sheaf of abelian groups on Spec K for the étale site. Let

$$j : \mathrm{Spec}\ K \to \mathrm{Spec}\ A$$

be the structure morphism.

Then the Heegner module $\mathcal{H}(\rho)^{(0)}$, as a sheaf, is equipped with a surjective homomorphism of sheaves for the étale site on Spec K

$$j^*\mathcal{H}_K^{\mathrm{ab}} \otimes_{\mathbb{Z}} R \to \mathcal{H}(\rho)^{(0)}.$$

The kernel of this homomorphism consists precisely of the relations $\Gamma_{\leq c}$ for all c (see (5.3.7)).

6

Cohomology of the Heegner module

Let $\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$ be the Heegner module of the map $\rho : \Sigma_F \setminus \tilde{I} \to R$, the imaginary quadratic extension field K/F, and with coefficients in the ring R, where the notation is that of §5.3.

The objective of this technical chapter is to calculate the cohomology of the Heegner module $\mathcal{H}(\rho)$ as a $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module. More precisely, for a divisor c in $\mathrm{Div}_+(A)$ and a prime divisor $z \notin \tilde{I}$ in the support of c, let $K[c]/K[c-z]$ denote the corresponding extension of ring class fields of K. For a commutative R-algebra S, the aim is to compute the Galois cohomology groups

$$H^i(\mathrm{Gal}(K[c]/K[c-z]), \mathcal{H}_c \otimes_R S)$$

of the component Heegner module $\mathcal{H}_c \otimes_R S$. The main general result we obtain (proposition 6.6.3) expresses this cohomology group as a homomorphic image of a simpler module. The most precise results we obtain are for the case where $i = 0$ and where S is an *infinitesimal trait* (definition 6.7.5) with a supplementary hypothesis relative to the residue field characteristic of S (theorem 6.10.7); this is the case applied to the Tate conjecture in chapter 7.

Theorem 6.10.7 is the principal result of this chapter; only the case (1) of this theorem, where the prime z is inert and unramified in the field extension K/F, is applied to the Tate conjecture in the next chapter. Nevertheless, the other cases of this theorem, could be used to obtain further information on Tate-Shafarevich groups by the methods of the next Chapter 7.

Proposition 6.6.3 is a simple consequence of the main lemma 6.4.3. This main lemma states that the galois cohomology of the module of relations of the Heegner module may be computed by restriction to a submodule on which the galois group in question acts trivially. The proof of the main lemma, as well as that of the main theorem 6.10.7, uses extensively the results of §5.6 on cohomology of group rings.

M.L. Brown: LNM 1849, pp. 223–327, 2004.

6.1 General notation

(6.1.1) For this chapter, we retain the notation of (5.2.1), (5.3.1), and (5.7.1). Principally, we have

K/F is an imaginary quadratic extension of F with respect to ∞;
B is the integral closure of A in K;
Σ_F is the set of all places of F;
$\tilde{I}$ is a finite subset of Σ_F;
R is a commutative ring;
S is an R-algebra;
$\rho : \Sigma_F \setminus \tilde{I} \quad \to \quad R, \quad v \mapsto a_v,$ is a map of sets;
$\mathcal{H}(\rho) = \varinjlim_{c \in \mathrm{Div}_+(A)} \mathcal{H}_c$ is the Heegner module of ρ, K/F, with coefficients in R.

(6.1.2) For divisors $c \geq c'$ of $\mathrm{Div}_+(A)$, we write $G(c/c')$ for the galois group $\mathrm{Gal}(K[c]/K[c'])$ of the ring class field extension $K[c]/K[c']$.

We recall that the Heegner module $\mathcal{H}(\rho)$ is a discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module and that the component Heegner module $\mathcal{H}_c$ is a $\mathrm{Gal}(K[c]/K)$-module for all $c \in \mathrm{Div}_+(A)$.

(6.1.3) For any galois field extension K'/K with galois group G and any G-module M, we write

$$H^i(G, M)$$

for the usual galois cohomology groups; in particular $H^0(G, M) = M^G$ is the G-invariant submodule of M.

(6.1.4) If M is an R-module we frequently write M_S for the S-module $M \otimes_R S$. We write $\Delta_{c,R}$ and $\Delta_{c,S}$ for $\Delta_c \otimes_{\mathbb{Z}} R$ and $\Delta_c \otimes_{\mathbb{Z}} S$, respectively.

We put for any $c \in \mathrm{Div}_+(A)$ and any prime divisor z in $\mathrm{Supp}(c) \setminus \tilde{I}$

$$\Gamma_{c,c-z} = K_{c,c-z}(\Delta_{c,R}).$$

6.2 Exact sequences and preliminary lemmas

In this section, we give some results which are a simple consequence of the presentation of the Heegner module by generators and relations. The main exact sequences of cohomology which are obtained are those of lemmas 6.2.11 and 6.2.15.

(6.2.1) We assume throughout this section that

n is the image in R of the integer $|B^*|/|A^*|$ and is assumed to be a multiplicative unit of R;
$c' \leq c$ are effective divisors on Spec A;
z is a prime divisor in the support of c where $z \notin \tilde{I}$.

6.2.2. Lemma. (i) *The restriction to $\Gamma_{c,c-z}$ of the projection homomorphism $\Delta_{\leq c,R} \to \Delta_{c,R}$ induces isomorphism of $\Delta_{c,R}$-modules*

$$\Gamma_{c,c-z} \cong \Delta_{c-z,R}.$$

(ii) *The module $\Gamma_{c,c-z}$ is a universal R-submodule of $\Delta_{\leq c,R}$.*

Proof. (i) We have that $\Gamma_{c,c-z}$ is a submodule of $\Gamma_{\leq c,R}$ and the projection map $\Delta_{\leq c} \to \Delta_c$, with kernel $\Delta_{<c}$, induces a surjective homomorphism of $\Delta_{c,R}$-modules

$$\pi : \Gamma_{c,c-z} \to \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z}\Delta_{c,R}. \tag{6.2.3}$$

Let $\gamma = K_{c,c-z}(\delta)$ be an element of the kernel of this homomorphism π. We then have (see (5.3.6))

$$K_{c,c-z}(\delta) = (a_z - \epsilon(c,z))t^{\Delta}_{c,c-z}(\delta) - \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z}\delta.$$

As $\pi(\gamma) = 0$, we have that $e_{c,c-z}\delta = 0$ as n is a multiplicative unit in R; hence we obtain $t_{c,c-z}(\delta) = 0$. Therefore we have $\gamma = 0$ and π is an injection; therefore π is an isomorphism. We then obtain the isomorphisms of $\Delta_{c,R}$-modules

$$\Gamma_{c,c-z} \cong e_{c,c-z}\Delta_{c,R} \cong \Delta_{c-z,R}$$

as required.
(ii) The isomorphism π of the proof of part (i) may be inserted into a commutative diagram with exact rows and with injective vertical homomorphisms provided by inclusion

$$\begin{array}{ccccccccc} & & 0 & \to & \Gamma_{c,c-z} & \overset{\pi}{\to} & \frac{|O^*_{c-z}|}{|A^*|} e_{c,c-z}\Delta_{c,R} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \Delta_{<c,R} & \to & \Delta_{\leq c,R} & \to & \Delta_{c,R} & \to & 0 \end{array} \tag{6.2.4}$$

If we put

$$N = \operatorname{coker}(\Gamma_{c,c-z} \to \Delta_{\leq c,R})$$

then the snake lemma applied to this diagram provides the exact sequence of cokernels

$$0 \to \Delta_{<c,R} \to N \to \Delta_{c,R}/e_{c,c-z}\Delta_{c,R} \to 0$$

as $\frac{|O^*_{c-z}|}{|A^*|}$ is a unit of R.

As $\Delta_{c,R}/e_{c,c-z}\Delta_{c,R}$ and $\Delta_{<c,R}$ are finite free R-modules it follows that this short exact sequence is split and N is a finite free R-module. Therefore we have an isomorphism of R-modules

$$\Delta_{\leq c,R} \cong \Gamma_{c,c-z} \oplus N$$

and hence $\Gamma_{c,c-z}$ is a universal R-submodule of $\Delta_{\leq c,R}$, as required.□

For the next lemma, we use the notation of 5.8.2 and remarks 5.8.3.

6.2.5. Lemma. *Let E be a finite saturated subset of* $\mathrm{Div}_+(A)$. *The module $\Gamma(E)$ is a universal R-submodule of $\Delta(E)_R$.*

Proof of lemma. The group $\mathcal{H}(E)$ lies in the exact sequence of $\Delta_{c,R}$-modules, for any $c \in \mathrm{Div}_+(A)$ larger than all elements of E,

$$0 \to \Gamma(E) \to \Delta(E)_R \to \mathcal{H}(E) \to 0. \tag{6.2.6}$$

As $\mathcal{H}(E)$ is a finite flat R-module (proposition 5.9.2) it follows that $\Gamma(E)$ is a universal R-submodule of $\Delta(E)_R$ (by remark 5.5.22(i)). □

6.2.7. Lemma. (i) *If $c' < c$ and $d \leq c$, where $c', d \in \mathrm{Div}_+(A)$ and $z \notin \tilde{I}$ is a prime divisor in* $\mathrm{Supp}(c - c')$ *then we have the equality of $G(c/c')$-invariant submodules of $\Delta_{\leq d,S}$ provided that $d \not\leq c - z$*

$$\left(\Delta_{d,S} \oplus \Delta_{\leq d-z,S}\right)^{G(c/c')} = (\Gamma_{d,d-z,S})^{G(c/c')} + (\Delta_{\leq d-z,S})^{G(c/c')}. \tag{6.2.8}$$

(ii) *For divisors $d \leq c$ of* $\mathrm{Div}_+(A)$ *and prime divisors $z, w \notin \tilde{I}$ we have isomorphisms of $\Delta_{c,S}$-modules*

$$(\Gamma_{d,d-w,S})^{G(c/c-z)} \cong \begin{cases} \Delta_{d-z,S} & \text{if } d \leq c - z \text{ or } w = z; \\ \Delta_{d-w-z,S}, & \text{otherwise.} \end{cases}$$

Proof of lemma. (i) The group $G(c/c - z)$ is a subgroup of the abelian group $G(c/c')$ and the quotient group is isomorphic to the galois group $G(c - z/c')$; that is to say we have the short exact sequence of abelian galois groups

$$0 \to G(c/c - z) \to G(c/c') \to G(c - z/c') \to 0.$$

We have

$$(\Delta_{d,S})^{G(c/c')} = (e_{d,d-z}\Delta_{d,S})^{G(c-z/c')} \text{ if } d \not\leq c-z. \tag{6.2.9}$$

To prove this, from the commutative diagram with exact rows and columns (5.8.10), for all $d \leq c$ such that $d \not\leq c-z$ we have that $G(d/d-z)$ is a homomorphic image of $G(c/c-z)$. Hence if $d \leq c$ and $d \not\leq c-z$ then we have

$$(\Delta_{d,S})^{G(c/c-z)} = (\Delta_{d,S})^{G(d/d-z)}.$$

As there is an isomorphism of $\mathrm{Gal}(K[c]/K)$-modules

$$\Delta_{d,S} \cong S[\mathrm{Gal}(K[d]/K)]$$

where the group algebra $S[\mathrm{Gal}(K[d]/K)]$ is a cohomologically trivial $\mathrm{Gal}(K[d]/K)$-module, it follows that we have an equality of submodules of $\Delta_{c,S}$

$$(\Delta_{d,S})^{G(d/d-z)} = e_{d,d-z}\Delta_{c,S} \text{ if } d \not\leq c-z.$$

Hence we obtain

$$(\Delta_{d,S})^{G(c/c-z)} = e_{d,d-z}\Delta_{d,S} \text{ if } d \not\leq c-z.$$

This proves (6.2.9).

If $d \not\leq c-z$ then $\Delta_{\leq d-z,S}$ is invariant under $G(c/c-z)$. From this, (6.2.9), and the definition of the homomorphism $K_{d,d-z}$ (see (5.3.6))

$$K_{d,d-z}(\delta) = (a_z - \epsilon(d,z))t^{\Delta}_{d,d-z}(\delta) - \frac{|O^*_{d-z}|}{|A^*|}e_{d,d-z}\delta$$

we obtain the inclusion

$$\frac{|O^*_{d-z}|}{|A^*|}(\Delta_{d,S})^{G(c/c')} \subseteq (\Gamma_{d,d-z,S})^{G(c/c')} + (\Delta_{\leq d-z,S})^{G(c/c')}, \text{ if } d \not\leq c-z,$$

where the inclusion and sum here are as submodules of $\Delta_{\leq c,S}$. As the image of $|B^*|/|A^*|$ in S is a unit we obtain the equality (6.2.8) stated in the lemma. (ii) This follows immediately from (6.2.9) and the isomorphism of $\Delta_{c,S}$-modules (lemma 6.2.2(i))

$$\Gamma_{d,d-z,S} \cong \Delta_{d-z,S}. \qquad \square$$

6.2.10. Notation. For a subset E of $\mathrm{Div}_+(A)$ and an element c of $\mathrm{Div}_+(A)$ we write $E_{\leq c}$ for the subset of E given by

$$E_{\leq c} = \{e \in E |\ e \leq c\}.$$

6.2.11. Lemma. *Let $c' \leq c$ be effective divisors in $\mathrm{Div}_+(A)$. Assume that $\mathrm{Supp}(c-c')$ is disjoint from $\tilde{I}$. Let E be a finite saturated subset of $\mathrm{Div}_+(A)$ all of whose elements are $\leq c$. There is a long exact sequence*

$$0 \to \mathcal{H}(E_{\leq c'})_S \to (\mathcal{H}(E)_S)^{G(c/c')} \to$$

$$H^1(G(c/c'), \Gamma(E)_S) \to H^1(G(c/c'), \Delta(E)_S) \to H^1(G(c/c'), \mathcal{H}(E)_S) \to$$
$$H^2(G(c/c'), \Gamma(E)_S) \to H^2(G(c/c'), \Delta(E)_S) \to H^2(G(c/c'), \mathcal{H}(E)_S) \to \dots$$

Proof. If $c = c'$ there is nothing to prove so we may assume that $c' < c$.

Let z be a prime divisor in $\mathrm{Supp}(c-c')$. Then $z \notin \tilde{I}$ as $\mathrm{Supp}(c-c')$ is disjoint from $\tilde{I}$. From lemma 6.2.7, we have for all divisors d in $\mathrm{Div}_+(A)$ such that $0 \leq d \leq c$ and $d \not\leq c - z$

$$\left(\Delta_{d,S} \oplus \Delta_{d-z,S}\right)^{G(c/c')} = (\Gamma_{d,d-z,S})^{G(c/c')} + (\Delta_{d-z,S})^{G(c/c')}.$$

By taking the sum over all divisors d of E, we obtain the equality of submodules of $\Delta(E)_S$

$$(\Delta(E)_S)^{G(c/c')} = \sum_{d \in E,\ d \not\leq c-z} (\Gamma_{d,d-z,S})^{G(c/c')} \quad + \quad (\Delta(E_{\leq c-z})_S)^{G(c/c')}.$$

This equality shows that the image of $(\Delta(E)_S)^{G(c/c')}$ in $\mathcal{H}(E)_S$ coincides with the image of $(\Delta(E_{\leq c-z})_S)^{G(c/c')}$ in $\mathcal{H}(E)_S$; but $(\Delta(E_{\leq c-z})_S)^{G(c/c')} = (\Delta(E_{\leq c-z})_S)^{G(c-z/c')}$ as $\Delta(E_{\leq c-z})_S$ is $G(c/c-z)$-invariant. Hence the image of $(\Delta(E)_S)^{G(c/c')}$ in $\mathcal{H}(E)_S$ coincides with the image of $\Delta(E_{\leq c'})_S$ in $\mathcal{H}(E)_S$, by induction on $c-c'$. That is to say the image of $(\Delta(E)_S)^{G(c/c')}$ in $\mathcal{H}(E)_S$ coincides with the image of the transition homomorphism $\mathcal{H}(E_{\leq c'})_S \to \mathcal{H}(E)_S$. But (proposition 5.9.3), this last transition homomorphism is an injection. From the short exact sequence (6.2.6) we obtain the short universally exact sequence which is the standard presentation of the component Heegner module $\mathcal{H}(E)_S$

$$0 \to \Gamma(E)_S \to \Delta(E)_S \to \mathcal{H}(E)_S \to 0.$$

This provides the following long exact sequence of galois cohomology

$$0 \to (\Gamma(E)_S)^{G(c/c')} \to (\Delta(E)_S)^{G(c/c')} \to (\mathcal{H}(E)_S)^{G(c/c')} \to \dots \tag{6.2.12}$$

$$\to H^i(G(c/c'), \Gamma(E)_S) \to H^i(G(c/c'), \Delta(E)_S) \to H^i(G(c/c'), \mathcal{H}(E)_S) \to \dots$$

This exact sequence and the preceding argument provides an isomorphism

$$(\Delta(E)_S)^{G(c/c')}/(\Gamma(E)_S)^{G(c/c')} \cong \mathcal{H}(E_{\leq c'})_S.$$

Hence the long exact sequence of (6.2.12) becomes

$$0 \to \mathcal{H}(E_{\leq c'})_S \to (\mathcal{H}(E)_S)^{G(c/c')} \to$$

$$H^1(G(c/c'), \Gamma(E)_S) \to H^1(G(c/c'), \Delta(E)_S) \to H^1(G(c/c'), \mathcal{H}(E)_S) \to \dots$$

as required.□

6.2.13. Notation. The partially ordered set $\mathrm{Div}_+(A)$, with its usual order, is a *sieve* (definition 5.6.2). For two effective divisors d_1, d_2 in $\mathrm{Div}_+(A)$, we write $d_1 \cap d_2$ for the greatest divisor in $\mathrm{Div}_+(A)$ which is $\leq d_1$ and $\leq d_2$; we write $d_1 \cup d_2$ for the least divisor in $\mathrm{Div}_+(A)$ which is $\geq d_1$ and $\geq d_2$. The divisors $d_1 \cap d_2$ and $d_1 \cup d_2$ are uniquely determined by d_1 and d_2.

6.2.14. Lemma. *Let $c' \leq c$ be divisors in $\mathrm{Div}_+(A)$.*
(i) *Let $d \leq c$ where $d \in \mathrm{Div}_+(A)$. Then we have isomorphisms of $\Delta_{c,S}$-modules*

$$H^i(G(c/c'), \Delta_{d,S}) \;\cong\; \Delta_{d\cap c'} \otimes_{\mathbb{Z}} H^i(G(c/d \cup c'), S) \quad \textit{for all } i \geq 0.$$

(ii) *Let E be a finite saturated subset of $\mathrm{Div}_+(A)$ all of whose elements are $\leq c$. There are isomorphisms of $\mathrm{Div}_+(A)$-graded $\Delta_{c,S}$-modules*

$$H^i(G(c/c'), \Delta(E)_S) \cong \bigoplus_{d\in E} \left\{ \Delta_{d\cap c'} \otimes_{\mathbb{Z}} H^i(G(c/d \cup c'), S) \right\} \quad \textit{for } i \geq 0.$$

Proof. Part (ii) follows immediately from part (i) by taking the direct sum over all divisors d of E.

In order to prove part (i), we have the exact sequence of abelian groups obtained from the inclusion of ring class fields $K[c'] \subseteq K[d \cup c'] \subseteq K[c]$

$$0 \to G(c/d \cup c') \to G(c/c') \to G(d \cup c'/c') \to 0.$$

The Hochshild-Serre spectral sequence for the subgroup $G(c/d\cup c')$ of $G(c/c')$ then can be written

$$E_2^{i,j} = H^i(G(d \cup c'/c'), H^j(G(c/d \cup c'), \Delta_{d,S})) \Rightarrow H^{i+j}(G(c/c'), \Delta_{d,S}).$$

The group $G(c/d \cup c')$ acts trivially on the finite free S-module $\Delta_{d,S}$; hence we have isomorphisms

$$H^j(G(c/d \cup c'), \Delta_{d,S}) \cong H^j(G(c/d \cup c'), S) \otimes_{\mathbb{Z}} \Delta_d, \quad \text{for all } i \geq 0.$$

We then obtain the isomorphisms of $\Delta_{c,S}$-modules

$$E_2^{i,j} \cong H^i\Big(G(d\cup c'/c'), H^j(G(c/d\cup c'), S)\otimes_S \Delta_{d,S}\Big) \cong$$

$$H^i\big(G(d\cup c'/c'), \Delta_{d,S}\big)\otimes_S H^j\big(G(c/d\cup c'), S\big).$$

We have a commutative diagram of Picard groups obtained from the evident inclusions of orders

$$\begin{array}{ccc} \mathrm{Pic}(O_{d\cup c'}) & \to & \mathrm{Pic}(O_{c'}) \\ \downarrow & & \downarrow \\ \mathrm{Pic}(O_d) & \to & \mathrm{Pic}(O_{d\cap c'}) \end{array}$$

We obtain a surjective group homomorphism $G(d\cup c'/c') \to G(d/c'\cap d)$ whose kernel has order which is a unit in R (by the formulae (2.3.8), (2.3.10); see also the diagram (5.8.10)). Furthermore the above diagram shows that the action of $G(d\cup c'/c')$ on $\Delta_{d,S}$ factors through the natural action of $G(d/d\cap c')$ on $\Delta_{d,S}$. For all d such that $d\le c$, the $G(d/d\cap c')$-module $\Delta_{d,S}$ is cohomologically trivial; hence the $G(d\cup c'/c')$-module $\Delta_{d,S}$ is cohomologically trivial. Hence we have $E_2^{i,j}=0$ for all $i\ge 1$. Hence this spectral sequence degenerates and we obtain the isomorphisms

$$(\Delta_{d,S})^{G(d/d\cap c')}\otimes_S H^j(G(c/d\cup c'),S) \;\cong\; H^j(G(c/c'),\Delta_{d,S}) \;\text{ for all } j\ge 0.$$

The result then follows, as we have isomorphisms of $\Delta_{c,S}$-modules

$$(\Delta_{d,S})^{G(d/d\cap c')} \cong \Delta_{d\cap c',S}. \qquad \square$$

6.2.15. Lemma. *If z is a prime divisor in* $\mathrm{Supp}(c)\setminus \tilde{I}$, *there are short exact sequences for all $m\ge 0$*

$$H^m(G(c/c-z),\mathcal{H}_{c-z,S}) \to H^m(G(c/c-z),\mathcal{H}_{c,S}) \to$$

$$H^{m+1}(G(c/c-z),\Gamma_{\le c,S}) \to H^{m+1}(G(c/c-z),\Delta_{\le c,S}).$$

Proof. The exact sequence of lemma 6.2.11 applied to $\mathcal{H}_{c,S}$ and with $c'=c-z$ becomes

$$0\to \mathcal{H}_{c-z,S}\to (\mathcal{H}_{c,S})^{G(c/c-z)} \to \tag{6.2.16}$$

$$H^1(G(c/c-z),\Gamma_{\le c,S})\to H^1(G(c/c-z),\Delta_{\le c,S})\to H^1(G(c/c-z),\mathcal{H}_{c,S})\to$$

$$H^2(G(c/c-z),\Gamma_{\le c,S})\to H^2(G(c/c-z),\Delta_{\le c,S})\to H^2(G(c/c-z),\mathcal{H}_{c,S})\to\dots$$

For the case when $m=0$, the short exact sequence of the lemma results immediately from this long exact sequence.

For $m \geq 1$, from lemma 6.2.14(ii) we obtain the isomorphisms of graded modules
(6.2.17)

$$H^m(G(c/c-z), \Delta_{\leq c,S}) \cong \bigoplus_{0\leq d\leq c} \left\{ \Delta_{d\cap(c-z)} \otimes_{\mathbb{Z}} H^m(G(c/d \cup (c-z)), S) \right\}$$

$$\cong \bigoplus_{0\leq d\leq c-z} \left\{ \Delta_d \otimes_{\mathbb{Z}} H^m(G(c/c-z), S) \right\} \cong H^m(G(c/c-z), \Delta_{\leq c-z,S}).$$

The modules $\Gamma_{\leq c-z,S}, \Delta_{\leq c-z,S}, \mathcal{H}_{c-z,S}$ are finite flat S-modules (propositions 5.9.2, 5.9.6) on which the group $G(c/c-z)$ acts trivially. The short universally exact sequence (see (6.2.6)) for any finite saturated subset E of $\mathrm{Div}_+(A)$

$$0 \to \Gamma(E) \to \Delta(E)_R \to \mathcal{H}(E) \to 0$$

then provides the commutative diagram of cohomology with exact rows, where we write G for $G(c/c-z)$ and H^m for $H^m(G,S)$

$$\begin{array}{ccccccc}
\ldots \to H^m(G,\Gamma_{\leq c,S}) & \to H^m(G,\Delta_{\leq c,S}) & \to H^m(G,\mathcal{H}_{c,S}) & \to H^{m+1}(G,\Gamma_{\leq c,S}) \to \ldots \\
\uparrow & \uparrow\cong & \uparrow & \\
0 \to H^m \otimes_S \Gamma_{\leq c-z,S} & \to H^m \otimes_S \Delta_{\leq c-z,S} & \to H^m \otimes_S \mathcal{H}_{c-z,S} \to 0 &
\end{array}$$

where the middle vertical isomorphism results from the isomorphisms of (6.2.17). Hence for $m \geq 1$, the image of the homomorphism

$$H^m(G(c/c-z), \Delta_{\leq c,S}) \to H^m(G(c/c-z), \mathcal{H}_{c,S})$$

coincides with the image of the homomorphism, induced from the inclusion $\mathcal{H}_{c-z,S} \to \mathcal{H}_{c,S}$,

$$H^m(G(c/c-z), \mathcal{H}_{c-z,S}) \to H^m(G(c/c-z), \mathcal{H}_{c,S}).$$

The result then follows for $m \geq 1$ from the exact sequence (6.2.16). □

6.3 Cohomology of the Heegner module: vanishing cohomology

(6.3.1) We retain the notation of (6.1.1); assume that

n is the image in R of the integer $|B^*|/|A^*|$ and is
a multiplicative unit of R;
S is an R-algebra;
$c' \leq c$ are effective divisors on Spec A;
E is a saturated subset of $\mathrm{Div}_+(A)$ all of whose elements are $\leq c$;
$E_{\leq c'} = \{e \in E \mid e \leq c'\}$.

6.3.2. Proposition. *If the image in S of the order of the group $G(c/c')$ is a multiplicative unit and* $\mathrm{Supp}(c-c')$ *is prime to $\tilde{I}$ then there are isomorphisms of $\Delta_{c,S}$-modules*

$$H^i(G(c/c'), \mathcal{H}(E)_S) \cong \begin{cases} \mathcal{H}(E_{\leq c'})_S, & \text{if } i = 0; \\ 0, & \text{if } i \geq 1. \end{cases}$$

Proof. For any $G(c/c')$-module M the cohomology groups $H^i(G(c/c'), M)$ are annihilated by $|G(c/c')|$ for all $i \geq 1$ [CF, Chapter IV, §6, Cor.1]. As the image in S of the integer $|G(c/c')|$ is a unit, we have

$$H^i(G(c/c'), \mathcal{H}(E)_S) \cong 0 \quad \text{for all } i \geq 1.$$

For the same reason, we have $H^i(G(c/c'), \Gamma(E)_S) \cong 0$ for all $i \geq 1$; hence the long exact sequence of lemma 6.2.11 then provides the isomorphism

$$(\mathcal{H}(E)_S)^{G(c/c')} \cong \mathcal{H}(E_{\leq c'})_S$$

as required.□

6.4 The main lemma

The main lemma 6.4.3 is the basis of all further results given in this chapter on the cohomology of the Heegner module. The lemma expresses that the cohomology $H^m(G(c/c-z), \Gamma(E)_S)$ of the module of relations $\Gamma(E)_S$ of the Heegner module may be obtained by restriction to a submodule on which the group $G(c/c-z)$ acts trivially.

(6.4.1) Let

z be a prime divisor in $\mathrm{Div}_+(A)$ where $z \notin \tilde{I}$;
c be an effective divisor in $\mathrm{Div}_+(A)$ such that $z \in \mathrm{Supp}(c) \setminus \tilde{I}$;
E be a finite saturated subset of $\mathrm{Div}_+(A)$ such that c is an upper bound for E;
S be an R-algebra.

6.4.2. Notation. (1) Write

$$\mathrm{Max}(E, c, z) = \{d \in E \mid d \not\leq c - z\}.$$

A divisor $d \in E$ is called *z-maximal* if $d + z \notin E$. The set $\mathrm{Max}(E, c, z)$ is a subset of the set of z-maximal elements of E, but need *not* contain all the z-maximal elements; for example if $c - z$ is an upper bound for all elements of E then $\mathrm{Max}(E, c, z) = \emptyset$.

(2) Write $\Gamma_{c,z}(E)_S$ for the submodule of $\Gamma(E)_S$ given by

$$\Gamma_{c,z}(E)_S = \sum_{d \in \mathrm{Max}(E,c,z)} \Gamma_{d,d-z,S} \ + \ \Gamma(E \setminus \mathrm{Max}(E, c, z))_S$$

where $\Gamma(E \setminus \mathrm{Max}(E, c, z))_S$, as in notation 5.8.2, is given by

$$\Gamma(E \setminus \mathrm{Max}(E, c, z))_S = \sum_{d \in E \setminus \mathrm{Max}(E,c,z)} \ \sum_{w \in \mathrm{Supp}(d) \setminus \tilde{I}} \Gamma_{d,d-w,S}.$$

The submodule $\Gamma_{c,z}(E)_S$ is $G(c/c - z)$-invariant. For example, if E is the set of divisors d with $0 \leq d \leq c$ then

$$\Gamma_{c,z}(E)_S = \sum_{d \leq c, d \not\leq c-z} \Gamma_{d,d-z,S} \ + \ \Gamma_{\leq c-z,S}.$$

6.4.3. Main Lemma. *Assume that the image in R of the integer $|B^*|/|A^*|$ is a unit. The homomorphism induced from the inclusion $\Gamma_{c,z}(E) \subseteq \Gamma(E)$*

$$H^m(G(c/c - z), \Gamma_{c,z}(E)_S) \ \to \ H^m(G(c/c - z), \Gamma(E)_S)$$

is surjective for all $m \geq 1$.

[For the proof of lemma 6.4.3 see the next section §6.5.]

6.4.4. Remark. The surjective homomorphism of the main lemma 6.4.3 is not usually an isomorphism (see §6.9.8 and particularly proposition 6.8.10).

6.5 Proof of lemma 6.4.3.

(6.5.1) Let

z be a prime divisor in $\mathrm{Div}_+(A)$ where $z \notin \tilde{I}$;
c be an effective divisor in $\mathrm{Div}_+(A)$ such that $z \in \mathrm{Supp}(c) \setminus \tilde{I}$;
E be a finite saturated subset of $\mathrm{Div}_+(A)$ such that c is an upper bound of E;
G be the group $G(c/c-z)$.

6.5.2. Notation. The following notation is only required for this section.

(1) A finite subset T of $\mathrm{Div}_+(A)$ is *z-saturated* if for all divisors $d \in T$ then $d - nz \in T$ for all integers $n \geq 0$ such that $d - nz \geq 0$.

Note that:

(a) The intersection and the union of a finite family of z-saturated subsets of $\mathrm{Div}_+(A)$ are z-saturated.

(b) A finite subset T of $\mathrm{Div}_+(A)$ is saturated (see (5.9.1)) if and only if it is z-saturated for all prime divisors z.

(c) The empty set is assumed to be z-saturated for all prime divisors z.

(2) If T is a finite subset of $\mathrm{Div}_+(A)$ then the *z-saturation* $\mathrm{Sat}_z(T)$ of T is the smallest z-saturated subset of $\mathrm{Div}_+(A)$ containing T.

(3) Let T' be a finite subset of $\mathrm{Div}_+(A)$. Let T be a finite saturated subset of $\mathrm{Div}_+(A)$. Assume that all elements of $T \cup T'$ are $\leq c$. Then

$$\Gamma_{c,z}(T'||T)$$

is defined to be the subgroup of $\Gamma_{\leq c}$ given by

$$\Gamma_{c,z}(T'||T) = \sum_{d \in \mathrm{Max}(T',c,z)} \Gamma_{d,d-z} \; + \; \Gamma(T)$$

where $\Gamma(T)$ is defined in (5.8.2) and (5.8.3).

(4) Note that if T', T are subsets of a finite saturated subset T'' of $\mathrm{Div}_+(A)$ and that T is saturated then we have

(a) $\quad \Gamma_{c,z}(T'||T) \; \subseteq \; \Gamma(T'')$;

(b) $\quad \Gamma_{c,z}(T) = \Gamma_{c,z}(\mathrm{Max}(T,c,z)||T \setminus \mathrm{Max}(T,c,z))$.

6.5.3. Lemma. *Assume that the image in R of the integer $|B^*|/|A^*|$ is a multiplicative unit. Let E_1, E_2 be subsets of E where*
(i) *all elements of E_1 and E_2 are $\leq c$;*
(ii) *E_2 is saturated;*
(iii) *$E_1 \neq \emptyset$ and $E_2 \neq \emptyset$ imply that $\mathrm{Sat}_z(E_1) \cap E_2 \neq \emptyset$.*

Let d be a maximal element of E_2. Assume that $d \not\leq c - z$ and $d \notin E_1$. Then the inclusion

$$\Gamma_{c,z}(E_1 \cup \{d\} || E_2 \setminus \{d\}) \subseteq \Gamma_{c,z}(E_1 || E_2)$$

induces surjective homomorphisms for all $m \geq 1$

$$H^m(G, \Gamma_{c,z}(E_1 \cup \{d\} || E_2 \setminus \{d\})_S) \to H^m(G, \Gamma_{c,z}(E_1 || E_2)_S).$$

Proof that lemma 6.5.3 implies lemma 6.4.3. Fix an integer $m \geq 1$. It is easily checked that for any subset M of $\mathrm{Max}(E, c, z)$, the sets $E_1 = M$ and $E_2 = E \setminus M$ satisfy the conditions (i), (ii), and (iii) of lemma 6.5.3; for the check of condition (iii), one observes that as $z \in \mathrm{Supp}(c)$ the elements of $\mathrm{Max}(E, c, z)$, if any, all contain z in their support.

Let $\mathcal{T}$ be the set of subsets M of $\mathrm{Max}(E, c, z)$ such that the inclusion

$$\Gamma_{c,z}(M || E \setminus M) \subseteq \Gamma(E)$$

induces a surjective homomorphism

$$H^m(G, \Gamma_{c,z}(M || E \setminus M)_S) \to H^m(G, \Gamma(E)_S).$$

Then we have these three statements (a), (b), and (c):

(a) $\mathcal{T}$ is a non empty finite set.

(b) $\mathcal{T}$ is equipped with a partial order $\leq$ where $M_1 \leq M_2$ if and only if $M_1 \subseteq M_2$.

(c) If $M \in \mathcal{T}$ and d is a maximal element of $E \setminus M$ where $d \not\leq c - z$ then $M \cup \{d\} \in \mathcal{T}$.

The statement (a) holds as the empty set $\emptyset$ is an element of $\mathcal{T}$ and E is a finite set. The statement (b) is evident.

To prove (c), suppose that $M \in \mathcal{T}$. Let d be a maximal point of $E \setminus M$ where $d \not\leq c - z$. Then we have $d \notin \mathrm{Sat}_z(M)$ and if $M \neq \emptyset$ and $E \neq M$ then we have

$$\mathrm{Sat}_z(M) \cap (E \setminus M) \neq \emptyset.$$

For if $x \in M$ then we have $x \not\leq c - z$ and $z \in \mathrm{Supp}(c)$ so that $z \in \mathrm{Supp}(x)$. Hence we have $x - z \in E \setminus M$ and $x - z \in \mathrm{Sat}_z(M)$. By lemma 6.5.3, we then obtain that the homomorphism

$$H^m(G, \Gamma_{c,z}(M \cup \{d\} || E \setminus (M \cup \{d\}))_S) \to H^m(G, \Gamma_{c,z}(M || E \setminus M)_S)$$

is surjective. That is to say, we have $M \cup \{d\} \subset \mathrm{Max}(E, c, z)$ and $M \cup \{d\} \in \mathcal{T}$. We have therefore proved (a),(b), and (c).

To end the proof of the implication, by (a) and (b) there is a maximal element M_∞ of $\mathcal{T}$, with respect to the partial order $\leq$ of (b). By (c), no maximal point of $E \setminus M_\infty$ is $\not\leq c - z$. Hence we have $M_\infty \supseteq \mathrm{Max}(E, c, z)$. As $M_\infty \subseteq \mathrm{Max}(E, c, z)$ by definition, we therefore have $M_\infty = \mathrm{Max}(E, c, z)$ and furthermore $\mathcal{T}$ is the set of all subsets of $\mathrm{Max}(E, c, z)$; the statement of lemma 6.4.3 is equivalent to the assertion that $\mathrm{Max}(E, c, z)$ is an element of $\mathcal{T}$ (see notation 6.5.2(4)). This proves the result. □

The rest of this section is occupied with the proof of lemma 6.5.3. Assume that d is a maximal element of E_2 such that $d \not\leq c - z$ and $d \notin E_1$ where E_1, E_2 satisfy the conditions (i),(ii), and (iii) of the lemma. The proof occupies several stages.

Stage 1. Derivation of the equation $\delta_d(g) = -\sum_i \frac{|O^*_{d-z_i}|}{|A^*|} e_{d,d-z_i} \eta_i(g)$

Let h be a cohomology class of

$$H^m(G, \Gamma_{c,z}(E_1 || E_2)_S).$$

That is to say h is the cohomology class of a m-cocycle with values in $\Gamma_{c,z}(E_1 || E_2)_S$. Then h is the class of a m-cocycle

$$\delta : G^m \to \Gamma_{c,z}(E_1 || E_2)_S.$$

Furthermore, h induces a cohomology class in $H^m(G, \Delta_{\leq c,S})$ and hence the component cochain δ_f of the cocycle δ is also a cocycle, where δ_f is given explicitly by

$$\delta_f : G^m \to \Delta_{f,S}$$

and

$$\delta = \bigoplus_{f \leq c} \delta_f.$$

That $\delta(g) \in \Gamma_{c,z}(E_1 || E_2)_S$ for all $g \in G^m$ is equivalent to an equation of the form (see notation 6.5.2)

(6.5.4)

$$\delta(g) = \sum_{\substack{d' \in E_1 \\ d' \not\leq c - z}} \gamma_{d', d' - z}(g) + \sum_{c' \in E_2} \sum_{w \in \mathrm{Supp}(c') \setminus \tilde{I}} \gamma_{c', c' - w}(g), \quad \text{for all } g \in G^m$$

for cochains

$$\gamma_{f,f-w} \in \mathrm{Coch}^m(G, \Gamma_{f,f-w,S}), \quad \text{for all } f, w,$$

and where w runs over a finite set of prime divisors in $\mathrm{Supp}(f) \setminus \tilde{I}$.

Let d be the chosen maximal element of E_2 such that $d \not\leq c - z$ and $d \notin E_1$. Let δ_d be the component cocycle of δ with values in in $\Delta_{d,S}$. We may write the equation (6.5.4) in the form

$$\delta = \sum_{\substack{d' \in E_1 \\ d' \not\leq c-z}} \gamma_{d',d'-z_1} + \sum_{c' \in E_2 - \{d\}} \sum_{w \in \mathrm{Supp}(c') \setminus \tilde{I}} \gamma_{c',c'-w} + \sum_{i=1}^{n} \gamma_{d,d-z_i}. \tag{6.5.5}$$

where $z_1, \ldots, z_n$ are the prime divisors in $\mathrm{Supp}(d) \setminus \tilde{I}$ and where $z_1 = z$.

We then have (see (5.3.6))

$$K_{f,f-w}(\delta) = (a_w - \epsilon(f,w)) t^{\Delta}_{f,f-w}(\delta) - \frac{|O^*_{f-w}|}{|A^*|} e_{f,f-w}\delta.$$

The component of $\gamma_{f,f-w}(g)$ in $\Delta_{d,S}$ is therefore zero if f is not equal to d, $d + w$ or $d + 2w$ (by the definition of $K_{f,f-w}$).

The hypothesis on d implies that d, $d + z_1$ and $d + 2z_1$ do not lie in the set E_1. Hence for the sum, for all $g \in G^m$,

$$\sum_{d' \in E_1, d' \not\leq c-z} \gamma_{d',d'-z_1}(g)$$

the component in $\Delta_{d,S}$ is equal to zero. Furthermore, for the sum, for all $g \in G^m$,

$$\sum_{c' \in E_2 - \{d\}} \sum_{w \in \mathrm{Supp}(c') \setminus \tilde{I}} \gamma_{c',c'-w}(g)$$

the component in $\Delta_{d,S}$ is equal to zero as d is a maximal element of the saturated set E_2.

The component in $\Delta_{d,S}$ of the right hand side of the equation (6.5.5) is then the component in $\Delta_{d,S}$ of the sum

$$\sum_{i=1}^{n} \gamma_{d,d-z_i}(g)$$

for all $g \in G^m$. The cochains $\gamma_{d,d-z_i}$ are of the form

$$g \mapsto K_{d,d-z_i}(\eta_i(g)), \ G^m \to \Gamma_{d,d-z_i,S},$$

for some cochains

$$\eta_i \in \mathrm{Coch}^m(G, \Delta_{d,S}).$$

Hence the component of this equation (6.5.5) in $\Delta_{d,S}$ is the equation (see (5.3.6))

$$\delta_d(g) = -\sum_{i=1}^{n} \frac{|O^*_{d-z_i}|}{|A^*|} e_i \eta_i(g) \quad \text{for all } g \in G^m \tag{6.5.6}$$

where we write

$$e_i = e_{d,d-z_i} = \sum_{g \in G_i} g \tag{6.5.7}$$

and

$$G_i = \ker(t_{d,d-z_i}) = G(d/d-z_i), \quad \text{for all } i,$$

and $\delta_d(g)$ is the component in $\Delta_{d,S}$ of $\delta(g)$, in particular δ_d is a cocycle in $\mathrm{Cocy}^m(G_1, \Delta_{d,S})$.

Stage 2. Formulae for the η_i.

By proposition 5.8.4, $\{G_i\}_{i=1,\ldots,n}$ forms an S-admissible family of subgroups of $\mathrm{Pic}(O_d)$, where $\Delta_{d,S}$ is the group algebra $S[\mathrm{Pic}(O_d)]$. We may then apply proposition 5.6.28 to the equation (6.5.6). We obtain that there are cochains

$$\eta^{(i,j)} : G_1^m \to \Delta_{d,S} \quad \text{for all } i \neq j \text{ and } 1 \leq i, j \leq n$$

such that

$$\eta^{(i,j)} = -\eta^{(j,i)}, \quad \text{for all } i \neq j \text{ and } 1 \leq i, j \leq n, \tag{6.5.8}$$

and cochains

$$\delta_i : G_1^m \to \Delta_{d,S} \quad \text{for all } 1 \leq i \leq n \tag{6.5.9}$$

such that the maps $e_i\delta_i : G_1^m \to \Delta_{d,S}$ are m-cocycles (in fact they are m-coboundaries for $i \geq 2$) for all $i = 1, \ldots, n$ where we have

$$\frac{|O^*_{d-z_i}|}{|A^*|} e_i \eta_i(g) = e_i \delta_i(g) + \sum_{j \neq i} e_{ij} \eta^{(i,j)}(g) \quad \text{for all } 1 \leq i \leq n, g \in G_1^m \tag{6.5.10}$$

where we put

$$e_{ij} = \sum_{h \in G_i G_j} h. \tag{6.5.11}$$

From this we obtain the equation

$$\delta_d = -\sum_{i=1}^{n} e_i \delta_i. \tag{6.5.12}$$

The equation (6.5.10) then may be written

$$\frac{|O^*_{d-z_i}|}{|A^*|}e_i\eta_i = e_i\delta_i + \sum_{j\neq i} e_{ij}\eta^{(i,j)} \quad \text{for all } 1 \leq i \leq n. \tag{6.5.13}$$

Stage 3. The formula $\sum_i K_{d,d-z_i}(\eta_i(g))$; the case where $n = 1$.

The equation (6.5.5) becomes

$$\delta = \sum_{\substack{d'\in E_1\\ d'\not\leq c-z}} \gamma_{d',d'-z_1} + \sum_{c'\in E_2-\{d\}} \sum_{w\in \mathrm{Supp}(c')\setminus\tilde{I}} \gamma_{c',c'-w} + \gamma_{d,d-z_1}.$$

This expression may then be written as

$$\delta = \gamma_1 + \gamma_2 \tag{6.5.14}$$

where

$$\gamma_1 = \sum_{\substack{d'\in E_1\cup\{d\}\\ d'\not\leq c-z}} \gamma_{d',d'-z_1}$$

and

$$\gamma_2 = \sum_{c'\in E_2-\{d\}} \sum_{w\in \mathrm{Supp}(c')\setminus\tilde{I}} \gamma_{c',c'-w}.$$

Put

$$\Gamma = \Gamma_{c,z_1}(E_1\cup\{d\}||E_2-\{d\})_S.$$

We have for all $g \in G^m$

$$\gamma_1(g) \in \Gamma$$

$$\gamma_2(g) \in \Gamma(E_2-\{d\})_S \subseteq \Gamma.$$

Hence we have for all $g \in G_1^m$

$$\delta(g) \ \in \ \Gamma.$$

This completes the proof of the lemma 6.4.3 in this case where $n = 1$.

Stage 4. The formula $\sum_i K_{d,d-z_i}(\eta_i(g))$; the case where $n \geq 2$.

The divisor d is not prime, as it has at least two prime divisors in its support by the hypothesis $n \geq 2$. The equation (6.5.13) becomes

$$e_i\eta_i(g) = e_i\delta_i(g) + \sum_{j\neq i} e_{ij}\eta^{(i,j)}(g) \quad \text{for all } 1 \leq i \leq n, g \in G_1^m.$$

We may now apply lemma 5.10.1 to the sum $\sum_{j\neq i} e_{ij}\eta^{(i,j)}(g)$. We obtain that for all $g \in G_1^m$

(6.5.15)

$$N\sum_{i=1}^{n}\gamma_{d,d-z_i}(g) = N\Big\{\sum_{i=1}^{n}K_{d,d-z_i}(\eta_i(g))\Big\} = N\Big\{\sum_{i=1}^{n}K_{d,d-z_i}(\delta_i(g))\Big\} + S(g)$$

where

(6.5.16)

$$S(g) = -\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i} - \epsilon(d,z_i))K_{d-z_i,d-z_i-z_j}(t^{\Delta}_{d,d-z_i}(\eta^{(i,j)}(g)))$$

and where

$$N = \frac{|O^*_{d-z_1-z_2}|}{|A^*|}. \tag{6.5.17}$$

Note that $N = 1$ unless $n = 2$ and $d = z_1 + z_2$.

As N is a unit of R, we have from (6.5.15)

$$\sum_{i=1}^{n}\gamma_{d,d-z_i}(g) = \sum_{i=1}^{n}K_{d,d-z_i}(\delta_i(g)) + \frac{1}{N}S(g). \tag{6.5.18}$$

As E_2 is saturated we have $f \in E_2 \setminus \{d\}$ for all divisors $f \geq 0$ such that $f < d$. From the expression (6.5.16) of S, and the compatibility of the K's with the transition homomorphisms t^{Δ} (proposition 5.7.8(iii)), we obtain

$$S(g) \quad \in \quad \Gamma(E_2 - \{d\})_S \quad \text{for all } g \in G_1^m. \tag{6.5.19}$$

The form (6.5.5) of the equation (6.5.4) reads

$$\delta = \sum_{\substack{d'\in E_1\\ d'\not\leq c-z}}\gamma_{d',d'-z_1} + \sum_{c'\in E_2-\{d\}}\sum_{w\in \mathrm{Supp}(c')\setminus\tilde{I}}\gamma_{c',c'-w} + \sum_{i=1}^{n}\gamma_{d,d-z_i}.$$

Hence by (6.5.18) we obtain for all $g \in G_1^m$

$$\delta(g) = \sum_{\substack{d'\in E_1\\ d'\not\leq c-z}}\gamma_{d',d'-z_1}(g) + \sum_{c'\in E_2-\{d\}}\sum_{w\in \mathrm{Supp}(c')\setminus\tilde{I}}\gamma_{c',c'-w}(g) +$$

$$\sum_{i=1}^{n}K_{d,d-z_i}(\delta_i(g)) + \frac{1}{N}S(g)$$

where $S(g) \in \Gamma(E_2 - \{d\})_S$ is given by (6.5.16).

We obtain

$$\delta(g) - \sum_{i=2}^{n}K_{d,d-z_i}(\delta_i(g)) = \gamma_1(g) + \gamma_2(g) \tag{6.5.20}$$

where γ_1, γ_2 are given by, for all $g \in G_1^m$,

$$\gamma_1(g) = \sum_{\substack{d' \in E_1 \\ d' \not\leq c-z}} \gamma_{d',d'-z_1}(g) + K_{d,d-z_1}(\delta_1(g))$$
$$\gamma_2(g) = \sum_{c' \in E_2 - \{d\}} \sum_{w \in \mathrm{Supp}(c') \setminus \tilde{I}} \gamma_{c',c'-w}(g) + \frac{1}{N} S(g)$$

where

$$\gamma_1(g) \in \Gamma_{c,z}(E_1 \cup \{d\} || \emptyset)_S \quad \text{for all } g \in G_1^m$$

and where

$$\gamma_2(g) \in \Gamma(E_2 - \{d\})_S \quad \text{for all } g \in G_1^m.$$

Hence we have that $\gamma_1 + \gamma_2$ is a cochain

$$\gamma_1 + \gamma_2 \ : \ G_1^m \ \rightarrow \ \Gamma_{c,z_1}(E_1 \cup \{d\} || E_2 - \{d\})_S.$$

As

$$e_i \delta_i : G_1^m \rightarrow \Delta_{d,S}$$

is an m-coboundary for all $i \geq 2$ and is an m-cocycle for $i = 1$, we have that

$$g \mapsto \sum_{i=2}^{n} K_{d,d-z_i}(\delta_i(g))$$

is a m-coboundary in $\mathrm{Cob}^m(G_1, \Gamma(E_2)_S)$ as the maps $K_{d,d-z_i}$ are homomorphisms of Δ_d-modules. As δ is a cocycle it follows from the equation (6.5.20), that the cochain $\gamma_1 + \gamma_2$ is an m-cocycle. It also follows from the equation (6.5.20) that the cohomology class h of $\delta \in \mathrm{Cocy}^m(G_1, \Gamma_{c,z}(E_1 || E_2)$ is represented by this cocycle $\gamma_1 + \gamma_2$. That is to say, h lies in the image of the homomorphism

$$H^m(G, \Gamma_{c,z}(E_1 \cup \{d\} || E_2 \setminus \{d\})_S) \rightarrow H^m(G, \Gamma_{c,z}(E_1 || E_2)_S). \qquad \square$$

6.6 The main proposition

Proposition 6.6.3 below is the main result on the cohomology of the Heegner module for a general R-algebra S. In the case when S is an artin local ring of embedding dimension 1 (an *infinitesimal trait*), we obtain more precise results in the next sections.

(6.6.1) We assume throughout this section that

n is the image in R of the integer $|B^*|/|A^*|$ and is assumed to be a multiplicative unit of R;
S is an R-algebra;
$c' \leq c$ are effective divisors on Spec A;
z is a prime divisor in the support of c where $z \notin \tilde{I}$;
G is the galois group $G(c/c-z)$.

(6.6.2) The transition homomorphism $\mathcal{H}_{c-z,S} \to \mathcal{H}_{c,S}$ induces homomorphisms of cohomology for all $m \geq 1$

$$H^{m-1}(G, \mathcal{H}_{c-z,S}) \xrightarrow{t} H^{m-1}(G, \mathcal{H}_{c,S}).$$

We write

$$\frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))}$$

for the cokernel of this homomorphism.

Let Γ_R be the submodule of $\Gamma_{\leq c,R}$ given by

$$\Gamma_R = \bigoplus_{\substack{c' \leq c \\ c' \not\leq c-z}} \Gamma_{c',c'-z}.$$

That Γ_R is a direct sum of the modules $\Gamma_{c',c'-z}$ for all $c' \leq c$ such that $c' \not\leq c - z$ follows from the inclusions

$$\Gamma_{c',c'-z} \subseteq \Delta_{c',R} \oplus \Delta_{c'-z,R} \oplus \Delta_{c'-2z,R}$$

for all c'. There is a projection homomorphism

$$\pi : \Gamma_R \to \Delta_{\leq c-z,R}$$

obtained as a composite $\Gamma_R \hookrightarrow \Delta_{\leq c,R} \to \Delta_{\leq c-z,R}$.

6.6.3. Proposition. *There are natural surjective homomorphisms of $\Delta_{c-z,S}$-modules for all $m \geq 1$*

$$\Xi : \ker\{H^m(G,S) \otimes_R \Gamma_R \xrightarrow{\mathrm{Id}\otimes\pi} H^m(G,S) \otimes_R \Delta_{\leq c-z,R}\} \to \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))}.$$

Proof of proposition 6.6.3. Let E be the subset of $\mathrm{Div}_+(A)$ of divisors $\leq c$. By lemma 6.4.3 and lemma 6.2.15, for all integers $m \geq 1$ we may construct a commutative diagram with an exact row

$$\begin{array}{ccccccc} H^{m-1}(G, \mathcal{H}_{c-z,S}) & \xrightarrow{t} & H^{m-1}(G, \mathcal{H}_{c,S}) & \to & H^m(G, \Gamma_{\leq c,S}) & \xrightarrow{f} & H^m(G, \Delta_{\leq c,S}) \\ & & & & i \uparrow & \nearrow h & \\ & & & & H^m(G, \Gamma_{c,z}(E)_S) & & \end{array}$$

where the vertical arrow i is a surjective homomorphism induced from the inclusion $\Gamma_{c,z}(E)_S \subseteq \Gamma_{\leq c,S}$ (see notation 6.4.2(2)). Furthermore, for $m = 1$ the homomorphism t is an injection (by lemma 6.2.11).

Let H be the kernel of the homomorphism

$$f : H^m(G, \Gamma_{\leq c,S}) \to H^m(G, \Delta_{\leq c,S}).$$

This diagram provides a surjection

$$\ker\{h : H^m(G, \Gamma_{c,z}(E)_S) \to H^m(G, \Delta_{\leq c,S})\} \to H.$$

By lemma 6.6.4 below, we obtain an isomorphism of $\Delta_{c,R}$-modules

$$\Gamma_{c,z}(E)_R \cong \Gamma_{\leq c-z} \oplus \Gamma_R.$$

By corollary 5.9.6 and lemma 6.2.2(i), the modules $\Gamma_{\leq c-z}$ and $\Gamma_{c',c'-z}$ are finite flat R-modules for all c'; hence Γ_R is a finite flat R-module. Hence we have an isomorphism, as G acts trivially on $\Gamma_{\leq c-z}$ and on $\Gamma_{c',c'-z}$ for all $c' \leq c$,

$$H^m(G, \Gamma_{c,z}(E)_S) \cong H^m(G, S) \otimes_R \Big(\Gamma_{\leq c-z} \oplus \Gamma_R\Big).$$

Furthermore, by lemma 6.2.14, we have isomorphisms of $\Delta_{c,S}$-modules

$$H^m(G, \Delta_{\leq c,S}) \cong H^m(G, S) \otimes_R \Delta_{\leq c-z,R} \quad \text{for all } m \geq 1.$$

Hence the kernel

$$\ker\{h : H^m(G, \Gamma_{c,z}(E)_S) \to H^m(G, \Delta_{\leq c,S})\}$$

is isomorphic as a $\Delta_{c,S}$-module to the kernel of the homomorphism

$$H^m(G, S) \otimes_R \big(\Gamma_{\leq c-z} \oplus \Gamma_R\big) \to H^m(G, S) \otimes_R \Delta_{\leq c-z,R}.$$

But

$$H^m(G, S) \otimes_R \Gamma_{\leq c-z} \;\to\; H^m(G, S) \otimes_R \Delta_{\leq c-z,R}$$

is an injection, as $\Gamma_{\leq c-z}$ is a universal R-submodule of $\Delta_{\leq c-z,R}$ (lemma 6.2.5).

Hence the kernel of the homomorphism h is isomorphic to

$$\bigoplus_{\substack{c' \le c \\ c' \not\le c-z}} \ker\{H^m(G,S) \otimes_R \Gamma_{c',c'-z} \to H^m(G,S) \otimes_R \Delta_{\le c-z,R}\}.$$

The surjection $\ker(h) \to H$ combined with the isomorphism of $\Delta_{c-z,S}$-modules, obtained from the above diagram,

$$H \cong \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))}, \quad \text{for } m \ge 1,$$

completes the proof. □

6.6.4. Lemma. *Let E be the saturated set*

$$E = \{c' |\ c' \le c,\ c' \in \mathrm{Div}_+(A)\}.$$

Then the natural map (see notation 6.4.2(2))

$$\Gamma_{\le c-z} \oplus \Gamma_R \quad \to \quad \Gamma_{c,z}(E)$$

is an isomorphism of $\Delta_{c,R}$-modules.

Proof of lemma 6.6.4. Evidently, $\Gamma_{c,z}(E)$ is the sum of the $\Delta_{c,R}$-submodules $\Gamma_{\le c-z}$ and $\Gamma_{c',c'-z}$ for all c' such that $c' \le c,\ c' \not\le c-z$; the problem is to show that this sum is direct.

By definition Γ_R is the submodule of $\Delta_{\le c,R}$ given by

$$\Gamma_R = \bigoplus_{c' \le c,\ c' \not\le c-z} \Gamma_{c',c'-z}.$$

Let

$$\mathrm{pr} : \Delta_{\le c,R} \to \bigoplus_{c' \le c,\ c' \not\le c-z} \Delta_{c',R}$$

be the projection homomorphism with kernel $\Delta_{\le c-z,R}$. The restriction of pr to $\Gamma_{c',c'-z}$ induces an isomorphism $\Gamma_{c',c'-z} \cong e_{c',c'-z}\Delta_{c',R}$ for all $c' \le c$ such that $c' \not\le c-z$, by lemma 6.2.2(i). Hence we may construct a commutative diagram with an exact row and injective vertical inclusion maps

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Delta_{\le c-z,R} & \longrightarrow & \Delta_{\le c,R} & \xrightarrow{\mathrm{pr}} & \displaystyle\bigoplus_{c' \le c,\ c' \not\le c-z} \Delta_{c',R} & \longrightarrow & 0 \\
 & & & & \uparrow & & \uparrow & & \\
 & & & & \Gamma_R & \xrightarrow{\cong} & \displaystyle\bigoplus_{c' \le c,\ c' \not\le c-z} e_{c',c'-z}\Delta_{c',R} & &
\end{array}$$

It follows from this diagram that

$$\Gamma_R \cap \Delta_{\leq c-z,R} = 0.$$

Hence $\Gamma_{c,z}(E)$ is a direct sum as in the statement of the lemma. □

6.7 The submodule $J_{c,z,S}$

In this section we define the submodule $J_{c,z,S}$ of $\Delta_{c,S}$ and determine its isomorphism class when S is an infinitesimal trait (theorem 6.7.16). The connection with the cohomology of the Heegner module is that if the group $H^m(G,S)$ is isomorphic to S then the map Ξ of proposition 6.6.3 concides with a surjective homomorphism

$$\Xi : J_{c,z,S} \ \rightarrow \ \frac{H^{m-1}(G,\mathcal{H}_{c,S})}{t(H^{m-1}(G,\mathcal{H}_{c-z,S}))}.$$

This is considered further in the next sections §§6.9-6.11.

(6.7.1) We assume throughout this section that

S is an R-algebra;
n is the image in R of the integer $|B^*|/|A^*|$ and is assumed to be a multiplicative unit of R;
c is an effective divisor on Spec A;
z is a prime divisor in the support of c where $z \notin \tilde{I}$.

Definition of $J_{c,z,S}$

(6.7.2) The R-module $\Gamma_{c,c-z} = K_{c,c-z}(\Delta_{c,R})$ is a universal submodule of $\Delta_{\leq c,R}$ (by lemma 6.2.2(ii) and (6.2.1)). For any R-algebra S we then obtain the two homomorphisms of $\Delta_{c,S}$-modules

$$\Gamma_{c,c-z,S} \ \hookrightarrow \ \Delta_{\leq c,S} \ \stackrel{\pi}{\rightarrow} \ \Delta_{\leq c-z,S}$$

where π is the projection homomorphism onto the submodule $\Delta_{\leq c-z,S}$ of $\Delta_{\leq c,S}$. The composite of these two homomorphisms is the homomorphism of $\Delta_{c,S}$-modules

$$\pi_\Gamma : \Gamma_{c,c-z,S} \rightarrow \Delta_{\leq c-z,S}.$$

6.7.3. Definition. Put

$$J_{c,z,S} = \ker\bigl(\pi_\Gamma : \Gamma_{c,c-z,S} \to \Delta_{\leq c-z,S}\bigr).$$

Note that $J_{c,z,S}$, as a submodule of the graded module $\Delta_{\leq c,S}$, has all its components zero except for that in $\Delta_{c,S}$; hence $J_{c,z,S}$ is a submodule of $\Delta_{c,S}$.

(6.7.4) By definition of $\Gamma_{c,c-z}$, the module $J_{c,z,S}$ is $\Delta_{c,S}$-isomorphic to the kernel of the $\Delta_{c,S}$-module homomorphism (see (5.3.5) et seq.)

$$(a_z - \epsilon(c,z)) : \Delta_{c-z,S} \to \Delta_{\leq c-z,S}, \quad \delta \mapsto a_z\delta - \epsilon(c,z)\delta.$$

Infinitesimal traits

6.7.5. Definition. (1) An *infinitesimal trait* M is an artin local ring M which is a quotient of a discrete valuation ring.

This condition is equivalent to M being an artin local ring whose maximal ideal is principal. For example, for any prime number l and any integer $n \geq 0$ the ring $\mathbb{Z}/l^n\mathbb{Z}$ is an infinitesimal trait.
(2) A *local parameter* π of the infinitesimal trait M is an element $\pi \in M$ which generates the maximal ideal of M.
(3) Let π be a local parameter of the infinitesimal trait M. Let $v_M : M \to \mathbb{N}$ be the map defined by $v_M(x) = n$ where $n \geq 0$ is the greatest integer such that $x \in \pi^n M$. We put $v_M(0) = l$, where l is the length of M as an artin M-module.

The map v_M is the *valuation* of the infinitesimal trait M.

(6.7.6) An *n-dimensional character* χ of a finite group G with values in the infinitesimal trait M is a group homomorphism $\chi : G \to \mathrm{GL}_n(M)$; this is equivalent to an action of G on a free M-module of rank n.

6.7.7. Proposition. *Let M be an infinitesimal trait with local parameter π. Let G be a finite group of order prime to the residue characteristic of M. Then any character*

$$\chi_m : G \to \mathrm{GL}_n(M/\pi^m M)$$

lifts to a character

$$\chi_{m+1} : G \to \mathrm{GL}_n(M/\pi^{m+1} M)$$

and this lifting is unique up to conjugation by an element of $\mathrm{GL}_n(M/\pi^{m+1}M)$ which is congruent to 1 modulo π^m.

In particular, any character

$$\chi : G \to \mathrm{GL}_n(M/\pi M)$$

lifts essentially uniquely to a character

$$\chi^\sharp : G \to \mathrm{GL}_n(M).$$

[This result is Exercise 15.9 of [S2]. It is assumed there that M is a quotient of a mixed characteristic discrete valuation ring; but this hypothesis is superfluous for this proposition.] □

Notation

(6.7.8) Let M be a (commutative) ring and let V *either* be a module over M *or* an endomorphism of M as an M-module. The *annihilator* of V is the ideal of M

$$\mathrm{Ann}_M(V) = \{m \in M |\ \ mV = 0\}.$$

Note that if $a \in M$ and M is an infinitesimal trait with valuation v and local parameter π, then we have $\mathrm{Ann}_M(a) = \pi^{l-v(a)}M$, where l is the length of M as an artin M-module.

(6.7.9) Let $\mathfrak{p}_i$, $i = 1, \ldots, m$, (where $m \leq 2$) be the prime ideals of the order O_{c-z} of K lying over the prime ideal of A corresponding to z. Let $[[\mathfrak{p}_i]]$ denote the divisor class (as in (4.6.2)) of $\mathrm{Pic}(O_{c-z})$ defined by the fractionary ideal $\mathfrak{p}_i$ of O_{c-z} when z is disjoint from the support of $c - z$.

Let P be the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the classes $[[\mathfrak{p}_i]]$, $i = 1, \ldots, m$; that is to say P is the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by all prime divisors of O_{c-z} lying over z when $z \notin \mathrm{Supp}(c - z)$.

Characters of rank 1 of the group P

(6.7.10) Let P the group defined in (6.7.9). Suppose the R-algebra S is an infinitesimal trait with local parameter π. Let L be an ideal of S. Let χ be a rank 1 character of P with values in the R-algebra S/L that is to say χ is a group homomorphism

$$\chi : P \to (S/L)^*$$

where $(S/L)^*$ denotes the group of units of S/L. Fix an isomorphism of $\Delta_{c,S}$-modules

$$i : \Delta_{c,S/L} \xrightarrow{\sim} \mathrm{Ann}_S(L)\Delta_{c,S}.$$

Recall that $t_{c,c-z} : \mathrm{Pic}(O_c) \to \mathrm{Pic}(O_{c-z})$ is the group homomorphism induced from the inclusion of orders $O_c \subseteq O_{c-z}$ (see (5.2.2)). Let $\tilde{P}$ be the subgroup of $\mathrm{Pic}(O_c)$ given by

$$\tilde{P} = t_{c,c-z}^{-1}(P).$$

From χ, we obtain a character $\tilde{\chi}$ of $\tilde{P}$ via

$$\tilde{\chi} : \tilde{P} \to (S/L)^*, \quad g \mapsto \chi(t_{c,c-z}(g)).$$

Let f_χ be the element of $e_{c,c-z}\Delta_{c,S/L}$ given by

$$f_\chi = \sum_{g \in \tilde{P}} g\tilde{\chi}(g).$$

Let I_χ be the ideal of the group algebra $\Delta_{c,S}$ given by

$$I_\chi = i(f_\chi \Delta_{c,S/L}).$$

The ideal I_χ is independent of the choice of isomorphism $i : \Delta_{c,S/L} \to \mathrm{Ann}_S(L)\Delta_{c,S}$ and we have the inclusion

$$I_\chi \ \subseteq \ \mathrm{Ann}_S(L)e_{c,c-z}\Delta_{c,S}.$$

In particular, I_χ is naturally a $\Delta_{c-z,S/L}$-module and hence a $\frac{S}{L}[P]$-module.

(6.7.11) Let χ be a rank 1 character of P with values in the R-algebra S/L

$$\chi : P \to (S/L)^*.$$

The ideal I_χ, which is a $\Delta_{c-z,S/L}$-module, satisfies that for all $g \in P$ we have

$$gI_\chi = \chi^{-1}(g)I_\chi.$$

More precisely, it is easily checked that

$$I_\chi = \{x \in \mathrm{Ann}_S(L)e_{c,c-z}\Delta_{c,S} |\ \ gx = \chi^{-1}(g)x \ \text{ for all } \ g \in P\}.$$

If S is a field, then I_χ is the χ^{-1}-isotypical component of $e_{c,c-z}\Delta_{c,S}$; that is to say I_χ is the submodule of $e_{c,c-z}\Delta_{c,S}$ on which P acts like the character χ^{-1}, which is the contragredient character to χ.

(6.7.12) If L' is an ideal of S such that $L' \supseteq L$ then $\chi : P \to (S/L)^*$ defines a character

$$\psi : P \to \big(\frac{S}{L'}\big)^*.$$

by composing χ with the surjective homomorphism $(S/L)^* \to (S/L')^*$. It is easily checked that

$$I_\psi = [L : L']I_\chi$$

where $[L : L']$ is the conductor ideal

$$[L : L'] = \{s \in S| \ \ sL' \subseteq L\}.$$

Representations of $P_{(l)}$

(6.7.13) Let l be the characteristic of the residue field of the infinitesimal trait S with local parameter π. Let $P_{(l)}$ be the l-primary subgroup of P, that is to say the subgroup of elements whose orders are prime to l. If $l = 0$ then $P_{(l)} = P$.

(6.7.14) Let M be a $S[P_{(l)}]$-module which is free as an S-module. Then $M \otimes_S S/(\pi)$ is a direct sum of irreducible $S/(\pi)[P_{(l)}]$-modules

$$M \otimes_S S/(\pi) = \bigoplus_i N_i.$$

This decomposition lifts to M (see [S2, Exercice 14.3])

$$M = \bigoplus_i M_i$$

where the M_i are submodules of M and $M_i/\pi M_i$ is isomorphic to N_i. The M_i are then indecomposable $S[P_{(l)}]$-modules.

For any irreducible character $\chi : P_{(l)} \to \mathrm{GL}_n(S/(\pi))$, let $N(\chi)$ be the χ-isotypical component of $M \otimes_S S/(\pi)$. Then χ lifts essentially uniquely to an indecomposable representation (proposition 6.7.7)

$$\chi^\sharp : P_{(l)} \to \mathrm{GL}_n(S).$$

Let $M(\chi)$ be the direct sum of the components M_i of M which are isomorphic to the representation $\chi^\sharp$. Then we have the decomposition

$$M = \bigoplus_{\chi} M(\chi).$$

We call $M(\chi)$ the *χ-isotypical component* of M.

(6.7.15) Let P_{l^∞} denote the lth-power torsion subgroup of P. Then P decomposes as the direct product

$$P \cong P_{(l)} \times P_{l^\infty}$$

and the algebra $S[P]$ decomposes as

$$S[P] \cong S[P_{(l)}] \otimes_S S[P_{l^\infty}].$$

Then $S[P_{(l)}]$, as a module over itself, decomposes as

$$S[P_{(l)}] \cong \bigoplus_{\chi} S(\chi)$$

where $S(\chi)$ is the χ-isotypical component of $S[P_{(l)}]$ and χ runs over all the distinct irreducible representations of $S/(\pi)[P_{(l)}]$ over the field $S/(\pi)$.

We obtain the decomposition of $S[P]$ as a module over itself

$$S[P] \cong \bigoplus_{\chi} S(\chi) \otimes_S S[P_{l^\infty}].$$

We call $S(\chi) \otimes_S S[P_{l^\infty}]$ the *χ-isotypical component* of $S[P]$.

Similarly, if M is a finite free $S[P]$-module we obtain a decomposition of M as an $S[P]$-module

$$M \cong \bigoplus_{\chi} M(\chi)$$

where $M(\chi)$ is the *χ-isotypical component* of M.

The main theorem

6.7.16. Theorem. *Suppose that the R-algebra S is an infinitesimal trait with local parameter π and residue field of characteristic $l \geq 0$. For an element $a \in R$ we write $a \otimes 1$ for its image in S. Then the $\Delta_{c,S}$-submodule $J_{c,z,S}$ of $\Delta_{c,S}$ is given by the following table (the notation is the same as that of table 4.6.9):*

(1) If z remains prime in K/F and is prime to $c-z$ then $J_{c,z,S}$ is: $\mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{c,S}$
(2) If z is ramified in K/F and is prime to $c-z$ where $\mathfrak{m}'_z$ is the prime ideal of O_{c-z} lying above the ideal $\mathfrak{m}_z$ of A defining z then $J_{c,z,S}$ is: I_{χ_L} where L is the smallest ideal of S for which there is a rank 1 character $\chi_L : P \to (S/L)^*$ of P such that $a_z \otimes 1 \equiv \chi_L([[\mathfrak{m}'_z]])\pmod{L}$.
(3) If z is split completely in K/F and is prime to $c-z$ where $\mathfrak{m}_z O_{c-z} = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct prime ideals of O_{c-z} then $J_{c,z,S}$ is: $\bigoplus_{\chi} \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1})$ where the sum runs over the irreducible characters $\chi : P_{(l)} \to \mathrm{GL}_n(S/(\pi))$ for all n of $P_{(l)}$ and where $\Delta(\chi)$ is the χ-isotypical component of $e_{c,c-z}\Delta_{c,S}$ (see (6.7.15)).
(4) If $z \in \mathrm{Supp}(c-z)$ then $J_{c,z,S}$ is: $\mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}I_{c,c-2z,S}$ where $I_{c,c-2z,S}$ is the kernel of $t^{\Delta}_{c,c-2z} : \Delta_{c,S} \to \Delta_{c-2z,S}$.

Table 6.7.16: $J_{c,z,S}$ as a submodule of $\Delta_{c,S}$ when S is an infinitesimal trait

Proof of theorem 6.7.16. By definition of $J_{c,z,S}$, we have the exact sequence of $\Delta_{c,S}$-modules

$$0 \to J_{c,z,S} \to \Gamma_{c,c-z,S} \to \Delta_{\leq c-z,S}.$$

Hence we have an isomorphism of $\Delta_{c,S}$-modules

$$J_{c,z,S} \cong \{x \in \Delta_{c-z,S} \mid (a_z \otimes 1 - \epsilon(c,z))(x) = 0\}$$

where the homomorphisms $\epsilon(c,z)$ are defined in (5.3.5) and (5.3.6).

We now distinguish the 4 cases in the table 6.7.16.

(1) Suppose that z is inert in K/F and $z \notin \mathrm{Supp}(c-z)$; then we have (see (5.3.5))

$$\epsilon(c,z) = 0.$$

As a submodule of $\Delta_{c,S}$ we obtain

$$J_{c,z,S} = \{e_{c,c-z}\delta \mid \delta \in \Delta_{c,S} \text{ and } (a_z \otimes 1)e_{c,c-z}\delta = 0\}.$$

Hence we have the equality of submodules of $\Delta_{c,S}$

$$J_{c,z,S} = \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{c,S}.$$

(2) Suppose that z is ramified in K/F and $z \notin \mathrm{Supp}(c-z)$; then we have (see (5.3.5))

$$\epsilon(c,z) =< [[\mathfrak{m}'_z]]^{-1}, c-z >= [[\mathfrak{m}'_z]]^{-1}.$$

Put

$$g = \epsilon(c,z).$$

Then we have an equality of submodules of $\Delta_{c,S}$

$$J_{c,z,S} = \{e_{c,c-z}\delta \mid \delta \in \Delta_{c,S} \text{ and } (a_z \otimes 1 - g)t^{\Delta}_{c,c-z}(\delta) = 0\}.$$

Let P be the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by g, as in (6.7.9).

Let L be an ideal of S and let

$$\chi : P \to (S/L)^*$$

be a rank 1 character of P with values in S/L. From (6.7.11), we have that

$$I_\chi = \{x \in \mathrm{Ann}_S(L)e_{c,c-z}\Delta_{c,S} \mid \ hx = \chi^{-1}(h)x \ \text{ for all } \ h \in P\}.$$

As P is generated by g, it follows that

$$I_\chi \subseteq J_{c,z,S}$$

whenever χ satisfies

$$a_z \otimes 1 \equiv \chi(g)^{-1} \pmod{L}.$$

We obtain the inclusion of submodules of $\Delta_{c,S}$

$$J_{c,z,S} \supseteq \sum_L I_{\chi_L} \tag{6.7.17}$$

where the sum $\sum_L$ runs over all ideals L of S for which there is a character $\chi_L : P \to (S/L)^*$ of P such that

$$a_z \otimes 1 \equiv \chi_L([[\mathfrak{m}'_z]]) \pmod{L}.$$

Note that if such a character χ exists, it is uniquely determined by the ideal L.

Let j be an element of $J_{c,z,S}$. Let L be the ideal of S given by

$$L = \{s \in S \mid sj = 0\}$$

which is the annihilator of j. Then S/L acts on the S-submodule Sj of $J_{c,z,S}$ generated by j. Furthermore, as $j \in J_{c,z,S}$ we have

$$gt^{\Delta}_{c,c-z}(j) = (a_z \otimes 1)t^{\Delta}_{c,c-z}(j).$$

As g generates the group P we may define a character

$$\phi : P \to (S/L)^*$$

via

$$g^{-1} \mapsto a_z \otimes 1 \pmod{L}.$$

As the group P acts on $J_{c,z,S}$ and $j \in J_{c,z,S}$, we have for all $h \in P$

$$hj = \phi(h)^{-1} j.$$

We then have that $j \in I_\phi$ (see (6.7.10)). As j is any element of $J_{c,z,S}$, this shows that the inclusion (6.7.17) stated in the previous paragraph is an equality of submodules of $\Delta_{c,S}$

$$J_{c,z,S} = \sum_L I_{\chi_L}$$

where the sum $\sum_L$ runs over all ideals L of S for which there is a character $\chi_L : P \to (S/L)^*$ of P such that

$$a_z \otimes 1 \equiv \chi_L([[\mathfrak{m}'_z]]) \pmod{L}.$$

As S is an infinitesimal trait, there is a smallest ideal L_0 of S such that the order of $a_z \otimes 1$ in $(S/L_0)^*$ divides the order of g in $\mathrm{Pic}(O_{c-z})$. Then we have

$$J_{c,z,S} = I_{\chi_0}$$

where

$$\chi_0 : P \to (S/L_0)^*$$

is the character defined via

$$g^{-1} \mapsto a_z \otimes 1 \pmod{L_0}.$$

(3) Suppose that z is split completely in K/F and $z \notin \mathrm{Supp}(c-z)$; then we have (see (5.3.5))

$$\epsilon(c,z) = < [[\mathfrak{p}_1]]^{-1}, c-z > + < [[\mathfrak{p}_2]]^{-1}, c-z > .$$

Put

$$g = < [[\mathfrak{p}_1]]^{-1}, c-z >$$
$$h = < [[\mathfrak{p}_2]]^{-1}, c-z > .$$

Thus P is the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by g and h, as in (6.7.9). Then we have an equality of submodules of $\Delta_{c,S}$

$$J_{c,z,S} = \{e_{c,c-z}\delta \mid \delta \in \Delta_{c,S} \text{ and } (a_z \otimes 1 - g - h)t^{\Delta}_{c,c-z}(\delta) = 0\}. \tag{6.7.18}$$

Let l be the characteristic of the residue field of S. Let $P_{(l)}$ be the l-primary subgroup of P (as in (6.7.13)).

We may identify the modules $e_{c,c-e}\Delta_{c,S}$ and $\Delta_{c-z,S}$, which are isomorphic as $\Delta_{c,S}$-modules; in particular the group P acts on $e_{c,c-e}\Delta_{c,S}$. As $e_{c,c-z}\Delta_{c,S}$ is a finite free $S[P]$-module, we have a decomposition of $S[P]$-modules where Δ_χ is the χ-isotypical component of $e_{c,c-z}\Delta_{c,S}$ (see (6.7.15))

$$e_{c,c-z}\Delta_{c,S} \cong \bigoplus_{\chi} \Delta(\chi)$$

and where $\chi : P_{(l)} \to \mathrm{GL}_n(S/(\pi))$ runs over the distinct irreducible representations of $P_{(l)}$ over $S/(\pi)$.

We obtain from (6.7.18) the decomposition

$$J_{c,z,S} = \bigoplus_{\chi} \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - g - h)$$

where the sum runs over all distinct irreducible characters $\chi : P_{(l)} \to \mathrm{GL}_n(S/(\pi))$ of $P_{(l)}$.

(4) Suppose that $z \in \mathrm{Supp}(c-z)$; then we have (see (5.3.5))

$$\epsilon(c,z) = t^{\Delta}_{c-z,c-2z}.$$

Hence we have an equality of $\Delta_{c,S}$-submodules

$$J_{c,z,S} = \{e_{c,c-z}\delta \mid \delta \in \Delta_{c,S},\ (a_z \otimes 1)t^{\Delta}_{c,c-z}(\delta) = 0,\ \text{and}\ t^{\Delta}_{c,c-2z}(\delta) = 0\}.$$

As the $\Delta_{c,S}$-modules $\Delta_{c-z,S}$ and $e_{c,c-z}\Delta_{c,S}$ are isomorphic, we then obtain the equality of submodules of $\Delta_{c,S}$

$$J_{c,z,S} = \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}I_{c,c-2z,S}.$$

where $I_{c,c-2z,S}$ is the kernel of the homomomorphism $t^{\Delta}_{c,c-2z,S}$. □

6.7.19. Corollary. *Suppose that the R-algebra S is a field of characteristic $l \geq 0$. Then the $\Delta_{c,S}$-submodule $J_{c,z,S}$ of $\Delta_{c,S}$ is given by the left column in the following table (the notation is that of table 6.7.16):*

(1) If z remains prime in K/F and is prime to $c-z$ then $J_{c,z,S}$ is:	
$e_{c,c-z}\Delta_{c,S}$	if $a_z \otimes 1 = 0$;
0	if $a_z \otimes 1 \neq 0$.
(2) If z is ramified in K/F and is prime to $c-z$ and $\mathfrak{m}'_z$ is the prime ideal of O_{c-z} lying above the ideal $\mathfrak{m}_z$ of A defining z then $J_{c,z,S}$ is:	
I_χ	where $\chi : P \to S^*$ is a rank 1 character such that $a_z \otimes 1 = \chi([[\mathfrak{m}'_z]])$;
0	if no such character exists.
(3) If z splits completely in K/F and is prime to $c-z$ where $\mathfrak{m}_z O_{c-z} = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals of O_{c-z}, and $h : P \to P_{(l)}$ is the projection homomorphism with kernel P_{l^∞} then $J_{c,z,S}$ is:	
$\bigoplus_\chi \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1})$	where χ runs over all irreducible representations $\chi : P_{(l)} \to \mathrm{GL}_n(S)$ such that $a_z \otimes 1 = \chi(h([[\mathfrak{p}_1]])^{-1}) + \chi(h([[\mathfrak{p}_2]])^{-1})$ and where $\Delta(\chi)$ is the χ-isotypical component of $e_{c,c-z}\Delta_{c,S}$;
0	if no such character χ exists.
(4) If $z \in \mathrm{Supp}(c-z)$ then $J_{c,z,S}$ is:	
$I_{c,c-2z,S}e_{c,c-z}\Delta_{c,S}$	if $a_z \otimes 1 = 0$ in S;
0	if $a_z \otimes 1 \neq 0$ in S.

Table 6.7.19: $J_{c,z,S}$ as a submodule of $\Delta_{c,S}$ when S is a field

Proof. We consider the 4 cases of the table above.
(1), (2), and (4). These cases follow immediately from theorem 6.7.16.
(3) The module $e_{c,c-z}\Delta_{c,S}$ is a direct sum of the χ-isotypical components $\Delta(\chi)$ (see (6.7.15) where χ runs over the irreducible representations of $P_{(l)}$. As $P_{(l)}$ is an abelian group of order prime to the characteristic of the field S, an irreducible representation χ of $P_{(l)}$ over S is a finite separable field extension $S(\chi)$ of the field S. Hence $\Delta(\chi)$ is a finite free $S(\chi)[P_{l^\infty}]$-module (see (6.7.15)). Hence the annihilator

$$\mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} + [[\mathfrak{p}_2]]^{-1})$$

is non-zero only if the element

$$a_z \otimes 1 - \chi(h([[\mathfrak{p}_1]]^{-1})) - \chi(h([[\mathfrak{p}_2]]^{-1}))$$

of the field $S(\chi)$ is equal to zero, where $h : P \to P_{(l)}$ is the projection homomorphism with kernel P_{l^∞}. This case now follows from theorem 6.7.16.□

6.7.20. Corollary. *Let $S \to S'$ be a homomorphism of R-algebras where S, S' are infinitesimal traits with residue characteristic l. Assume further that if z is split completely in K/F and z is prime to $c - z$ then the group P has order prime to l. Then there is an isomorphism of $\Delta_{c,S'}$-modules*

$$J_{c,z,S'} \cong J_{c,z,S} \otimes_S S'.$$

Proof. For any infinitesimal trait U and any element $u \in U$, there is an isomorphism of U-modules

$$\mathrm{Ann}_U(u) \cong \frac{U}{uU}.$$

It follows immediately from theorem 6.7.16 that if z satisfies one of the conditions (1), (2), or (4) of the table 6.7.16 then there is an isomorphism of $\Delta_{c,S'}$-modules $J_{c,z,S'} \cong J_{c,z,S} \otimes_S S'$.

Suppose that case (3) of the table 6.7.16 holds that is to say z is split completely in K/F and z is prime to $c - z$. By hypothesis, P has order prime to l. Let π be a local parameter of S. Let $a \in S[P]$ be the element

$$a = a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}.$$

By definition 6.7.3, the module $J_{c,z,S}$ is $\Delta_{c,S}$-isomorphic to

$$\mathrm{Ann}_{\Delta_{c-z,S}}(a).$$

The algebra $S[P]$ is finite and étale over S. Hence $S[P]$ is a direct product

$$S[P] = \prod_{i=1}^{m} S_i$$

where S_i is an infinitesimal trait with local parameter π for all i. The algebra $S[P] \otimes_S S'$ is a finite étale S'-algebra and hence is a direct product of a finite number of infinitesimal traits. Hence there is an isomorphism of $S[P] \otimes_S S'$-modules

$$\mathrm{Ann}_{S[P]}(a) \otimes_S S' \cong \mathrm{Ann}_{S[P]\otimes_S S'}(a \otimes 1)$$

where $a \otimes 1$ is the image of a in $S[P] \otimes_S S'$.

The algebra $\Delta_{c-z,S}$ is a finite free $S[P]$-algebra and we have an isomorphism of $\Delta_{c,S}$-modules, where $\Delta_{c,S}$ acts on the second factor of the tensor product,

$$J_{c,z,S} \cong \mathrm{Ann}_{\Delta_{c-z,S}}(a) \cong \mathrm{Ann}_{S[P]}(a) \otimes_{S[P]} \Delta_{c-z,S}.$$

It follows that we have an isomorphism of $\Delta_{c,S'}$-modules

$$J_{c,z,S'} \cong J_{c,z,S} \otimes_S S'. \quad \square$$

6.7.21 Lemma. *Let $S \to S'$ be a homomorphism of infinitesimal traits. Let $f : M \to N$ be a homomorphism of free S-modules of finite type. Then there is an isomorphism of S'-modules*

$$\ker\{f \otimes \mathrm{Id}_{S'} : M \otimes_S S' \to N \otimes_S S'\} \cong \ker\{f : M \to N\} \otimes_S S'.$$

Proof of lemma 6.7.21. The image $f(M)$ of f is an S-module of finite type and hence, as S is a quotient of a discrete valuation ring, there is an isomorphism of S-modules

$$f(M) \cong \bigoplus_{i=1}^{r} C_i$$

where C_i is a non-zero cyclic S-submodule of $f(M)$ for all i. Let $v_i \in f(M)$ be a generator of C_i for all $i = 1, \ldots, r$.

Select elements $m_1, \ldots, m_r \in M$ such that $f(m_i) = v_i$ for all i. Let κ be the residue field of S. Then f induces a homomophism of κ-vector spaces $M \otimes_S \kappa \to f(M) \otimes_S \kappa$ and the images of $v_1, \ldots, v_r$ form a basis of $f(M) \otimes_S \kappa$. Hence the images of $m_1, \ldots, m_r$ in $M \otimes_S \kappa$ are linearly independent. Hence we may find elements $m_{r+1}, \ldots, m_s \in M$ such that the images of $m_1, \ldots, m_s$ in $M \otimes_S \kappa$ form a basis of $M \otimes_S \kappa$. Nakayama's lemma implies that $m_1, \ldots, m_s$ generate M as an S-module. As M is a free S-module and the images of $m_1, \ldots, m_s$ in $M \otimes_S \kappa$ form a basis of $M \otimes_S \kappa$, it follows that $m_1, \ldots, m_s$ form a free basis of the S-module M.

Let M_1 be the submodule of M generated by $m_1, \ldots, m_r$. As $f(M) = f(M_1)$, it follows that for all $i = r+1, \ldots, s$ there are elements $n_i \in M_1$ such that $f(m_i - n_i) = 0$. The elements $m_1, \ldots, m_r, m_{r+1} - n_{r+1}, \ldots, m_s - n_s$ then form a free basis of M where $f(m_i - n_i) = 0$ for all $i = r+1, \ldots, s$; write this basis as $m'_1, \ldots, m'_s$. There is then a free basis $u_1, \ldots, u_t$ of N over S such that

$$f(m'_i) = \pi^{n_i} u_i, i = 1, \ldots, r.$$

We obtain that $f : M \to N$ is given by

$$f(m'_i) = \pi^{n_i} u_i, i = 1, \ldots, r, \text{ and } f(m'_i) = 0 \text{ for } i = r+1, \ldots s.$$

Hence we have

$$\ker(f) = \left(\bigoplus_{i=1}^{r} \mathrm{Ann}_S(\pi^{n_i}) \right) \oplus M_2$$

where M_2 is the submodule of M generated by $m'_{r+1}, \ldots, m'_s$. Furthermore we have that $f \otimes_S 1_{S'} : M \otimes_S S' \to N \otimes_S S'$ has kernel equal to

$$\ker(f \otimes_S 1_{S'}) = \left(\bigoplus_{i=1}^{r} \mathrm{Ann}_{S'}(\pi^{n_i}) \right) \oplus (M_2 \otimes_S S')$$

$$\cong \left(\bigoplus_{i=1}^{r} \frac{S'}{\pi^{n_i} S'} \right) \oplus (M_2 \otimes_S S')$$

$$\cong \left(\bigoplus_{i=1}^{r} \frac{S}{\pi^{n_i} S} \right) \otimes_S S' \oplus (M_2 \otimes_S S') \cong \ker(f) \otimes_S S'$$

as required.□

6.7.22. Proposition. *Suppose that the R-algebra S is an infinitesimal trait with local parameter π. Write J_m for $J_{c,z,S/(\pi^m)}$. For integers $0 \leq l \leq m$ there is an isomorphism of $\Delta_{c,S}$-modules*

$$J_l \cong (J_m)_{\pi^l}$$

and an isomorphism of S-modules

$$J_l \cong J_m \otimes S/(\pi^l).$$

6.7.23. Remark. The $\Delta_{c,S}$-modules J_l and $J_m \otimes_S S/(\pi^l)$ need not be isomorphic although they are S-isomorphic modules (see example 6.7.24 below).

Proof of proposition 6.7.22. We have the commutative diagram of $\Delta_{c,S}$-modules with exact columns

$$\begin{array}{ccccc}
\Delta_{\leq c-z,S/(\pi^l)} & \xrightarrow{\cong} & \pi^{m-l}\Delta_{\leq c-z,S/(\pi^m)} & \hookrightarrow & \Delta_{\leq c-z,S/(\pi^m)} \\
\uparrow & & \uparrow & & \uparrow \\
\Gamma_{c,c-z,S/(\pi^l)} & \xrightarrow{\cong} & \pi^{m-l}\Gamma_{c,c-z,S/(\pi^m)} & \hookrightarrow & \Gamma_{c,c-z,S/(\pi^m)} \\
\uparrow & & & & \uparrow \\
J_l & & & & J_m \\
\uparrow & & & & \uparrow \\
0 & & & & 0
\end{array}$$

It follows from this, as $\Gamma_{c,c-z,S}$ is a finite free S-module (lemma 6.2.2(i)), that we have an isomorphism of $\Delta_{c,S}$-modules

$$J_l \cong \{j \in J_m |\ \pi^l j = 0\}$$

which proves the first part of the lemma.

The $S/(\pi^m)$-modules

$$\Gamma_{c,c-z,S/(\pi^m)}, \quad \Delta_{\leq c-z,S/(\pi^m)}$$

are finite and free (lemma 6.2.2(i)). Let

$$\pi_\Gamma : \Gamma_{c,c-z,S/(\pi^m)} \to \Delta_{\leq c-z,S/(\pi^m)}$$

be the projection homomorphism (see (6.7.2)). From the previous lemma (lemma 6.7.21) we obtain an isomorphism of S-modules

$$\ker(\pi_\Gamma \otimes_S \mathrm{Id}_{S/(\pi^l)}) \cong \ker(\pi_\Gamma) \otimes_S S/(\pi^l).$$

As J_l is isomorphic to

$$\ker(\pi_\Gamma \otimes_S \mathrm{Id}_{S/(\pi^l)})$$

and $J_m \otimes_S S/(\pi^l)$ is isomorphic to

$$\ker(\pi_\Gamma) \otimes_S S/(\pi^l),$$

we obtain the isomorphism of S-modules

$$J_l \cong J_m \otimes_S S/(\pi^l)$$

as required.□

An example where $J_{c,z,S} \otimes \kappa$ and $J_{c,z,\kappa}$ are not isomorphic

The base change property of $J_{c,z,S}$ given by corollary 6.7.20 fails to hold in case (3) of table 6.7.16 if the order of the group P is not prime to the residue characteristic of the infinitesimal trait S. An example of this is given below.

6.7.24. Example. In case (3) of table 6.7.16, put $g = [[\mathfrak{p}_1]]^{-1}, h = [[\mathfrak{p}_2]]^{-1}$. Assume that

(1) the group P is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$;
(2) S is an infinitesimal trait with residue field κ of characteristic 2;
(3) $a_z \otimes 1 = 2$ and $4 \neq 0$ in S.

Then there are isomorphisms of $\Delta_{c,S}$-modules

$$J_{c,z,S} \otimes_S \kappa \cong \kappa[\mathrm{Pic}(O_{c-z})/P] \oplus \kappa[\mathrm{Pic}(O_{c-z})/P]$$

$$J_{c,z,\kappa} \cong ((g+h)\kappa[P]) \otimes_{\kappa[P]} \Delta_{c-z,\kappa}.$$

In particular, $J_{c,z,S} \otimes_S \kappa$ and $J_{c,z,\kappa}$ are not isomorphic $\Delta_{c,S}$-modules, as P acts trivially on $J_{c,z,S} \otimes_S \kappa$ but not on $J_{c,z,\kappa}$.

Proof of example 6.7.24. For the proof of this example, which takes several steps, we have an isomorphism of S-algebras, where g, h are the images in $S[P]$ of x, y respectively,

$$S[P] \cong S[x,y]/(x^2-1, y^2-1).$$

Here $S[x,y]$ is a free polynomial algebra in x, y over S. The elements $g = [[\mathfrak{p}_1]]^{-1}, h = [[\mathfrak{p}_2]]^{-1}$ both have order 2 and generate P. Let π be a local parameter of S.

Step 1. There is an isomorphism of $\Delta_{c,S}$-modules

$$J_{c,z,S} \cong \mathrm{Ann}_{S[P]}(2-g-h) \otimes_{S[P]} \Delta_{c-z,S}$$

where the sum runs over a set of coset representatives of P in $\mathrm{Pic}(O_{c-z})$.

The module $J_{c,z,S}$ is $\Delta_{c,S}$-isomorphic to the submodule of $\Delta_{c-z,S}$ given by (theorem 6.7.16)

$$\mathrm{Ann}_{\Delta_{c-z,S}}(2-g-h).$$

As the module $\Delta_{c-z,S}$ is a finite free $S[P]$-module the result follows immediately.

Step 2. Let C be the cyclic subgroup of P generated by g and let $S[C] \subset S[P]$ be the corresponding group subalgebra of $S[P]$. Let $q \in \mathrm{Ann}_{S[P]}(2-g-h)$. Then for some element $w \in S[C]$ we have

$$q = (g-h-2)w$$

and

$$4(g-1)w = 0.$$

Put $L = 2-x-y \in S[x,y]$. We select any lifting $Q \in S[x,y]$ of q. Then we have

$$LQ = (x^2-1)w_0(x,y) + (y^2-1)w_1(x,y)$$

where w_0, w_1 are elements of $S[x,y]$. As

$$S[x,y] = \bigoplus_{n=0}^{\infty} L^n S[x]$$

we may expand the polynomials w_i in powers of L with coefficients in $S[x]$. We may therefore select a lifting Q in $S[x,y]$ of q such that we have the equation in the algebra $S[x,y]$

$$LQ = (x^2-1)u(x) + (y^2-1)v(x).$$

where $u = u(x), v = v(x)$ are elements of $S[x]$.

We may write this equation as

$$LQ = (x^2-1)u + ((2-x-L)^2-1)v$$

$$= (x^2-1)u + ((2-x)^2-1)v + L(L+2x-4)v.$$

As $S[x,L] = S[x] \oplus LS[x,L]$, we may here equate of powers of L and obtain the equation in the algebra $S[x]$

$$0 = (x^2-1)u + ((2-x)^2-1)v$$

$$= (x^2-1)(u+v) + 4(1-x)v$$

and the equation in $S[x,y]$

$$LQ = L(L+2x-4)v.$$

As $L = (2-x-y)$ is not a zero divisor in $S[x,y]$, we obtain

$$Q = (x-y-2)v.$$

We then take w to be the image of v in $S[C]$ as required.

Step 3. We have the equality of S-submodules of $S[P]$

$$\mathrm{Ann}_{S[P]}(2-g-h) = (h+1)(g+1)S \oplus M$$

where

$$M = (h+2-g)\mathrm{Ann}_S(4).$$

Let $q \in \mathrm{Ann}_{S[P]}(2-g-h)$. By Step 2 above, there is a lifting $Q \in S[x,y]$ of q and elements $u, v \in S[x]$ such that

$$Q = (x-y-2)v \quad \text{and} \quad 4(x-1)v + (x^2-1)u = 0. \tag{6.7.25}$$

The second equation of (6.7.25) may be written

$$(x-1)(x+1)u = -4(x-1)v.$$

As $(x-1)$ is not a zero divisor of the ring $S[x]$ we obtain the equation

$$(x+1)u = -4v.$$

The element v satisfies this equation if and only if v is an element of the ideal of $S[x]$ given by

$$(x+1)S[x] + \mathrm{Ann}_S(4)S[x].$$

As $Q = (x-y-2)v$, we obtain that Q is an element of the ideal of $S[x,y]$ given by

$$(y+2-x)((x+1)S[x,y] + \mathrm{Ann}_S(4)S[x,y]).$$

That is to say, as q is any element of $\mathrm{Ann}_{S[P]}(2-g-h)$, we have

$$\mathrm{Ann}_{S[P]}(2-g-h) = (h+2-g)((g+1)S[P] + \mathrm{Ann}_S(4)S[P]).$$

We have in $S[P]$ the equations

$$(g+1)(h+2-g) = (h+1)(g+1) \tag{6.7.26}$$

$$(h+1)(h+2-g) = 4(1+h) - (h+1)(g+1).$$

From the decomposition of $S[P]$ as a sum of S-modules

$$S[P] = S \oplus S(g+1) \oplus S(h+1) \oplus S(g+1)(h+1)$$

we obtain the decomposition into S-submodules of $S[P]$

$$(h+2-g)\mathrm{Ann}_S(4)S[P] = (h+1)(g+1)\mathrm{Ann}_S(4) \oplus M$$

where

$$M = (h+2-g)\mathrm{Ann}_S(4).$$

We obtain the decomposition of the $S[P]$-module $\mathrm{Ann}_{S[P]}(2-g-h)$ as a sum of S-modules, as required,

$$\mathrm{Ann}_{S[P]}(2-g-h) = (h+1)(g+1)S \oplus M.$$

Step 4. There is an isomorphism of $\Delta_{c,S}$-modules

$$J_{c,z,\kappa} \cong \Big\{(h+g)\kappa[P]\Big\} \otimes_{\kappa[P]} \Delta_{c-z,\kappa}.$$

For we have an isomorphism of $\Delta_{c,S}$-modules, by Steps 1 and 3,

$$J_{c,z,S} \cong \Big\{(h+1)(g+1)S[P] + (h+2-g)\mathrm{Ann}_S(4)S[P]\Big\} \otimes_{S[P]} \Delta_{c-z,S}.$$

Hence we obtain isomorphisms of $\Delta_{c,S}$-modules, as the residue field κ has characteristic 2,

$$J_{c,z,\kappa} \cong \Big\{(h+g)\kappa[P]\Big\} \otimes_{\kappa[P]} \Delta_{c-z,\kappa}$$

as required.

Step 5. If $4 \neq 0$ in S then we have an isomorphism of $\Delta_{c,S}$-modules

$$J_{c,z,S} \otimes_S \kappa \cong \kappa[\mathrm{Pic}(O_{c-z})/P] \oplus \kappa[\mathrm{Pic}(O_{c-z})/P].$$

We obtain from Step 3 the decomposition of the $S[P]$-module $\mathrm{Ann}_{S[P]}(2-g-h)$ as a sum of S-modules

$$\mathrm{Ann}_{S[P]}(2-g-h) = (h+1)(g+1)S \oplus M$$

where

$$M = (h+2-g)\mathrm{Ann}_S(4).$$

It follows from the equations (6.7.26) that provided $4 \neq 0$ in S, and hence $\mathrm{Ann}_S(4)$ is contained in the maximal ideal πS, we have that g, h act on M such that

$$(g+1)M \subseteq (h+1)(g+1)\pi S$$

and

$$(h+1)M \subseteq (h+1)(g+1)\pi S.$$

It follows that provided $4 \neq 0$ in S, we have

$$\big\{(h+1)(g+1)S \oplus M\big\} \otimes_S \kappa = (h+1)(g+1)\kappa \oplus (M \otimes_S \kappa)$$

is a $\kappa[P]$-module on which P acts trivially on both components $(h+1)(g+1)\kappa$ and $M \otimes_S \kappa$ as κ has characteristic 2. We obtain that

$$\mathrm{Ann}_{S[P]}(2-g-h) \otimes_S \kappa$$

is isomorphic as a $\kappa[P]$-module to $\kappa \oplus \kappa$ on which the group P acts trivially.

From Step 1, we obtain isomorphisms of $\Delta_{c,S}$-modules provided $4 \neq 0$ in S

$$\begin{aligned} J_{c,z,S} \otimes_S \kappa &= \mathrm{Ann}_{S[P]}(2-g-h) \otimes_{S[P]} \Delta_{c-z,S} \otimes_S \kappa \\ &\cong \left\{\kappa \oplus \kappa\right\} \otimes_{\kappa[P]} \Delta_{c-z,\kappa} \\ &\cong \kappa[\mathrm{Pic}(O_{c-z})/P] \oplus \kappa[\mathrm{Pic}(O_{c-z})/P]. \end{aligned}$$

From this and Step 4, provided $4 \neq 0$ in S we have that $J_{c,z,S} \otimes_S \kappa$ and $J_{c,z,\kappa}$ are not isomorphic $\Delta_{c,S}$-modules.□

The case (3) of table 6.7.16 when S is an infinitesimal trait

In view of the previous example 6.7.24, we consider further this case where the order of P is not prime to the residue characteristic of S.

(6.7.27) Assume that case (3) of table 6.7.16 holds; that is to say z splits completely in K/F and is prime to $\mathrm{Supp}(c-z)$. Let P be the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by $[[\mathfrak{p}_1]]$ and $[[\mathfrak{p}_2]]$.

(6.7.28) As in (6.7.15), the group P decomposes as a direct product

$$P \cong P_{(l)} \times P_{l^\infty}$$

where $P_{(l)}$ is the p-primary subgroup of P and P_{l^∞} is the Sylow l-subgroup of P. The algebra $S[P]$ decomposes as

$$S[P] \cong S[P_{(l)}] \otimes_S S[P_{l^\infty}].$$

Then $S[P_{(l)}]$, as a module over itself, decomposes as (see (6.7.15))

$$S[P_{(l)}] \cong \bigoplus_\chi S(\chi)$$

where $S(\chi)$ is the χ-isotypical component of $S[P_{(l)}]$ and χ runs over all the distinct irreducible representations of $S/(\pi)[P_{(l)}]$ over the field $\kappa = S/(\pi)$.

The module $S[P_{(l)}]$ is a finite étale S-algebra where S is an infinitesimal trait. Hence the decomposition $S[P_{(l)}] \cong \bigoplus_\chi S(\chi)$ is also the decomposition of the algebra $S[P_{(l)}]$ as a product of étale local S-algebras $S(\chi)$. Each $S(\chi)$ is an infinitesimal trait with local parameter π and with residue field which is

a finite separable extension $\kappa(\chi)$ of κ. The irreducible representation χ over κ is then a group homomorphism

$$\chi : P_{(l)} \to \kappa(\chi)^*.$$

We obtain the decomposition of $S[P]$ as a module over itself

$$S[P] \cong \bigoplus_{\chi} S(\chi)[P_{l^\infty}] \tag{6.7.29}$$

where $S(\chi)[P_{l^\infty}]$ is the χ-isotypical component of $S[P]$.

(6.7.30) We write

$$g = [[\mathfrak{p}_1]]^{-1}, \quad h = [[\mathfrak{p}_2]]^{-1}.$$

Let $(g_l, g_{(l)}), (h_l, h_{(l)})$ be the components of g, h, respectively, under the decomposition $P \cong P_{l^\infty} \times P_{(l)}$, where $g_l, h_l \in P_{l^\infty}$ and $g_{(l)}, h_{(l)} \in P_{(l)}$. . Let l^r be the order of g_l in P_{l^∞} and let l^t be the order of h_l in P_{l^∞}. The group P_{l^∞} then lies in an exact sequence of finite abelian groups

$$\begin{array}{ccccccccc} 0 & \to & V & \to & \frac{\mathbb{Z}}{l^r\mathbb{Z}} \times \frac{\mathbb{Z}}{l^t\mathbb{Z}} & \to & P_{l^\infty} & \to & 0 \\ & & & & (1,0) & \mapsto & g_l & & \\ & & & & (0,1) & \mapsto & h_l. & & \end{array} \tag{6.7.31}$$

6.7.32. Lemma. *The group V is cyclic.*

Proof of lemma 6.7.32. Suppose that this is not true and that the l-group V is not cyclic.

Let $\mathbb{F}_l$ be the finite prime field with l elements. We apply $\mathrm{Hom}(\mathbb{F}_l, -)$, which is a left exact functor on the category of finite abelian groups, to the above exact sequence (6.7.31) defining the group V. We obtain the exact sequence of vector spaces over $\mathbb{F}_l$

$$0 \to \mathrm{Hom}(\mathbb{F}_l, V) \to \mathrm{Hom}(\mathbb{F}_l, \frac{\mathbb{Z}}{l^r\mathbb{Z}} \times \frac{\mathbb{Z}}{l^t\mathbb{Z}}) \to \mathrm{Hom}(\mathbb{F}_l, P).$$

As V is not cyclic we have that $\mathrm{Hom}(\mathbb{F}_l, V)$ is 2-dimensional vector space over $\mathbb{F}_l$. Hence $\mathrm{Hom}(\mathbb{F}_l, \frac{\mathbb{Z}}{l^r\mathbb{Z}} \times \frac{\mathbb{Z}}{l^t\mathbb{Z}})$ is also 2-dimensional and the map

$$\mathrm{Hom}(\mathbb{F}_l, V) \to \mathrm{Hom}(\mathbb{F}_l, \frac{\mathbb{Z}}{l^r\mathbb{Z}} \times \frac{\mathbb{Z}}{l^t\mathbb{Z}})$$

is an isomorphism. It follows that both r and t are ≥ 1 and the map $\mathrm{Hom}(\mathbb{F}_l, \frac{\mathbb{Z}}{l^r\mathbb{Z}} \times \frac{\mathbb{Z}}{l^t\mathbb{Z}}) \to \mathrm{Hom}(\mathbb{F}_l, P)$ is zero. Therefore g_l and h_l have orders l^{r-1} and l^{t-1} in P, respectively, which is a contradiction. □

(6.7.33) By the previous lemma 6.7.32, the group P_{l^∞} has a presentation of the form

$$g_l^{l^r} = 1, h_l^{l^t} = 1, g_l^{l^c} = h_l^{l^d}, g_l h_l = h_l g_l.$$

Furthermore, we have $r - c = t - d$ as $g_l^{l^c}$ has the same order as the element $h_l^{l^d}$.

Let $S(\chi)[x, y]$ denote the free polynomial algebra over $S(\chi)$ in the variables x, y. The algebra $S(\chi)[P_{l^\infty}]$ is then $S(\chi)$-isomorphic to the algebra

$$S(\chi)[x, y]/(x^{l^r} - 1, y^{l^t} - 1, x^{l^c} - y^{l^d})$$

where the integers r, t, c, d are independent of χ and depend only on the l-Sylow subgroup of P.

(6.7.34) The group P acts on the algebra $T = S(\chi)[P_{l^\infty}]$ as follows. Let 1_T be the multiplicative identity of $S(\chi)[P_{l^\infty}]$. The elements $g = (g_l, g_{(l)}), h = (h_l, h_{(l)})$ generate P. Let $\chi^\sharp : P_{(l)} \to S(\chi)^*$ be the homomorphism which is the unique lifting of the homomorphism $\chi : P_{(l)} \to \kappa(\chi)^*$ (proposition 6.7.7 and Hensel's lemma). As we have the decomposition $P \cong P_{l^\infty} \times P_{(l)}$ we may extend $\chi^\sharp$ to a group homomorphism, denoted by the same symbol,

$$\chi^\sharp : P \to S(\chi)^*$$

whose kernel contains P_{l^∞}. The elements g, h then act on $S(\chi)[P_{l^\infty}]$ as

$$g.1_T = \chi^\sharp(g) g_l, \quad h.1_T = \chi^\sharp(h) h_l.$$

(6.7.35) The module $\Delta_{c-z,S}$ is a finite free $S[P]$-module and $J_{c,z,S}$ is isomorphic to the submodule of $\Delta_{c-z,S}$ given by

$$J_{c,z,S} \cong \mathrm{Ann}_{\Delta_{c-z,S}}(a_z \otimes 1 - g - h).$$

We have the decomposition of $\Delta_{c-z,S}$-modules

$$\Delta_{c-z,S} \cong \bigoplus_\chi \Delta(\chi)$$

where χ runs over all irreducible representations of $P_{(l)}$ over κ and where $\Delta(\chi)$ is the χ-isotypical component of $\Delta_{c-z,S}$.

We have, as $\Delta_{c-z,S} \cong \bigoplus_\chi \Delta(\chi)$,

$$\mathrm{Ann}_{\Delta_{c-z,S}}(a_z \otimes 1 - g - h) = \bigoplus_\chi \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - g - h)$$

$$= \bigoplus_\chi \bigoplus_{w \in \mathrm{Pic}(O_{c-z})/P} w\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g - h)$$

where w runs over a set of coset representatives of P in $\mathrm{Pic}(O_{c-z})$.

(6.7.36) The element $a_z \otimes 1 - g - h$ may be written as

$$a_z \otimes 1 - \chi^\sharp(g) - \chi^\sharp(h) - (g - \chi^\sharp(g)) - (h - \chi^\sharp(h)).$$

As $g - \chi^\sharp(g), h - \chi^\sharp(h)$ act nilpotently on $\Delta(\chi)$ it follows that $a_z \otimes 1 - g - h$ is an invertible endomorphism of $\Delta(\chi)$ if and only if

$$a_z \otimes 1 - \chi^\sharp(g) - \chi^\sharp(h)$$

is an invertible element of $S(\chi)$.

As the action of g, h on $S(\chi)[P_{l^\infty}]$ is given in (6.7.34), we obtain

$$\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g - h) = \mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g_l\chi^\sharp(g) - h_l\chi^\sharp(h)).$$

6.7.37. Proposition. *We write*

$$g = [[\mathfrak{p}_1]]^{-1}, \quad h = [[\mathfrak{p}_2]]^{-1}.$$

Let C_l be the subgroup of P_{l^∞} generated by g_l. Let $S(\chi)[C_l]$ be the corresponding subalgebra of $S(\chi)[P_{l^\infty}]$. Put

$$\gamma = a_z\chi^\sharp(h^{-1}) - g_l\chi^\sharp(gh^{-1}).$$

The module $\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g - h)$ is the submodule of elements $q \in S(\chi)[P_{l^\infty}]$ such that

$$q = -\Big\{\sum_{i=0}^{l^t-1} h_l^{l^t-i-1}\gamma^i\Big\}u_1 + \Big\{\sum_{j=0}^{l^d-1} \gamma^{l^d-j-1}h_l^j\Big\}u_2 \tag{6.7.38}$$

where the polynomials $u_1, u_2 \in S(\chi)[C_l]$ satisfy the equation in the algebra $S(\chi)[C_l]$

$$0 = \big\{\gamma^{l^t} - 1\big\}u_1 + \big\{g_l^{l^c} - \gamma^{l^d}\big\}u_2. \tag{6.7.39}$$

Proof of proposition 6.7.37. By (6.7.36) we have

$$\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g - h) = \mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g_l\chi^\sharp(g) - h_l\chi^\sharp(h)).$$

Let $q \in \mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - g_l\chi^\sharp(g) - h_l\chi^\sharp(h))$. We select a lifting, denoted by Q, of q to $S(\chi)[x, y]$. Then we have

$$(a_z \otimes 1 - x\chi^\sharp(g) - y\chi^\sharp(h))Q = (x^{l^r} - 1)w_0 + (y^{l^t} - 1)w_1 + (x^{l^c} - y^{l^d})w_2$$

where w_0, w_1, w_2 are elements of $S(\chi)[x,y]$. As both $\chi^\sharp(g)$ and $\chi^\sharp(h)$ are invertible elements of $S(\chi)$, we may expand the polynomials w_i in powers of

$$L = (a_z \otimes 1 - x\chi^\sharp(g) - y\chi^\sharp(h))$$

with coefficients in $S(\chi)[x]$ namely

$$w_i(x,y) = w_{i,0}(x) + \sum_{j\geq 1} w_{i,j}(x)L^j, \quad \text{for } i = 0,1,2,$$

where $w_{i,j} \in S(\chi)[x]$ for all i,j. Substituting this in the equation for Q we obtain the equation

$$L(Q - Q_1) = (x^{l^r} - 1)w_{0,0}(x) + (y^{l^t} - 1)w_{1,0}(x) + (x^{l^c} - y^{l^d})w_{2,0}(x)$$

where

$$Q_1 = \sum_{j\geq 1} \Big\{ (x^{l^r} - 1)w_{0,j}(x) + (y^{l^t} - 1)w_{1,j}(x) + (x^{l^c} - y^{l^d})w_{2,j}(x) \Big\} L^{j-1}.$$

In particular Q_1 has image equal to zero in $S(\chi)[P_{l^\infty}]$. We may replace then Q by $Q - Q_1$ and we have

$$LQ(x,y) = (x^{l^r} - 1)w_{0,0}(x) + (y^{l^t} - 1)w_{1,0}(x) + (x^{l^c} - y^{l^d})w_{2,0}(x). \tag{6.7.40}$$

This equation holds in the free algebra $S(\chi)[x,y]$. We may then put

$$y = a_z\chi^\sharp(h^{-1}) - x\chi^\sharp(gh^{-1})$$

and we obtain the equation

$$0 = (x^{l^r} - 1)w_{0,0}(x) + (\delta^{l^t} - 1)w_{1,0}(x) + (x^{l^c} - \delta^{l^d})w_{2,0}(x) \tag{6.7.41}$$

where

$$\delta = a_z\chi^\sharp(h^{-1}) - x\chi^\sharp(gh^{-1}).$$

We use this to eliminate the term $(x^{l^r} - 1)w_{0,0}(x)$ in the equation (6.7.40) for Q and we obtain

$$LQ(x,y) = (y^{l^t} - \delta^{l^t})w_{1,0}(x) + (\delta^{l^d} - y^{l^d})w_{2,0}(x).$$

The right hand side of this equation clearly has

$$L = (a_z \otimes 1 - x\chi^\sharp(g) - y\chi^\sharp(h)) = \chi^\sharp(h)(\delta - y)$$

as a factor. The element L is non zero divisor on $S(\chi)[x,y]$; hence we may divide both sides of this equation by L. Let $u_1, u_2 \in S(\chi)[C_l]$ be the images of the elements $\chi^\sharp(h^{-1})w_{1,0}, \chi^\sharp(h^{-1})w_{2,0} \in S(\chi)[x]$ respectively where $\chi^\sharp(h^{-1})$ is a unit of $S(\chi)$. Let $\gamma \in S(\chi)[C_l]$ be the image of δ in $S(\chi)[C_l]$. This gives

the required form (6.7.38) of q subject to $w_{i,0}$, $i = 0, 1, 2$, satisfying the equation (6.7.41). The image of the equation (6.7.41) multiplied by $\chi^\sharp(h^{-1})$ in $S(\chi)[P_{l^\infty}]$ is precisely the equation (6.7.39) $\square$

The case (3) of table 6.7.16 when S is a field

(6.7.42) Assume that S is field of characteristic $l \geq 0$.

As in (6.7.28), let

$$\chi : P_{(l)} \to S(\chi)^*$$

be an irreducible representation of $P_{(l)}$ given by the finite separable field extension $S(\chi)$ of S. Let

$$\chi^\sharp : P \to S(\chi)^*$$

be the unique extension of χ to P where the kernel of $\chi^\sharp$ contains P_{l^∞}.

6.7.43. Proposition. *Under the hypotheses and notation of proposition 6.7.37, assume that S is a field and that*

$$a_z \otimes 1 = \chi^\sharp([[\mathfrak{p}_1]]^{-1}) + \chi^\sharp([[\mathfrak{p}_2]]^{-1}).$$

Assume that $r \geq t$. Then the module $\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1})$ *is equal to the ideal $< q_1^\chi, q_2^\chi > S(\chi)[P_{l^\infty}]$ generated by the two elements $q_1^\chi, q_2^\chi \in S(\chi)[P_{l^\infty}]$ of the form*

$$q_1^\chi = X^{l^r - l^t}(X+Y)^{l^t - 1}$$

$$q_2^\chi = -(X+Y)^{l^t-1}(X^{l^c-l^d}+1) + (X+Y)^{l^d-1}X^{l^t-l^d}$$

where

$$X = \chi^\sharp([[\mathfrak{p}_1]]^{-1})(g_l - 1),\ Y = \chi^\sharp([[\mathfrak{p}_2]]^{-1})(h_l - 1).$$

Proof. We write

$$g = [[\mathfrak{p}_1]]^{-1}, \quad h = [[\mathfrak{p}_2]]^{-1}.$$

As usual g_l, h_l denote the components of g, h in P_{l^∞}. From (6.7.33), we have an isomorphism of S-algebras

$$S(\chi)[P_{l^\infty}] \cong S(\chi)[x,y]/(x^{l^r} - 1, y^{l^t} - 1, x^{l^c} - y^{l^d})$$

$$g_l \mapsto x, \quad h_l \mapsto t.$$

We have, as in (6.7.34), that $a_z \otimes 1 - g - h$ acts on $S(\chi)[P_{l^\infty}]$ as

$$L = a_z \otimes 1 - g_l\chi^\sharp(g) - h_l\chi^\sharp(h).$$

Hence we have

$$\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}) = \mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(L).$$

If $a_z \otimes 1 - \chi^\sharp(g) - \chi^\sharp(h) \neq 0$ then L is a unit of the algebra $S(\chi)[P_{l^\infty}]$ and hence the annihilator of L is zero.

Assume then that

$$a_z \otimes 1 - \chi^\sharp(g) - \chi^\sharp(h) = 0.$$

Note if the characteristic l of the field S is stricly positive then we have $(-1)^{l^n} = -1$ for all $n \geq 0$. If the characteristic of S is zero then P_{l^∞} is the trivial group and hence $\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1})$ is equal to $S(\chi)$ and there is nothing further to prove; we now assume that $l > 0$.

We furthermore have

$$\chi^\sharp(g)^{l^c} = \chi^\sharp(h)^{l^d}.$$

We therefore change variables in the polynomial algebra $S(\chi)[x, y]$ and put

$$X = \chi^\sharp(g)(x-1), \quad Y = \chi^\sharp(h)(y-1).$$

We then have an isomorphism of S-algebras

$$S(\chi)[P_{l^\infty}] = S(\chi)[X, Y]/(X^{l^r}, Y^{l^t}, X^{l^c} - Y^{l^d}).$$

Furthermore as $a_z \otimes 1 - \chi^\sharp(g) - \chi^\sharp(h) = 0$, we have,

$$L = -(X + Y).$$

We therefore require to determine the annihilator of $X + Y$ on $S(\chi)[P_{l^\infty}]$. This is independent of the representation χ if the field $S(\chi)$ remains fixed; in particular, to determine $\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(L)$ we may reduce to the case where χ is the trivial representation and that $S = S(\chi)$.

We may apply proposition 6.7.37 to the infinitesimal trait $S(\chi)$ and the trivial representation. Hence $\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(L)$ is isomorphic to the module of all elements $q \in S(\chi)[P_{l^\infty}]$ satisfying the equations (6.7.38) and (6.7.39). Let Q be a lifting of q to $S(\chi)[x, y]$ and let $w_1, w_2 \in S(\chi)[x, y]$ be liftings to $S(\chi)[x]$ of $u_1, u_2 \in S(\chi)[C_l]$, where u_1, u_2 are as in proposition 6.7.37 and satisfy the equation (6.7.39).

The equation (6.7.38) lifted to $S(\chi)[x, y]$ becomes, as $S(\chi)$ is a field and χ is the trivial representation,

$$Q = -\Big(\sum_{i=0}^{l^t-1} y^{l^t-i-1}(2-x)^i\Big)w_1 + \Big(\sum_{j=0}^{l^d-1}(2-x)^{l^d-j-1}y^j\Big)w_2$$

where for some $w_0 \in S(\chi)[x]$ the elements $w_0, w_1, w_2 \in S(\chi)[x]$ satisfy the equation (see (6.7.41) and (6.7.39))

$$0 = (x^{l^r} - 1)w_0 + ((2-x)^{l^t} - 1)w_1 + (x^{l^c} - (2-x)^{l^d})w_2. \tag{6.7.44}$$

The equation for Q may be written

$$Q = -(y + x - 2)^{l^t - 1} w_1(x) + (2 - x - y)^{l^d - 1} w_2(x).$$

Under the change of variables $A = x - 1, B = y - 1$, this may be written as

$$Q = -(A + B)^{l^t - 1} w_1 + (A + B)^{l^d - 1} w_2. \tag{6.7.45}$$

As $S(\chi)$ is a field, the equation (6.7.44) then becomes

$$0 = (x-1)^{l^r} w_0 + (1-x)^{l^t} w_1 + (x^{l^c} - 2^{l^d} + x^{l^d})w_2. \tag{6.7.46}$$

This is equal to, where w_0, w_1, w_2 under the same change of variables $A = x - 1, B = y - 1$ are elements of $S(\chi)[A]$,

$$0 = A^{l^r} w_0 - A^{l^t} w_1 + (A^{l^c} + A^{l^d})w_2. \tag{6.7.47}$$

As $r - c = t - d$ and we have assumed that $r \geq t$ we then have $c \geq d$. Hence this equation may be written as

$$0 = A^{l^t}\big(A^{l^r - l^t} w_0 - w_1\big) + A^{l^d}\big(A^{l^c - l^d} + 1\big)w_2. \tag{6.7.48}$$

Hence we have that $A^{l^t - l^d}$ divides the polynomial w_2 in the unique factorisation domain $S(\chi)[A]$. We may then find $v_2 \in S(\chi)[A]$ such that

$$w_2 = A^{l^t - l^d} v_2.$$

Dividing the equation (6.7.48) by A^{l^t}, as A^{l^t} is not a zero divisor, we obtain

$$0 = \big(A^{l^r - l^t} w_0 - w_1\big) + \big(A^{l^c - l^d} + 1\big)v_2.$$

Rewriting this last equation for w_1 we obtain the equation

$$w_1 = A^{l^r - l^t} w_0 + \big(A^{l^c - l^d} + 1\big)v_2. \tag{6.7.49}$$

We use this to eliminate the term w_1 in the equation (6.7.45) for Q and obtain the equation

$$Q = -(A+B)^{l^t-1}\big(A^{l^r-l^t} w_0 + \big(A^{l^c-l^d} + 1\big)v_2\big) + (A+B)^{l^d-1} A^{l^t-l^d} v_2$$

$$= -(A+B)^{l^t-1} A^{l^r-l^t} w_0 + \big(-(A+B)^{l^t-1}(A^{l^c-l^d}+1) + (A+B)^{l^d-1} A^{l^t-l^d}\big)v_2.$$

We obtain that Q lies in the ideal of $S(\chi)[x,y]$ generated by the two polynomials

$$Q_1 = A^{l^r-l^t}(A+B)^{l^t-1}$$

and

$$Q_2 = -(A+B)^{l^t-1}(A^{l^c-l^d}+1)+(A+B)^{l^d-1}A^{l^t-l^d}.$$

If $q_1^\chi, q_2^\chi \in S(\chi)[P_{l^\infty}]$ denote the images of the polynomials Q_1, Q_2, respectively, we have shown that if $a_z \otimes 1 = \chi^\sharp(g)+\chi^\sharp(h)$ then we have

$$\mathrm{Ann}_{S(\chi)[P_{l^\infty}]}(a_z\otimes 1-g-h) =< q_1^\chi, q_2^\chi > S(\chi)[P_{l^\infty}]. \qquad \square$$

6.7.50. Corollary. *Under the hypotheses of proposition 6.7.43, the module* $\mathrm{Ann}_{\Delta_{c-z,S}}(a_z\otimes 1-[[\mathfrak{p}_1]]^{-1}-[[\mathfrak{p}_2]]^{-1})$ *is equal to*

$$\bigoplus_\chi \bigoplus_{w\in \mathrm{Pic}(O_{c-z})/P} w < q_1^\chi, q_2^\chi > S(\chi)[P_{l^\infty}]$$

where the sum over χ *runs over all irreducible representations* χ *of* $P_{(l)}$ *over the field* S *such that*

$$a_z\otimes 1 = \chi^\sharp([[\mathfrak{p}_1]]^{-1})+\chi^\sharp([[\mathfrak{p}_2]]^{-1}).$$

and where q_1^χ, q_2^χ *are the elements of* $S(\chi)[P_{l^\infty}]$ *given by proposition 6.7.43 for the representation* χ. $\square$

The case (3) of table 6.7.16 when P_{l^∞} *is trivial*

(6.7.51) Assume that S is an infinitesimal trait of residue characteristic $l \geq 0$ which is prime to the order of the group P. Let κ be the residue field of S and let π be a local parameter of S. By theorem 6.7.16 we have that $J_{c,z,S}$ is

$$\bigoplus_\chi \mathrm{Ann}_{\Delta(\chi)}(a_z\otimes 1-[[\mathfrak{p}_1]]^{-1}-[[\mathfrak{p}_2]]^{-1})$$

where the sum runs over all the irreducible representations $\chi : P \to \mathrm{GL}_n(\kappa)$ of P and where $\Delta(\chi)$ is the χ-isotypical component of $e_{c,c-z}\Delta_{c,S}$ (see (6.7.15)).

(6.7.52) By (6.7.28) we have that

$$S[P] \cong \bigoplus_\chi S(\chi)$$

where $S(\chi)$ is the χ-isotypical component of $S[P]$. The S-algebra $S(\chi)$ is an infinitesimal trait with the same local parameter as S and whose residue field

is a finite separable extension $\kappa(\chi)$ of the residue field κ of S. We then have for each irreducible representation χ a group homomorphism

$$\rho_\chi : P \to S(\chi)^*$$

and where χ is the reduction of ρ_χ modulo π.

As $\Delta(\chi)$ is a direct sum of copies of $S(\chi)$, we have that $a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}$ acts on $\Delta(\chi)$ by multiplication by the element of $S(\chi)$

$$a_z \otimes 1 - \rho_\chi([[\mathfrak{p}_1]])^{-1} - \rho_\chi([[\mathfrak{p}_2]])^{-1}.$$

Hence we have

$$\mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}) = \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - \rho_\chi([[\mathfrak{p}_1]])^{-1} - \rho_\chi([[\mathfrak{p}_2]])^{-1}).$$

As $S(\chi)$ is an infinitesimal trait we have an isomorphism of $S[P]$-modules

$$\mathrm{Ann}_{S(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}) \cong \frac{S(\chi)}{< a_z \otimes 1 - \rho_\chi([[\mathfrak{p}_1]])^{-1} - \rho_\chi([[\mathfrak{p}_2]])^{-1} >}.$$

We have

$$J_{c,z,S} = \bigoplus_\chi \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - \rho_\chi([[\mathfrak{p}_1]])^{-1} - \rho_\chi([[\mathfrak{p}_2]])^{-1})$$

where the sum runs over the irreducible representations $\chi : P \to \mathrm{GL}_n(\kappa)$ of P. It follows that we have an isomorphism of $\Delta_{c,S}$-modules

$$J_{c,z,S} \cong \bigoplus_\chi \bigoplus_{w \in \mathrm{Pic}(O_{c-z})/P} w \frac{S(\chi)}{< a_z \otimes 1 - \rho_\chi([[\mathfrak{p}_1]])^{-1} - \rho_\chi([[\mathfrak{p}_2]])^{-1} >}$$

where the sum $\bigoplus_{w \in \mathrm{Pic}(O_{c-z})/P}$ runs over a set of coset representatives of P in $\mathrm{Pic}(O_{c-z})$.

6.8 The kernel of Ξ

We consider the kernel of the surjective homomorphism Ξ given by (see proposition 6.6.3; the notation of §6.6 holds)

$$\Xi : \ker\{H^m(G,S) \otimes_R \Gamma_R \to H^m(G,S) \otimes_R \Delta_{\leq c-z,R}\} \xrightarrow{\Xi} \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))}.$$

The main result we obtain is proposition 6.8.10 which takes a particularly simple form in the case where $m = 1$ (see corollary 6.8.11).

(6.8.1) We assume throughout this section that

S is an R-algebra which is an infinitesimal trait with local parameter π;
n is the image in R of the integer $|B^*|/|A^*|$ and is assumed to be a multiplicative unit of R;
$c' \leq c$ are effective divisors on Spec A;
z is a prime divisor in the support of c where $z \notin \tilde{I}$;
$G = G(c/c-z)$.

We write $\exp(G)$ for the exponent of the finite abelian group G; that is to say, $\exp(G)$ is the least positive integer such that $\exp(G)G = 0$.

(6.8.2) By definition (see (6.7.3)), the $\Delta_{c,S}$-module $J_{c,z,S}$ is the kernel

$$J_{c,z,S} = \ker\{\pi_\Gamma : \Gamma_{c,c-z,S} \to \Delta_{\leq c-z,S}\}$$

where the homomorphism π_Γ is induced by the natural projection $\Delta_{\leq c,S} \to \Delta_{\leq c-z,S}$.

More generally, for any S-module M define the $\Delta_{c,S}$-module $J_{c,z,S}(M)$ to be the kernel

$$J_{c,z,S}(M) = \ker\{\pi_\Gamma \otimes \mathrm{Id}_M : \Gamma_{c,c-z,S} \otimes_S M \to \Delta_{\leq c-z,S} \otimes_S M\}.$$

Then $J_{c,z,S}(M)$ is a submodule of $\Delta_{c,S} \otimes_S M$ and $J_{c,z,S}(S)$ is isomorphic to $J_{c,z,S}$.

(6.8.3) Put for any prime divisor w in $\mathrm{Supp}(c)$

$$J^w_{c,z,S}(M) = \{\delta \in e_{c,c-z}\Delta_{c,S} \otimes_S M | \ \ e_{c,c-w}\delta \in J_{c,z,S}(M)\}.$$

Then we have for all w

$$J^w_{c,z,S}(M) \supseteq J_{c,z,S}(M) \supseteq e_{c,c-w}J^w_{c,z,S}(M).$$

6.8.4. Remarks. (i) The assignments $M \mapsto J_{c,z,S}(M)$ and $M \mapsto J^w_{c,z,S}(M)$ are left exact functors

$$J_{c,z,S}(-), J^w_{c,z,S}(-) : \quad S - \mathbf{mod} \longrightarrow \Delta_{c,S} - \mathbf{mod}$$

where T-**mod** denotes the category of T-modules for any commutative ring T. The functors $J_{c,z,S}(-)$ and $J^w_{c,z,S}(-)$ transform finite direct sums into finite direct sums.

(ii) Suppose that M is an S-module of finite type. As S is an infinitesimal trait, the module M is non-canonically isomorphic to a finite direct sum $\bigoplus_i S/(\pi^{n_i})$

of cyclic S-modules where integers n_i are uniquely determined by M, up to permutation. We then obtain a non-canonical isomorphism of $\Delta_{c,S}$-modules

$$J_{c,z,S}(M) \cong \bigoplus_i J_{c,z,S/(\pi^{n_i})}.$$

6.8.5. Definition. Let M be an S-module of finite type. We define the $\Delta_{c,S}$-modules

$$J(M) = \bigoplus_{c' \leq c,\ c' \not\leq c-z} J_{c',z,S}(M)$$

$$\Gamma_S = \bigoplus_{c' \leq c,\ c' \not\leq c-z} \Gamma_{c',c'-z,S}.$$

6.8.6. Lemma. (i) *The following sequence of $\Delta_{c,S}$-modules is exact*

$$0 \quad \to \quad J(M) \quad \stackrel{i}{\to} \quad \Gamma_S \otimes_S M \quad \to \quad \Delta_{\leq c-z,S} \otimes_S M$$

where the map i is the natural inclusion.
(ii) *For all prime divisors $w \in \mathrm{Supp}(c') \setminus \tilde{I}$ where $w \neq z$ we have*

$$K_{c',c'-w}(J^w_{c',z,S}) \subseteq J(S) \quad \text{for all} \quad c' \quad \text{such that } c \geq c' \geq w + z.$$

For all prime divisors $w \neq z$ we have

$$t^{\Delta}_w(J(M)) \subseteq J(M).$$

Proof. (i) This follows from the definitions.
(ii) The commutative diagram

$$\begin{array}{ccccc}
0 \to J(M) \to & \bigoplus\limits_{\substack{c' \leq c \\ c' \not\leq c-z}} \Gamma_{c',c'-z,S} \otimes_S M & \to & \bigoplus\limits_{\substack{c' \leq c \\ c' \not\leq c-z}} \Delta_{\leq c'-z,S} \otimes_S M \\
& \downarrow t^{\Delta}_w & & \downarrow t^{\Delta}_w \\
& \bigoplus\limits_{\substack{c' \leq c \\ c' \not\leq c-w-z}} \Gamma_{c'-w,c'-w-z,S} \otimes_S M & \to & \bigoplus\limits_{\substack{c' \leq c \\ c' \not\leq c-w-z}} \Delta_{\leq c'-w-z,S} \otimes_S M
\end{array}$$

shows that $t^{\Delta}_w(J(M)) \subseteq J(M)$.

As we have for all prime divisors $w \neq z$ (see (6.8.3))

$$J^w_{c',z,S}(M) \supseteq J_{c',z,S}(M) \supseteq e_{c',c'-w} J^w_{c',z,S}(M)$$

and we have the inclusion $t^{\Delta}_w(J(M)) \subseteq J(M)$, it follows from the definition of the K homomorphisms (see (5.3.5), (5.3.6)) that $K_{c',c'-w}(J^w_{c',z,S}) \subseteq J(S)$. □

6.8.7. Proposition. *The map Ξ coincides with the natural surjection*

$$\Xi : J(H^m(G,S)) \quad \to \quad \frac{H^{m-1}(G,\mathcal{H}_{c,S})}{t(H^{m-1}(G,\mathcal{H}_{c-z,S}))}.$$

Proof. From the definition of $J_{c,z,S}(M)$, we have the exact sequence of $\Delta_{c,S}$-modules for all $c' \leq c$ such that $c' \not\leq c - z$

$$0 \to J_{c',z,S}(H^m(G,S)) \to \Gamma_{c',c'-z} \otimes_R H^m(G,S) \to \Delta_{\leq c'-z,R} \otimes_R H^m(G,S).$$

Hence the module

$$\bigoplus_{c' \leq c,\ c' \not\leq c-z} \ker\{H^m(G,S) \otimes_R \Gamma_{c',c'-z} \to H^m(G,S) \otimes_R \Delta_{\leq c-z,R}\}$$

is $\Delta_{c,S}$-isomorphic to $J(H^m(G,S))$. Hence the domain of the homomorphism Ξ of proposition 6.6.3 is $\Delta_{c,S}$-isomorphic to $J(H^m(G,S))$. □

6.8.8. Definition. For any S-module M, define $J_\Gamma(M)$ to be the $\Delta_{c,S}$-submodule of $J(M)$ given by

$$J_\Gamma(M) = \sum_{\substack{c' \leq c \\ c' \not\leq c-z}} \sum_{\substack{w \in \mathrm{Supp}(c') \setminus \bar{I} \\ w \neq z}} K_{c',c'-w}(J^w_{c',z,S}(M)).$$

The sum here runs over all divisors $c' \in \mathrm{Div}_+(A)$ such that $c' \leq c$ and $c' \not\leq c-z$ and also runs over all prime divisors $w \in \mathrm{Supp}(c')$ such that $w \neq z$.

Let $L(S)$ be the submodule of $\Gamma_{\leq c,S}$ given by

$$L(S) = \sum_{\substack{c' \leq c \\ c' \not\leq c-z}} \sum_{\substack{w \in \mathrm{Supp}(c') \setminus \bar{I} \\ w \neq z}} e_{c',c'-z}\Gamma_{c',c'-w,S}.$$

In particular, the group G acts trivially on $L(S)$.

6.8.9. Remarks. (i) That $J_\Gamma(M)$ is a submodule of $J(M)$ follows from lemma 6.8.6(ii).
(ii) We have that $J_\Gamma(S)$ is the submodule of $\Gamma_{\leq c,S}$ given by

$$J_\Gamma(S) = \sum_{\substack{c' \leq c \\ c' \not\leq c-z}} \sum_{\substack{w \in \mathrm{Supp}(c') \setminus \bar{I} \\ w \neq z}} K_{c',c'-w}(J^w_{c',z,S}).$$

(iii) If M is a direct sum $M_1 \oplus M_2$ of two S-modules M_1, M_2 then we have an isomorphism of $\Delta_{c,S}$-modules

$$J_\Gamma(M) \cong J_\Gamma(M_1) \oplus J_\Gamma(M_2).$$

The following proposition and its corollary are proved in the next section §6.9.

6.8.10. Proposition. (i) *Let* $\exp(G)$ *be the exponent of the group* G. *Put* $S' = S/\exp(G)S$. *If* $m \geq 1$ *then we have the exact sequence of* $\Delta_{c,S}$*-modules*

$$0 \to \frac{M \cap \left\{\mathrm{Cocy}^m(G, J(S')\right\}}{\mathrm{Cob}^m(G, J(S'))} \to J(H^m(G,S)) \xrightarrow{\Xi} \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))} \to 0$$

where

$$M = \mathrm{Cocy}^m(G, L(S')) + \mathrm{Cob}^m(G, \Gamma_{S'} + \Gamma_{\leq c-z,S'}).$$

(ii) *The group* $J_\Gamma(H^m(G,S))$ *lies in* $\ker(\Xi)$. □

6.8.11. Corollary. *Put* $S' = S/\exp(G)S$. *The following sequence of* $\Delta_{c,S}$*-modules is exact*

$$0 \longrightarrow H^1(G, L(S') \cap J(S')) \longrightarrow J(H^1(G,S)) \xrightarrow{\Xi} \frac{H^0(G, \mathcal{H}_{c,S})}{t(H^0(G, \mathcal{H}_{c-z,S}))} \longrightarrow 0. \quad \square$$

6.9 Proofs

In this section, the hypotheses of (6.8.1) hold and we shall prove proposition 6.8.10 and corollary 6.8.11. We write G for the galois group $G(c/c-z)$ and $\exp(G)$ for the exponent of the abelian group G.

(6.9.1) Let M be a $R[G]$-module. For any subgroup H of G, denote by

$$\{\mathrm{Coch}^m(H, M), \partial^m\}$$

the standard complex of inhomogeneous cochains (see (5.6.5) et seq. for more details). Denote also by

$\mathrm{Cocy}^m(H, M)$ the subgroup of $\mathrm{Coch}^m(H, M)$ of m-cocycles;
$\mathrm{Cob}^m(H, M)$ the subgroup of $\mathrm{Coch}^m(H, M)$ of m-coboundaries.

(6.9.2) From proposition 6.8.7 we have the surjective homomorphism for all $m \geq 1$

$$J(H^m(G,S)) \xrightarrow{\Xi} \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))} \tag{6.9.3}$$

where $J(H^m(G,S))$ is a submodule of $H^m(G,S)\otimes_S \Gamma_S$ where we put

$$\Gamma_S = \bigoplus_{c'\leq c, c'\not\leq c-z} \Gamma_{c',c'-z,S}. \tag{6.9.4}$$

6.9.5. Lemma. *Let T be a principal ideal domain and $r\geq 1$ be an integer. Let $\mathcal{G}_r(T)$ be the category of finite abelian groups J such that the homology groups $H_i(J,T)$ are finite free T/rT-modules for all $i\geq 1$ and where J acts trivially on T. Then we have:*
(i) *$\mathcal{G}_r(T)$ contains the cyclic groups of order r.*
(ii) *$\mathcal{G}_r(T)$ is stable under finite direct products of its objects.*

Proof. Let T be a principal ideal domain. If J is a finite abelian group which acts trivially on T, we write $H_n(J)$ for the group homology $H_n(J,T)$ of J with coefficients in T. If J, J' are finite abelian groups acting trivially on T, the Kunneth formula [BRO1, p.120] for group homology takes the form of a split short exact sequence

$$0\to \bigoplus_{p+q=n} H_p(J)\otimes_T H_q(J')\to H_n(J\times J')\to \bigoplus_{p+q=n-1} \mathrm{Tor}_1^T(H_p(J),H_q(J'))\to 0. \tag{6.9.6}$$

(i) Let $r\geq 1$ be an integer. Let $\mathcal{G}_r(T)$ be the category of finite abelian groups J such that the homology groups $H_i(J)$ are finite free T/rT-modules for all $i\geq 1$ and where J acts trivially on T. Here, we consider 0 to be a free T/rT-module.

If J is a finite cyclic group of order r then we have

$$H_i(J)\cong \begin{cases} T/rT & \text{if } i \text{ is odd} \\ T_r & \text{if } i\geq 2 \text{ is even.}\end{cases}$$

Here T_r is the submodule of T annihilated by r. As T is a domain, T_r is zero if the integer r is prime to the characteristic of the field of fractions of T and is equal to T otherwise. It follows that $H_i(J)$ is a finite free T/rT-module of rank ≤ 1 for all integers $i\geq 1$. Hence J belongs to the category $\mathcal{G}_r(T)$.
(ii) Suppose that J, and J' are groups which are objects of the category $\mathcal{G}_r(T)$. Then for all $n\geq 1$ the module

$$\bigoplus_{p+q=n} H_p(J)\otimes_T H_q(J')$$

is a finite free T/rT-module.

Put

$$M_n = \bigoplus_{p+q=n-1} \mathrm{Tor}_1^T(H_p(J),H_q(J')).$$

Suppose first that r is divisible by the characteristic of the field of fractions of T; then $H_p(J)$, $H_q(J')$ are free T-modules for all p, q and hence

$$\mathrm{Tor}_1^T(H_p(J), H_q(J')) = 0$$

for all p, q. Hence M_n is a finite free T/rT-module for all $n \geq 1$ in this case.

Suppose then that r is not divisible by the characteristic of the field of fractions of T. If either p or q is zero then at least one of $H_p(J)$ and $H_q(J')$ is a free T-module and hence

$$\mathrm{Tor}_1^T(H_p(J), H_q(J')) = 0.$$

If both p and q are non-zero then both $H_p(J)$ and $H_q(J')$ are finite free T/rT-modules; hence the short exact sequence

$$0 \ \rightarrow \ T \xrightarrow{r} T \rightarrow \ T/rT \ \rightarrow \ 0$$

tensored with $H_q(J')$ shows that

$$\mathrm{Tor}_1^T(T/rT, H_q(J')) \ = \ \ker(H_q(J') \xrightarrow{r} H_q(J')) \ \cong \ H_q(J')$$

and hence this group $\mathrm{Tor}_1^T(H_p(J), H_q(J'))$ is a finite free T/rT-module for all $p \geq 1$ and $q \geq 1$; hence M_n is a finite free T/rT-module for all $n \geq 1$ in this case.

In conclusion, we have shown that M_n is a finite free T/rT-module for all $n \geq 1$. It now follows from the Kunneth formula (6.9.6) that $H_n(J \times J')$ is also a finite free T/rT-module for all $n \geq 1$. Hence the direct product $J \times J'$ is an object of $\mathcal{G}_r(T)$. By induction, we obtain that the category $\mathcal{G}_r(T)$ of groups is stable under finite direct products of its objects.□

6.9.7. Lemma. (i) *The abelian group G is a finite direct sum of copies of $\mathbb{Z}/\exp(G)\mathbb{Z}$.*
(ii) *Put $S' = S/\exp(G)S$. For all $m \geq 1$, the cohomology group $H^m(G, S)$ is a finite free S'-module.*
(iii) *If S is a quotient of a discrete valuation ring T then for $m \geq 1$ the rank of the free S'-module $H^m(G, S)$ depends only on m, G, and T.*

Proof. (i) This is a restatement of (2.3.12)(c).
(ii) and (iii). The ring S is asssumed to be an infinitesimal trait. Hence S is a homomorphic image of a discrete valuation ring T, say. Let J be a finite abelian group which acts trivially on T. Write $H_n(J)$ for the group homology $H_n(J, T)$ of J with coefficients in T. For any T-module M where J acts trivially on M, the universal coefficient theorem for group cohomology $H^n(J, M)$ [BRO1, pp.7-8] then takes the form of a split short exact sequence of T-modules

$$(6.9.8) \ 0 \ \rightarrow \ \mathrm{Ext}_T^1(H_{n-1}(J), M) \ \rightarrow \ H^n(J, M) \ \rightarrow \ \mathrm{Hom}_T(H_n(J), M) \ \rightarrow \ 0.$$

The abelian group $G = G(c/c-z)$ is a direct sum of cyclic groups of the same order $r \geq 1$ by part (i). Hence G is an object of the category $\mathcal{G}_r(T)$ by lemma 6.9.5 that is to say, the module $H_n(G,T)$ is a finite free T/rT-module for all $n \geq 1$. Hence

$$\mathrm{Hom}_T(H_n(G,T),S)$$

is a finite free S/rS-module if $n \geq 1$.

Suppose first that either $n = 1$ or that r is divisible by the characteristic of the field of fractions of T. Then the group

$$\mathrm{Ext}^1_T(H_{n-1}(G,T),S)$$

is zero as $H_{n-1}(G,T)$ is a finite free T-module in this case.

Suppose now that $n \geq 2$ and that r is prime to the characteristic of the field of fractions of T. Then $H_{n-1}(G,T)$ is a finite free T/rT-module and hence has a free resolution of the form

$$0 \quad \to \quad F_0 \quad \stackrel{r}{\to} \quad F_0 \quad \to \quad H_{n-1}(G,T) \quad \to \quad 0$$

where F_0 is a finite free T-module. Applying the functor $\mathrm{Hom}_T(-,S)$ to this sequence we obtain the complex

$$0 \to \mathrm{Hom}_T(H_{n-1}(G,T),S) \to \mathrm{Hom}_T(F_0,S) \stackrel{r}{\to} \mathrm{Hom}_T(F_0,S) \to 0$$

whose cohomology gives $\mathrm{Ext}^i_T(H_{n-1}(G,T),S)$ for all $i \geq 0$. As $\mathrm{Hom}_T(F_0,S)$ is a finite free S-module, we have that $\mathrm{Ext}^1_T(H_{n-1}(G,T),S)$ is a finite free S/rS-module in this case.

In conclusion we have that $\mathrm{Ext}^1_T(H_{n-1}(G,T),S)$ and $\mathrm{Hom}_T(H_n(G,T),S)$ are finite free S/rS-modules for all $n \geq 1$ of ranks depending only on n, G, T. The universal coefficient theorem (see (6.9.8)) now shows that $H^n(G,S)$ is a finite free S/rS-module for all $n \geq 1$, where $r = \exp(G)$, and of rank depending only on n, G, T as required. □

6.9.9. Lemma. *Put $S' = S/\exp(G)S$. Then there are isomorphisms of $\Delta_{c,S}$-modules*

$$J(H^m(G,S)) \cong \begin{cases} H^m(G, J(S')) & \text{if } m \geq 1 \\ J(S) & \text{if } m = 0 \end{cases}$$

$$J_\Gamma(H^m(G,S)) \cong \begin{cases} H^m(G, J_\Gamma(S')) & \text{if } m \geq 1 \\ J_\Gamma(S) & \text{if } m = 0. \end{cases}$$

Proof. As $H^0(G,S) \cong S$ the result is obvious if $m = 0$.

Suppose now that $m \geq 1$. By lemma 6.9.7 the group $H^m(G,S)$ is a finite

free S'-module for all $m \geq 1$. It follows (remarks 6.8.4(i) and (ii), remark 6.8.9(iii)) that there are isomorphisms of $\Delta_{c,S}$-modules for $m \geq 1$

$$J(H^m(G,S)) \cong J(S') \otimes_S H^m(G,S)$$

$$J_\Gamma(H^m(G,S)) \cong J_\Gamma(S') \otimes_S H^m(G,S).$$

The group G acts trivially on $J(S')$ and $J_\Gamma(S')$. As S is an infinitesimal trait, the universal coefficient theorem (see (6.9.8)) now shows that there are isomorphisms of S-modules

$$J(S') \otimes_S H^m(G,S) \cong H^m(G, J(S'))$$

$$J_\Gamma(S') \otimes_S H^m(G,S) \cong H^m(G, J_\Gamma(S'))$$

which are compatible with the action on the right of the ring $\Delta_{c,S}$; hence these maps are isomorphisms of $\Delta_{c,S}$-modules.□

6.9.10. Lemma. *Put $S' = S/\exp(G)S$. For $m \geq 1$, an element $\alpha \in J(H^m(G,S))$ of the kernel of Ξ is represented by a cocycle in $\mathrm{Cocy}^m(G, J(S'))$ of the form*

$$j = \partial^{m-1}\eta$$

where

$$j \in \mathrm{Cocy}^m(G, J(S'))$$

and where

$$\eta \in \mathrm{Coch}^{m-1}(G, \Gamma_{\leq c,S'}).$$

Proof. Suppose that $m \geq 1$. Note first that from (6.9.3) and lemma 6.9.9 it follows that there is a surjective homomorphism of $\Delta_{c,S}$-modules

$$H^m(G, J(S')) \xrightarrow{\Xi} \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))}.$$

The modules $\Gamma_{\leq c,S}, \Delta_{\leq c,S}$ are finite flat S-modules (corollary 5.9.6). Furthermore, from corollary 5.9.5, we have an isomorphism of $\Delta_{c,S}$-modules

$$\mathcal{H}_{c,S} \otimes_S S' \cong \mathcal{H}_{c,S'}.$$

It follows from this and the standard presentation of the Heegner module $\mathcal{H}_{c,S}$

$$0 \to \Gamma_{\leq c,S} \to \Delta_{\leq c,S} \to \mathcal{H}_{c,S} \to 0$$

that there are isomorphisms of $\Delta_{c,S}$-modules

$$\Gamma_{\leq c,S} \otimes_S S' \cong \Gamma_{\leq c,S'}$$

and

$$\Delta_{\leq c,S} \otimes_S S' \cong \Delta_{\leq c,S'}.$$

From lemma 6.9.7 (or the universal coefficient theorem [BRO1, p.8]), there are isomorphisms of S-modules

$$H^m(G,S) \cong H^m(G,S')$$

and there are isomorphisms of $\Delta_{c,S}$-modules by the universal coefficient theorem

$$H^m(G,\Gamma_{\leq c,S}) \cong H^m(G,\Gamma_{\leq c,S'})$$

and

$$H^m(G,\Delta_{\leq c,S}) \cong H^m(G,\Delta_{\leq c,S'}).$$

By lemma 6.2.15, proposition 6.6.3 and (6.9.3), we may then construct a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 \to & \dfrac{H^{m-1}(G,\mathcal{H}_{c,S})}{t(H^{m-1}(G,\mathcal{H}_{c-z,S}))} & \to & H^m(G,\Gamma_{\leq c,S'}) & \xrightarrow{f} & H^m(G,\Delta_{\leq c,S'}) \\
& \Xi \uparrow & & i \uparrow & & \cong \uparrow \\
0 \to & H^m(G,J(S')) & \to & H^m(G,S') \otimes_S \Gamma_{S'} & \to & H^m(G,S') \otimes_S \Delta_{\leq c-z,S'}
\end{array}$$

where the vertical arrow i is induced from the inclusion $\Gamma_{S'} \subseteq \Gamma_{\leq c,S'}$.

We have the exact sequence

$$0 \to \mathrm{Cob}^m(G,J(S')) \to \mathrm{Cocy}^m(G,J(S')) \to H^m(G,J(S')) \to 0.$$

Hence an element $\alpha \in J(H^m(G,S)) \cong H^m(G,J(S'))$ (lemma 6.9.9) is represented by a cocycle j in $\mathrm{Cocy}^m(G,J(S'))$. The result now follows from the above commutative diagram.□

(6.9.11) We recall from (5.7.3) that if E is a finite saturated subset of $\mathrm{Div}_+(A)$ then $\Gamma(E)_S$ denotes the module

$$\Gamma(E)_S = \sum_{c' \in E} \sum_w K_{c',c'-w}(\Delta_{c',S})$$

where the sum runs over all $c' \in E$ and over all prime divisors $w \notin \tilde{I}$ such that $w \in \mathrm{Supp}(c')$.

(6.9.12) As in definition 6.8.8, let $L(S)$ be the subset of $\Gamma_{\leq c,S}$ given by

$$L(S) = \sum_{c' \leq c,\ c' \not\leq c-z} \sum_{\substack{w \in \mathrm{Supp}(c') \setminus \tilde{I} \\ w \neq z}} e_{c',c'-z} \Gamma_{c',c'-w,S}.$$

6.9.13. Lemma. *Let j be a cocycle such that*

$$j \in \mathrm{Cocy}^m(G, (\Delta_{\leq c,S})^G).$$

Let E be a saturated subset of $\mathrm{Div}_+(A)$, all elements of which are $\leq c$. Assume that there is an equality of cochains in $\mathrm{Coch}^m(G, \Delta_{\leq c,S})$

$$j = \partial^{m-1}\eta$$

where

$$\eta \in \mathrm{Coch}^{m-1}(G, \Gamma(E)_S).$$

Let d be a maximal element of E (that is to say $e \geq d$ and $e \in E$ implies $e = d$) such that $d \not\leq c - z$. Then we have

$$j = \zeta + \partial^{m-1}(\eta_1 + \eta_2)$$

where

$$\zeta \in \mathrm{Cocy}^m(G, S) \otimes_S L(S)$$
$$\eta_1 \in \mathrm{Coch}^{m-1}(G, \Gamma_{d,d-z,S})$$
$$\eta_2 \in \mathrm{Coch}^{m-1}(G, \Gamma(E \setminus \{d\})_S).$$

Proof of lemma 6.9.13. This proof is similar to that of lemma 6.5.3. Let j be a cocycle in $\mathrm{Cocy}^m(G, (\Delta_{\leq c,S})^G)$ such that for some saturated set E of effective divisors, all of which are $\leq c$,

$$j = \partial^{m-1}\eta$$

where

$$\eta \in \mathrm{Coch}^{m-1}(G, \Gamma(E)_S).$$

Assume that d is a maximal element of E such that $d \not\leq c - z$. The proof occupies several stages.

Stage 1. Derivation of the equation $j_d = -\sum_i \frac{|O^*_{d-z_i}|}{|A^*|} e_{d,d-z_i}\partial^{m-1}(\eta_i)$

The m-cocycle j takes the form

$$j = \bigoplus_{c' \le c} j_{c'}$$

where

$$g \;\mapsto\; j(g) = \big(\partial^{m-1} \sum_{d' \in E} \sum_{w \in \mathrm{Supp}(d') \setminus \tilde{I}} K_{d',d'-w}(\eta_{d',w})\big)(g) \tag{6.9.14}$$

and where $\eta_{d',w} \in \mathrm{Coch}^{m-1}(G, \Delta_{d',S})$ for all d' and prime divisors w and the cocycle $j_{c'}$ lies in $\mathrm{Cocy}^m(G, (\Delta_{c',S})^G)$ for all c'.

Let d be the chosen maximal element of the finite saturated set E where $d \not\leq c - z$, as stated in the lemma. The sum $\sum_{d' \in E}$ in (6.9.14) can be written in the form

$$j(g) = \big(\partial^{m-1} \sum_{w \in \mathrm{Supp}(d) \setminus \tilde{I}} \gamma_{d,d-w}\big)(g) + \partial^{m-1}(\gamma)(g) \quad \text{for all } g \in G \tag{6.9.15}$$

where

$$\partial^{m-1}\gamma = \sum_{c' \in E \setminus \{d\}} \sum_{w \in \mathrm{Supp}(c') \setminus \tilde{I}} \partial^{m-1}\gamma_{c',c'-w}$$

and

$$\gamma \in \mathrm{Coch}^{m-1}(G, \Gamma(E \setminus \{d\})_S) \tag{6.9.16}$$

$$\gamma_{d,d-w} = K_{d,d-w}(\eta_{d,w}) \in \mathrm{Coch}^{m-1}(G, \Gamma_{d,d-w,S}) \quad \text{for all } w$$

where w runs over the finite set of prime divisors in $\mathrm{Supp}(d) \setminus \tilde{I}$. As we have

$$\gamma_{d,d-z} \in \mathrm{Coch}^{m-1}(G, \Gamma_{d,d-z,S})$$

by taking the difference $j - \partial^{m-1}\gamma_{d,d-z}$ we may reduce to the case where $\partial^{m-1}\gamma_{d,d-z} = 0$.

We may then write the equation (6.9.15) in the form

$$j = \sum_{i=2}^{n} \partial^{m-1}\gamma_{d,d-z_i} + \partial^{m-1}\gamma \tag{6.9.17}$$

where $z_1, \ldots, z_n$ are the distinct prime divisors in $\mathrm{Supp}(d) \setminus \tilde{I}$ and where $z_1 = z$ and

$$\gamma_{d,d-w} \in \mathrm{Coch}^{m-1}(G, \Gamma_{d,d-w,S}) \quad \text{for all } w.$$

The definition of the K homomorphisms is the following equation (see (5.3.6))

$$K_{f,f-w}(\delta) = (a_w - \epsilon(f,w))t^{\Delta}_{f,f-w}(\delta) - \frac{|O^*_{f-w}|}{|A^*|}e_{f,f-w}\delta.$$

The component of $\gamma_{f,f-w}(g)$ in $\Delta_{d,S}$ is therefore zero if the divisor f is not equal to d, $d+w$ or $d+2w$ (by the definition of $K_{f,f-w}$); the component of $\gamma_{d,d-z_i}(g)$ in $\Delta_{d,S}$ is then equal to (see (6.9.16))

$$-\frac{|O^*_{d-z_i}|}{|A^*|}e_i\eta_{d,z_i}(g).$$

where we write

$$e_i = e_{d,d-z_i} = \sum_{g\in G_i} g$$

and

$$G_i = \ker(t_{d,d-z_i}) = G(d/d-z_i), \quad \text{for all } i.$$

The maximality of d implies that d, $d+w$ and $d+2w$ do not lie in the set $E\setminus\{d\}$ for all prime divisors w. Hence for the sum, for all $g\in G^m$,

$$\partial^{m-1}(\gamma)(g) = \sum_{c'\in E\setminus\{d\}} \sum_{w\in \mathrm{Supp}(c')\setminus\tilde{I}} \partial^{m-1}(\gamma_{c',c'-w})(g)$$

the component in $\Delta_{d,S}$ is equal to zero.

The component in $\Delta_{d,S}$ of the right hand side of the equation (6.9.17) is then the component in $\Delta_{d,S}$ of the sum

$$\sum_{i=2}^{n} \partial^{m-1}(\gamma_{d,d-z_i})(g)$$

for all $g\in G^m$. The cochains $\partial^{m-1}\gamma_{d,d-z_i}$ are of the form

$$g \mapsto K_{d,d-z_i}(\partial^{m-1}(\eta_{d,z_i})(g)),\ G^m \to \Gamma_{d,d-z_i,S},$$

for some cochains

$$\eta_i = \eta_{d,z_i} \ \in\ \mathrm{Coch}^{m-1}(G,\Delta_{d,S}).$$

Hence the component of this equation (6.9.17) in $\Delta_{d,S}$ is the equation

$$j_d(g) = -\sum_{i=2}^{n} \frac{|O^*_{d-z_i}|}{|A^*|}e_i\partial^{m-1}(\eta_i)(g) \quad \text{for all } g\in G^m \tag{6.9.18}$$

where $j_d(g)$ is the component in $\Delta_{d,S}$ of $j(g)$.

Stage 2. Formulae for the η_i.

We have $j_d(g) \in (\Delta_{d,S})^G = e_1\Delta_{d,S}$ for all $g \in G^m$, as $d \not\leq c - z$. Hence the equation (6.9.18) takes the form

$$e_1\eta = -\sum_{i=2}^{n} \frac{|O^*_{d-z_i}|}{|A^*|} e_i \partial^{m-1}(\eta_i)$$

where $g \mapsto j_d(g)$ is a cocycle $g \mapsto e_1\eta(g)$ and $\eta \in \mathrm{Coch}^m(G, \Delta_{d,S})$.

By proposition 5.8.4, $\{G_i\}_{i=1,\ldots,n}$ forms an R-admissible family of subgroups of $\mathrm{Pic}(O_d)$, where $G_i = G(d/d - z_i)$ for all i. Let e_{ik} be the elements of $\Delta_{d,S}$, where $\Delta_{d,S}$ is the group algebra $S[\mathrm{Pic}(O_d)]$, given by

$$e_{ik} = \sum_{g \in G_i G_k} g \quad \text{for all } i \neq k.$$

By proposition 5.6.29, there are cochains

$$u^{(i,k)} \in \mathrm{Coch}^{m-1}(G, \Delta_{d,S}) \quad \text{for all } i \neq k \text{ and } 1 \leq i, k \leq n$$

such that

$$u^{(i,k)} = -u^{(k,i)}, \quad \text{for all } i \neq k,$$

and a finite set M and there are cocycles $f_{ir} \in \mathrm{Cocy}^m(G, S)$, for all $i \geq 2$ and all $r \in M$, and elements

$$\theta_{ir} \in e_{1i}\Delta_{d,S} \quad \text{for all } i \geq 2 \text{ and all } r \in M$$

and a coboundary

$$e_1\partial^{m-1}(\epsilon) \in \mathrm{Cob}^m(G, e_1\Delta_{d,S}),$$

where $\epsilon \in \mathrm{Coch}^{m-1}(G, \Delta_{d,S})$, such that

(6.9.19)

$$\frac{|O^*_{d-z_i}|}{|A^*|}\partial^{m-1}(e_i\eta_i) = \sum_{r \in M} f_{ir} \otimes \theta_{ir} + \sum_{\substack{k \neq i \\ 1 \leq k \leq n}} e_{ik}\partial^{m-1}u^{(i,k)} \quad \text{for all } i \geq 2$$

$$0 = e_1\partial^{m-1}(\epsilon) + \sum_{k \neq 1} e_{1k}\partial^{m-1}u^{(1,k)}$$

where

$$e_1\eta = -e_1\partial^{m-1}(\epsilon) - \sum_{i \geq 2} \sum_{r \in M} f_{ir} \otimes \theta_{ir}.$$

As $\theta_{ir} \in e_1e_i\Delta_{d,S}$ we may write θ_{ir} as

$$\theta_{ir} = e_1e_i\Theta_{ir}, \quad \text{for all } i \geq 2 \text{ and all } r \in M,$$

where

$$\Theta_{ir} \in \Delta_{d,S}.$$

Hence we may write the equations (6.9.19) as

(6.9.20)
$$\frac{|O^*_{d-z_i}|}{|A^*|}e_i\partial^{m-1}(\eta_i) = \sum_{r\in M} f_{ir}\otimes e_1e_i\Theta_{ir} + \sum_{\substack{k\neq i\\ 1\leq k\leq n}} e_{ik}\partial^{m-1}u^{(i,k)}, \quad \text{for all } i\geq 2,$$

$$0 = e_1\partial^{m-1}(\epsilon) + \sum_{k\neq 1} e_{1k}\partial^{m-1}u^{(1,k)}.$$

Stage 3. The formula $\sum_i \partial^{m-1}\gamma_{d,d-z_i}$; the case where $n = 1$.

The equation (6.9.17) becomes when $n = 1$

$$j = \partial^{m-1}(\gamma).$$

As the term $\partial^{m-1}(\gamma)$ is a coboundary in $\mathrm{Cob}^m(G, \Gamma(E\setminus\{d\})$ this completes the proof of the lemma 6.9.13 in this case where $n = 1$.

Stage 4. The formula $\sum_i \partial^{m-1}\gamma_{d,d-z_i}$; the case where $n \geq 2$.

The divisor d is not prime, as it has at least two prime divisors in its support by hypothesis. The equations (6.9.20) become

(6.9.21)
$$e_i\partial^{m-1}(\eta_i) = \sum_{r\in M} f_{ir}\otimes e_1e_i\Theta_{ir} + \sum_{\substack{k\neq i\\ 1\leq k\leq n}} e_{ik}\partial^{m-1}u^{(i,k)}, \quad \text{for all } i\geq 2,$$

$$0 = e_1\partial^{m-1}(\epsilon) + \sum_{k\neq 1} e_{1k}\partial^{m-1}u^{(1,k)}.$$

From lemma 5.10.1, these equations (6.9.21) then give the equation

(6.9.22)
$$N\left\{\sum_{i=2}^{n} K_{d,d-z_i}(\partial^{m-1}(\eta_i)) - K_{d,d-z_1}(\partial^{m-1}(\epsilon)) - \sum_{i=2}^{n}\sum_{r\in M} f_{ir}\otimes K_{d,d-z_i}(e_1\Theta_{ir})\right\}$$

$$= -\sum_{i=1}^{n}\sum_{1\leq k\leq n, k\neq i} (a_{z_i} - \epsilon(d,z_i))K_{d-z_i,d-z_i-z_k}(t^{\Delta}_{d,d-z_i}(\partial^{m-1}u^{(i,k)}))$$

where

$$N = \frac{|O^*_{d-z_1-z_2}|}{|A^*|}$$

and where we have that $N = 1$ unless $n = 2$ and $d = z_1 + z_2$; in particular, N is a unit in R, by the hypotheses (6.8.1).

We obtain from (6.9.15) and (6.9.17)

$$j = \sum_{i=2}^{n} \partial^{m-1}\gamma_{d,d-z_i} + \partial^{m-1}\gamma$$

where

$$\gamma \in \mathrm{Coch}^{m-1}(G, \Gamma(E \setminus \{d\})_S).$$

We then obtain from (6.9.22), as $\gamma_{d,d-z_i} = K_{d,d-z_i}(\eta_i)$ for all i,

$$j = K_{d,d-z_1}(\partial^{m-1}(\epsilon)) + \sum_{i=2}^{n} \sum_{r \in M} f_{ir} \otimes K_{d,d-z_i}(e_1 \Theta_{ir})$$

$$-\frac{1}{N} \sum_{i=1}^{n} \sum_{\substack{k=1 \\ k \neq i}}^{k=n} (a_{z_i} - \epsilon(d, z_i)) K_{d-z_i, d-z_i-z_k}(t^{\Delta}_{d,d-z_i}(\partial^{m-1} u^{(i,k)})) + \partial^{m-1}\gamma.$$

We may write this formula as

$$j = \partial^{m-1} K_{d,d-z_1}(\epsilon) + e_1 \sum_{i=2}^{n} \sum_{r \in M} f_{ir} \otimes K_{d,d-z_i}(\Theta_{ir}) + \partial^{m-1}\delta + \partial^{m-1}\gamma$$

where

$$\delta = -\frac{1}{N} \sum_{i=1}^{n} \sum_{\substack{k=1 \\ k \neq i}}^{k=n} (a_{z_i} - \epsilon(d, z_i)) K_{d-z_i, d-z_i-z_k}(t^{\Delta}_{d,d-z_i}(u^{(i,k)})) \tag{6.9.23}$$

and

$$\partial^{m-1}\delta \in \mathrm{Cob}^m(G, \Gamma(E \setminus \{d\})_S). \tag{6.9.24}$$

As $\partial^{m-1} K_{d,d-z_1}(\epsilon)$ is a coboundary in $\mathrm{Cob}^m(G, \Gamma_{d,d-z_1})$ and as $e_1 \sum_{i=2}^{n} \sum_{r \in M} f_{ir} \otimes K_{d,d-z_i}(\Theta_{ir})$ is an element of $\mathrm{Cocy}^m(G, S) \otimes_S L(S)$, we may now put

$$\zeta = e_1 \sum_{i=2}^{n} \sum_{r \in M} f_{ir} \otimes K_{d,d-z_i}(\Theta_{ir})$$

$$\eta_1 = K_{d,d-z_1}(\epsilon)$$

$$\eta_2 = \delta + \gamma.$$

This completes the proof. □

6.9.25. Remarks. (i) The module $L(S)$ is a finite flat S-module on which G acts trivially. In particular, there is an isomorphism of $\Delta_{c,S}$-modules

$$\mathrm{Cocy}^m(G, S) \otimes_S L(S) \cong \mathrm{Cocy}^m(G, L(S)).$$

[For the proof, it is evident that $L(S)$ is a finite S-module. It is only required to show that $L(S)$ is a flat S-module. Put

$$M = \sum_{\substack{c' \leq c \\ c' \not\leq c-z}} \sum_{\substack{w \neq z \\ w \in \mathrm{Supp}(c') \setminus \bar{I}}} \Gamma_{c', c'-w, S}.$$

We have an equality of $\Delta_{c,S}$-submodules of $\Delta_{\leq c,S}$

$$L(S) = e_{c,c-z}M.$$

Taking the exceptional set of primes in the definition of $\Gamma_{\leq c-z,S}$ to be $\tilde{I} \cup \{z\}$ instead of $\tilde{I}$, we have an isomorphism of $\Delta_{c,S}$-modules

$$\Gamma_{\leq c-z,S} \cong \bigoplus_{n=0}^{m-1} e_{c,c-(n+1)z}M$$

where $m \geq 1$ is the greatest integer such that $c - mz \geq 0$. As $\Gamma_{\leq c-z,S}$, for the exceptional set $\tilde{I} \cup \{z\}$, is a flat S-module (corollary 5.9.6), it follows that $e_{c,c-z}M$ is S-flat. Hence $L(S)$ is a flat S-module.]

(ii) That $\mathrm{Cocy}^m(G, L(S))$ lies in $\mathrm{Cob}^m(G, \Gamma_{\leq c,S})$ follows from the existence of Kolyvagin elements (§5.6, definition 5.6.12).

6.9.26. Lemma. *If $m \geq 1$, the submodule $J_\Gamma(H^m(G,S))$ of $J(H^m(G,S))$ lies in the kernel of Ξ.*

Proof. Assume that $m \geq 1$. Put

$$S' = S/\exp(G)S.$$

There is an inclusion of S-modules $J_\Gamma(H^m(G,S)) \subseteq J(H^m(G,S))$ (remark 6.8.9(i)). Hence we obtain a commutative diagram of S-modules

$$\begin{array}{ccc} & & \Gamma_{S'} \otimes_S H^m(G,S) \\ & & \uparrow \\ J(H^m(G,S)) & \cong & J(S') \otimes_S H^m(G,S) \\ \uparrow & & \uparrow \\ J_\Gamma(H^m(G,S)) & \cong & J_\Gamma(S') \otimes_S H^m(G,S) \end{array}$$

It follows from the above diagram that the arrow

$$J_\Gamma(S') \otimes_S H^m(G,S) \to J(S') \otimes_S H^m(G,S)$$

of this diagram is an injection obtained from tensoring the inclusion $J_\Gamma(S') \subseteq J(S')$ with $H^m(G,S)$. The isomorphisms of this diagram

$$J(H^m(G,S)) \cong J(S') \otimes_S H^m(G,S)$$

$$J_\Gamma(H^m(G,S)) \cong J_\Gamma(S') \otimes_S H^m(G,S)$$

follow from $H^m(G,S)$ being a finite free S'-module (lemma 6.9.7) and from remarks 6.8.4(i) and (ii) and remark 6.8.9(ii).

As $H^m(G,S) \cong H^m(G,S')$ for $m \geq 1$ by the universal coefficient theorem or lemma 6.9.7, we may tensor the exact sequence

$$0 \quad \to \quad \mathrm{Cob}^m(G,S') \quad \to \quad \mathrm{Cocy}^m(G,S') \quad \to \quad H^m(G,S) \quad \to \quad 0$$

with $J_\Gamma(S')$ and obtain the exact sequence

$$J_\Gamma(S') \otimes_S \mathrm{Cob}^m(G,S') \to J_\Gamma(S') \otimes_S \mathrm{Cocy}^m(G,S') \to J_\Gamma(S') \otimes_S H^m(G,S) \to 0.$$

Hence an element of $J_\Gamma(S') \otimes_S H^m(G,S)$ is represented by a cocycle in

$$J_\Gamma(S') \otimes_S \mathrm{Cocy}^m(G,S').$$

Let

$$E : \mathrm{Cocy}^m(G,S') \to \mathrm{Coch}^{m-1}(G, S'[G])$$

be the Kolyvagin map (see (5.6.10) and proposition 5.6.12) such that the following diagram is commutative

$$\begin{array}{ccc} \mathrm{Cocy}^m(G,S') & \stackrel{E}{\to} & \mathrm{Coch}^{m-1}(G,S'[G]) \\ & \searrow & \downarrow \partial^{m-1} \\ & & \mathrm{Cocy}^m(G,S'[G]) \end{array}$$

where the diagonal arrow is induced from the map

$$S' \to S'[G], \quad s \mapsto s e_{c,c-z}.$$

That is to say, we have for all $f \in \mathrm{Cocy}^m(G,S')$

$$(\partial^{m-1} E_f)(g) = f(g) e_{c,c-z} \quad \text{for all } g \in G^m.$$

As we have inclusions of $\Delta_{c,S}$-modules (see (6.8.3))

$$J^w_{c,z,S}(S') \subseteq e_{c,c-z} \Delta_{c,S'}$$

it follows that

$$K_{c,c-w}(J^w_{c,z,S}(S')) \subseteq e_{c,c-z} \Gamma_{c,c-w,S'}.$$

Hence we obtain

$$J_\Gamma(S') = \sum_{\substack{c' \leq c \\ \text{such that } c' \not\leq c-z}} \sum_{w \neq z \atop w \in \mathrm{Supp}(c') \setminus \tilde{I}} K_{c',c'-w}(J^w_{c',z,S}(S')) \subseteq e_{c,c-z} \Gamma_{\leq c,S'}.$$

it follows that there is a $\Delta_{c,S}$-submodule M of $\Gamma_{\leq c,S'}$ which contains $J_\Gamma(S')$ and such that

$$J_\Gamma(S') = e_{c,c-z} M.$$

We may then form this commutative diagram where E is the Kolyvagin map (see (5.6.10) and proposition 5.6.12)

$$
\begin{array}{ccc}
\mathrm{Cocy}^m(G,S')\otimes_S M & & \\
E\otimes \mathrm{Id}\downarrow & \searrow^{\phi} & \\
\mathrm{Coch}^{m-1}(G,S'[G])\otimes_S M & & \mathrm{Cocy}^m(G,S')\otimes_S J_\Gamma(S') \\
\partial^{m-1}\otimes \mathrm{Id}\downarrow & \swarrow_{\chi} & \\
\mathrm{Coch}^m(G,S'[G])\otimes_S M & & \\
\psi\downarrow & & \\
\mathrm{Coch}^m(G,\Gamma_{\leq c,S'}) & &
\end{array}
$$

where the top diagonal arrow

$$\phi : \mathrm{Cocy}^m(G,S')\otimes_S M \to \mathrm{Cocy}^m(G,S')\otimes_S J_\Gamma(S')$$

is $\mathrm{Id}\otimes e_{c,c-z}$, that is to say multiplication by $e_{c,c-z}$ on the second component and is therefore a surjective homomorphism. The diagonal arrow

$$\chi : \mathrm{Cocy}^m(G,S')\otimes_S J_\Gamma(S') \to \mathrm{Coch}^m(G,S'[G])\otimes_S M$$

is $i\otimes j$ where i is the inclusion map $\mathrm{Cocy}^m(G,S') \to \mathrm{Coch}^m(G,S'[G])$, $s\mapsto se_{c,c-z}$, and j is the inclusion map $J_\Gamma(S')\subseteq M$.

The map

$$\psi : \mathrm{Coch}^m(G,S'[G])\otimes_S M \to \mathrm{Coch}^m(G,\Gamma_{\leq c,S'})$$

is obtained by the composition

$$
\begin{array}{ccccc}
S'[G]\otimes_S M & \to & M & \subseteq & \Gamma_{\leq c,S'} \\
x\otimes m & \mapsto & xm & &
\end{array}
$$

As the map ϕ is surjective, this commutative diagram shows that the image in $\mathrm{Coch}^m(G,\Gamma_{\leq c,S'})$ of $\mathrm{Cocy}^m(G,S')\otimes_S J_\Gamma(S')$ lies in the coboundaries $\mathrm{Cob}^m(G,\Gamma_{\leq c,S'})$ where we have from lemma 6.2.15 the diagram with an exact top row

$$
0\to \quad \frac{H^{m-1}(G,\mathcal{H}_{c,S})}{t(H^{m-1}(G,\mathcal{H}_{c-z,S}))} \quad \to \quad H^m(G,\Gamma_{\leq c,S'}) \quad \stackrel{f}{\to} \quad H^m(G,\Delta_{\leq c,S'})
$$
$$
\uparrow \Xi
$$
$$
J(H^m(G,S))
$$

Hence we have that $J_\Gamma(S')\otimes_S H^m(G,S)$ lies in the kernel of Ξ. $\square$

We now prove proposition 6.8.10 and corollary 6.8.11 of the previous section.

Proof of proposition 6.8.10

Part (ii) of this proposition follows from the previous lemma 6.9.26.

For the proof of part (i), put $S' = S/\exp(G)S$ and let E be the saturated subset of divisors

$$E = \{c' \mid c' \leq c, c' \in \mathrm{Div}_+(A)\}.$$

Let $\alpha \in \ker(\Xi)$ where we assume the integer m is ≥ 1. By lemma 6.9.10, for $m \geq 1$, the element $\alpha \in J(H^m(G,S))$ of the kernel of Ξ is represented by a cocycle in $\mathrm{Cocy}^m(G, J(S'))$ of the form

$$j = \partial^{m-1}\eta$$

where

$$j \in \mathrm{Cocy}^m(G, J(S'))$$

and where

$$\eta \in \mathrm{Coch}^{m-1}(G, \Gamma_{\leq c,S'}).$$

We have $j \in \mathrm{Cocy}^m(G, (\Delta_{\leq c,S'})^G)$ as $J(S') = \bigoplus_{c' \leq c, c' \not\leq c-z} J_{c',z,S'}$ and G acts trivially on $J_{c',z,S'}$ for all $c' \leq c$.

Put $E_0 = E$ and $E_1 = E_0 \setminus \{c\}$. From lemma 6.9.13, we have that α can be represented by a cochain of the form

$$j = \zeta_1 + \partial^{m-1}(\eta_1 + \theta_1)$$

where

$$\zeta_1 \in \mathrm{Cocy}^m(G, S') \otimes_S L(S')$$
$$\eta_1 \in \mathrm{Coch}^{m-1}(G, \Gamma_{c,c-z,S'})$$
$$\theta_1 \in \mathrm{Coch}^{m-1}(G, \Gamma(E_0 \setminus \{c\})_{S'}).$$

Using lemma 6.9.13, we may construct inductively finite sequences $E_i, \zeta_i, \eta_i, \theta_i$ for $i = 1, 2, \ldots$ where

(i) E_i are saturated subsets of E forming a strictly decreasing sequence

$$E_0 \supset E_1 \supset \ldots \supset E_n \supset \ldots$$

such that $E_i \setminus E_{i+1} = \{d_i\}$ where $d_i \not\leq c - z$ and d_i is a maximal element of E_i.

(ii) ζ_i are cocycles in $\mathrm{Cocy}^m(G, S') \otimes_S L(S')$ for all i;

(iii) $\eta_i \in \mathrm{Coch}^{m-1}(G, \Gamma_{S'})$

(iv) $\theta_i \in \mathrm{Coch}^{m-1}(G, \Gamma(E_i)_{S'})$.

(v) $j = \zeta_i + \partial^{m-1}(\eta_i + \theta_i)$.

The sequence $\{E_i\}_i$ of subsets of the finite set E is finite and terminates with a set E_n all of whose elements are $\leq c - z$. Hence we have that the sequence $\{\theta_i\}_i$ terminates with $\theta_n \in \mathrm{Coch}^{m-1}(G, \Gamma_{\leq c-z,S'})$. Hence we have

$$j = \zeta_n + \partial^{m-1}(\eta_n + \theta_n)$$

where

$$\zeta_n \in \mathrm{Cocy}^m(G, S') \otimes_S L(S')$$
$$\eta_n \in \mathrm{Coch}^{m-1}(G, \Gamma_{S'})$$
$$\theta_n \in \mathrm{Coch}^{m-1}(G, \Gamma_{\leq c-z,S'}).$$

As $L(S')$ is a finite flat S'-module on which G acts trivially, we have an isomorphism of $\Delta_{c,S}$-modules (remark 6.9.25(i))

$$\mathrm{Cocy}^m(G, S') \otimes_S L(S') \cong \mathrm{Cocy}^m(G, L(S')).$$

Hence we have that j lies in the module of cocycles

$$M \cap \mathrm{Cocy}^m(G, J(S'))$$

where

$$M = \mathrm{Cocy}^m(G, L(S')) + \mathrm{Cob}^m(G, \Gamma_{S'}) + \mathrm{Cob}^m(G, \Gamma_{\leq c-z,S'}).$$

The submodule of coboundaries $\mathrm{Cob}^m(G, J(S'))$ lies in both $\mathrm{Cocy}^m(G, J(S'))$ and $\mathrm{Cob}^m(G, \Gamma_{S'})$. Hence $\mathrm{Cob}^m(G, J(S'))$ is a submodule of $M \cap \mathrm{Cocy}^m(G, J(S'))$. The map Ξ fits into a diagram (lemma 6.9.9 and (6.9.3))

$$H^m(G, J(S')) \;\cong\; J(H^m(G, S)) \xrightarrow{\Xi} \frac{H^{m-1}(G, \mathcal{H}_{c,S})}{t(H^{m-1}(G, \mathcal{H}_{c-z,S}))}.$$

We then have that the kernel of Ξ is isomorphic to the quotient

$$\frac{M \cap \{\mathrm{Cocy}^m(G, J(S'))\}}{\mathrm{Cob}^m(G, J(S'))}$$

as required.□

Proof of corollary 6.8.11

Put $S' = S/\exp(G)S$. We have for any R-module U on which G acts trivially $\mathrm{Cob}^1(G, U) = 0$. Hence the module M of proposition 6.8.10 given by

$$M = \mathrm{Cocy}^1(G, L(S')) + \mathrm{Cob}^1(G, \Gamma_{S'} + \Gamma_{\leq c-z,S'})$$

is equal to $\mathrm{Cocy}^1(G, L(S'))$ and we have $\mathrm{Cob}^1(G, J(S')) = 0$. Hence the quotient

$$\frac{M \cap \mathrm{Cocy}^1(G, J(S'))}{\mathrm{Cob}^1(G, J(S'))}$$

is isomorphic to $H^1(G, L(S') \cap J(S'))$. The corollary now follows immediately from proposition 6.8.10. □

6.10 Galois invariants of the Heegner module: S is an infinitesimal trait

Write G for the galois group $G(c/c-z)$ and assume that S is an infinitesimal trait. The main result of this and the next section is theorem 6.10.7 which determines, under hypotheses, the isomorphism class of the $\Delta_{c,S}$-module

$$\frac{H^0(G, \mathcal{H}_{c,S})}{t(H^0(G, \mathcal{H}_{c-z,S}))}.$$

In the case when S is the infinitesimal trait $\mathbb{Z}/l^n\mathbb{Z}$, this is applied to the cohomology of elliptic curves in chapter 7.

(6.10.1) We assume throughout this section that

S is an infinitesimal trait which is an R-algebra; for an element $a \in R$ we write $a \otimes 1$ for its image in the R-algebra S;
n is the image in R of the integer $|B^*|/|A^*|$ and is assumed to be a multiplicative unit of R;
$c' \leq c$ are effective divisors on Spec A;
z is a prime divisor in the support of c where $z \notin \tilde{I}$;
$\rho : \Sigma_F \setminus \tilde{I} \to R$, $v \mapsto a_v$, is a map of sets;
$\mathcal{H}(\rho)_S = \varinjlim \mathcal{H}_{c,S}$ is the Heegner module attached to ρ, K/F, with exceptional set $\tilde{I}$ and with coefficients in S.

We shall use the notation of §6.7, more precisely that of theorem 6.7.16; a summary of this notation is given in (6.10.2)-(6.10.6) below.

(6.10.2) As in (6.7.9), let $\mathfrak{p}_i$, $i = 1, \ldots, m$ where $m \leq 2$, be the prime ideals of the order O_{c-z} of K lying over the prime ideal $\mathfrak{m}_z$ of A corresponding to z. When z is disjoint from the support of $c - z$, let $[[\mathfrak{p}_i]]$ denote the divisor class of $\mathrm{Pic}(O_{c-z})$ defined by the fractionary ideal $\mathfrak{p}_i$ of O_{c-z} (as in (4.6.2)).

Let P be the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the classes $[[\mathfrak{p}_i]]$, $i = 1, \ldots, m$, when $z \notin \mathrm{Supp}(c - z)$.

(6.10.3) If z is ramified in K/F and $z \notin \mathrm{Supp}(c-z)$ then there is a unique prime ideal $\mathfrak{m}'_z$ of O_{c-z} lying above the prime ideal $\mathfrak{m}_z$ of A. In this case P is the cyclic group generated by the element

$$[[\mathfrak{m}'_z]] \ \in \ \mathrm{Pic}(O_{c-z}).$$

Let L be an ideal of S. Let χ be a character of P with values in S/L; that is to say χ is a group homomorphism

$$\chi : P \to (S/L)^*.$$

Let I_χ be the submodule of $e_{c,c-z}\mathrm{Ann}_S(L)\Delta_{c,S}$ on which P acts as χ^{-1} (see (6.7.10) for further details).

(6.10.4) Suppose that $z \notin \mathrm{Supp}(c-z)$ and z is split completely in K/F. Then there are two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of O_{c-z} lying above the prime ideal $\mathfrak{m}_z$ of A. In this case P is the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the two elements $[[\mathfrak{p}_1]], [[\mathfrak{p}_2]]$.

Assume that the order of the group P is prime to the residue characteristic of S. Then for any $S[P]$-module M of finite type we have the decomposition into isotypical components

$$M = \bigoplus_\chi M(\chi)$$

where the sum runs over the irreducible representations $\chi : P \to \mathrm{GL}_n(\kappa)$ of P where κ is the residue field of S.

In particular, we have the decomposition

$$S[P] \cong \bigoplus_\chi S(\chi)$$

where $S(\chi)$ is the χ-isotypical component of $S[P]$. The S-algebra $S(\chi)$ is a finite étale S-algebra and hence is an infinitesimal trait with the same local parameter as S and whose residue field is a finite separable extension $\kappa(\chi)$ of the residue field κ of S. We then have for each irreducible representation χ of P over κ, that there is a group homomorphism

$$\chi : P \to \kappa(\chi)^*$$

where $\kappa(\chi)$ is a finite separable extension field of κ.

The algebra $S[P]$ acts on the module $S(\chi)$. We have that

$$\mathrm{Ann}_{S(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1})$$

is an ideal of the algebra $S(\chi)$ and hence is of the form $\pi^m S(\chi)$ for some integer $m \geq 0$ where π is a local parameter of S; hence there is an ideal $I(\chi)$

of S such that we have the equality of ideals of $S(\chi)$

$$I(\chi)S(\chi) = \mathrm{Ann}_{S(\chi)}(a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}). \tag{6.10.5}$$

(6.10.6) Suppose that $z \in \mathrm{Supp}(c - z)$. Let $I_{c,c-2z,S}$ be the kernel in $\Delta_{c,S}$ of the algebra homomorphism

$$t^{\Delta}_{c,c-2z} : \Delta_{c,S} \to \Delta_{c-2z,S}.$$

The Heegner module $\mathcal{H}_{c-z,S}$ is that attached to K/F and the map of sets

$$\rho : \Sigma_F \setminus \tilde{I} \ \to \ S, \quad v \mapsto a_v.$$

Let

$$\rho^* : \Sigma_F \setminus (\tilde{I} \cup \{z\}) \ \to \ S, \quad v \mapsto a_v,$$

be the restriction of ρ to the subset $\Sigma_F \setminus (\tilde{I} \cup \{z\})$. Let $\mathcal{H}^*_{c-z,S}$ be the Heegner module with coefficients in S attached to ρ^* and K/F where the exceptional set of primes is $\tilde{I} \cup \{z\}$.

There is a decomposition of $\Delta_{c,S}$-modules

$$\Delta_{\leq c,S} = \bigoplus_{n \geq 0} \bigoplus_{\substack{c' \leq c - nz \\ c' \not\leq c-(n+1)z}} \Delta_{c',S}.$$

The module $\mathcal{H}^*_{c-z,S}$ admits a corresponding decomposition as a finite direct sum of $\Delta_{c,S}$-modules, as z is an exceptional prime for ρ^*,

$$\mathcal{H}^*_{c-z,S} = \bigoplus_{n \geq 1} H_{c-nz}.$$

Here H_{c-nz} is the image in $\mathcal{H}^*_{c-z,S}$ of the module $\displaystyle\bigoplus_{\substack{c' \leq c - nz \\ c' \not\leq c-(n+1)z}} \Delta_{c',S}$. Let

$$\pi_{c-z} : \mathcal{H}^*_{c-z,S} \to H_{c-z}$$

be the projection homomorphism onto the component H_{c-z} of the Heegner module $\mathcal{H}^*_{c-z,S}$ where the kernel of π_{c-z} is $\displaystyle\bigoplus_{n \geq 2} H_{c-nz}$.

6.10.7. Theorem. *Write G for the galois group $G(c/c-z)$. Assume that S is an infinitesimal trait with local parameter π. Then the isomorphism class of the $\Delta_{c,S}$-module*

$$\frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))}$$

is given by the following table.

(1) If z remains prime in K/F and is prime to $c-z$: $H^1(G,S)\otimes_S \mathrm{Ann}_S(a_z\otimes 1)\mathcal{H}_{c-z,S}$
(2) If z is ramified in K/F and is prime to $c-z$ where $\mathfrak{m}'_z$ is the prime ideal of O_{c-z} lying above the ideal $\mathfrak{m}_z$ of A defining z and $\lvert P\rvert$ is prime to the residue characteristic of S: $H^1(G,S)\otimes_S I_{\chi_L}\mathcal{H}_{c-z,S}$ where L is the smallest ideal of S for which there is a homomorphism $\chi_L : P\to (S/L)^*$ such that $a_z\otimes 1\equiv \chi_L([[\mathfrak{m}'_z]])\pmod L$.
(3) If z is split completely in K/F and is prime to $c-z$ where $\mathfrak{m}_z O_{c-z}=\mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1,\mathfrak{p}_2$ are two distinct prime ideals of O_{c-z} and $\lvert P\rvert$ is prime to the residue characteristic of S: $H^1(G,S)\otimes_S \bigoplus_\chi I(\chi)\mathcal{H}_{c-z,S}(\chi)$ where the sum runs over the irreducible representations $\chi : P\to \mathrm{GL}_n(S/(\pi))$, for all n, of P and where $\mathcal{H}_{c-z,S}(\chi)$ is the χ-isotypical component of $\mathcal{H}_{c-z,S}$ (see (6.7.15)).
(4) If $z\in \mathrm{Supp}(c-z)$: $H^1(G,S)\otimes_S I_{c,c-2z,S}\mathrm{Ann}_S(a_z\otimes 1)\pi_{c-z}(\mathcal{H}^*_{c-z,S})$ where $I_{c,c-2z,S}$ is the kernel of $t^{\Delta}_{c,c-2z}:\Delta_{c,S}\to\Delta_{c-2z,S}$.

Table 6.10.7: $H^0(G,\mathcal{H}_{c,S})/t(H^0(G,\mathcal{H}_{c-z,S}))$ **when S is an infinitesimal trait**

6.10.8. Remark. In the cases (2) and (3) of this table, where z is ramified or split completely in K/F, it is assumed that the order of the group P is prime to the residue characteristic of the infinitesimal trait S. The general case where P is divisible by the residue characteristic is left as an open problem.

6.11 Proof of theorem 6.10.7

We first prove the next proposition 6.11.1 and lemma 6.11.3 before proving theorem 6.10.7. Let S be an R-algebra which is an infinitesimal trait with local parameter π.

6.11.1. Proposition. *We have*

$$L(S) \cap J(S) = J_\Gamma(S)$$

provided that if $z \notin \mathrm{Supp}(c-z)$ *and that either* z *is ramified or* z *is split completely in* K/F *then* $|P|$ *is prime to the residue characteristic of* S.

(6.11.2) Recall (definition 6.8.8) that $L(S)$ is given as subset of $\Gamma_{\leq c,S}$ by

$$L(S) = \sum_{\substack{c' \leq c \\ c' \not\leq c-z}} \sum_{w \in \mathrm{Supp}(c') \setminus (\tilde{I} \cup \{z\})} e_{c',c'-z} \Gamma_{c',c'-w,S}.$$

For any saturated subset E of $\mathrm{Div}_+(A)$ all of whose elements are $\leq c$ we put

$$L(E,S) = \sum_{\substack{c' \in E, \\ c' \not\leq c-z}} \sum_{w \in \mathrm{Supp}(c') \setminus (\tilde{I} \cup \{z\})} e_{c',c'-z} \Gamma_{c',c'-w,S}.$$

6.11.3. Lemma. *Assume that if* $z \notin \mathrm{Supp}(c-z)$ *and that either* z *is ramified or split completely in* K/F *then* $|P|$ *is prime to the residue characteristic of the infinitesimal trait* S. *Let* $j \in L(S) \cap J(S)$ *and suppose that for some saturated subset* E *of* $\mathrm{Div}_+(A)$, *all elements of which are* $\leq c$, *we have*

$$j = \theta + \eta$$

where

$$\eta \in L(E,S) \cap J(S), \quad \theta \in J_\Gamma(S).$$

Let x *be a maximal element of* E *such that* $x \not\leq c - z$. *Then we have*

$$j = \theta' + \eta'$$

where

$$\eta' \in L(E \setminus \{x\}, S), \quad \theta' \in J_\Gamma(S).$$

Proof that lemma 6.11.3 implies proposition 6.11.1.

First it is clear that $J_\Gamma(S)$ is contained in both $L(S)$ and $J(S)$ and hence it is contained in their intersection.

Let $j \in L(S) \cap J(S)$. Let E_0 be the saturated subset of $\mathrm{Div}_+(A)$ given by $\{c' \mid c' \leq c\}$. We have that j can be written in the form

$$j = \theta_1 + \eta_1$$

where, taking $\theta_1 = 0$,

$$\theta_1 \in J_\Gamma(S)$$

and

$$\eta_1 \in L(E_0, S) \cap J(S).$$

Using lemma 6.11.3, we may construct inductively finite sequences E_i, θ_i, η_i, for $i = 1, 2, \ldots$ where

(i) E_i are saturated subsets of E_0 forming a strictly decreasing sequence

$$E_0 \supset E_1 \supset \ldots \supset E_n \supset \ldots$$

such that $E_i \setminus E_{i+1} = \{d_i\}$ where $d_i \not\leq c - z$ and d_i is a maximal element of E_i;
(ii) θ_i are elements of $J_\Gamma(S)$ for all i;
(iii) $\eta_i \in L(E_i, S) \cap J(S)$ for all i;
(iv) $j = \theta_i + \eta_i$ for all i.

The sequence $\{E_i\}_i$ of subsets of the finite set E_0 is finite and terminates with a set E_n all of whose elements are $\leq c - z$. Hence we have that the sequence $\{\eta_i\}_i$ terminates with $\eta_n \in \Delta_{\leq c-z,S} \cap L(S) \cap J(S)$; that is to say $\eta_n = 0$. We obtain that $j = \theta_n$ where $\theta_n \in J_\Gamma(S)$. It follows that $J_\Gamma(S)$ contains $L(S) \cap J(S)$ and hence $J_\Gamma(S) = L(S) \cap J(S)$ as required.□

Proof of lemma 6.11.3.

The proof of this is similar to the proof of lemma 6.5.3.

Let $j \in L(S) \cap J(S)$ and suppose that for some saturated set E of effective divisors, all of which are $\leq c$, the element j can be written as

$$j = \theta + \eta$$

where

$$\eta \in L(E, S) \cap J(S)$$

and

$$\theta \in J_\Gamma(S).$$

The module $J_\Gamma(S)$ is a submodule of $J(S)$ (remark 6.8.9(i)) and is evidently a submodule of $L(S)$. Hence we have

$$J_\Gamma(S) \subseteq L(S) \cap J(S).$$

By taking the difference $j - \theta$, where $\theta \in J_\Gamma(S)$, we may reduce to the case where the element j in the lemma is of the form $j = \eta$ where $\eta \in L(E, S) \cap J(S)$.

We may therefore suppose that j is an element of the form

$$j = \bigoplus_{c' \leq c,\ c' \not\leq c-z} j_{c'}, \quad j_{c'} \in J_{c',z,S} \ \text{ for all } c',$$

where

$$j = e_{c,c-z} \sum_{d' \in E} \sum_{w \notin \tilde{I} \cup \{z\}} K_{d',d'-w}(\eta_{d',w}) \tag{6.11.4}$$

where $\eta_{d',w} \in \Delta_{d',S}$ for all d' and for all prime divisors $w \notin \tilde{I} \cup \{z\}$ and where the element j lies in $L(E, S) \cap J(S)$.

Let x be the chosen maximal element of the finite saturated set E where $x \not\leq c - z$, as stated in the lemma. Let $z_1, z_2, \ldots, z_n$ be the distinct prime divisors in $\mathrm{Supp}(x) \setminus (\tilde{I} \cup \{z\})$. We consider the component of this element j in $\Delta_{x,S}$ namely the sum $\sum_{d' \in E}$ in (6.11.4) can be written in the form

$$j = e_{c,c-z} \sum_{i=1}^{n} K_{x,x-z_i}(\eta_{x,z_i}) + \gamma \tag{6.11.5}$$

where

$$\gamma \in L(E \backslash \{x\}, S). \tag{6.11.6}$$

The definition of the K homomorphisms is the following equation (see (5.3.6))

$$K_{f,f-w}(\delta) = (a_w - \epsilon(f, w)) t^{\Delta}_{f,f-w}(\delta) - \frac{|O^*_{f-w}|}{|A^*|} e_{f,f-w}\delta.$$

The component of $K_{f,f-w}(\delta)$ in $\Delta_{x,S}$ is therefore zero if the divisor f is not equal to x, $x + w$ or $x + 2w$ (by the definition of $K_{f,f-w}$); the component of $K_{x,x-z_i}(\delta)$ in $\Delta_{x,S}$ is then equal to

$$-\frac{|O^*_{x-z_i}|}{|A^*|} e_i \delta$$

where we write

$$e_i = e_{x,x-z_i} = \sum_{g \in G_i} g$$

and

$$G_i = \ker(t_{x,x-z_i}) = G(x/x - z_i), \quad \text{for all } i.$$

The maximality of x implies that x, $x + w$ and $x + 2w$ do not lie in the set $E \setminus \{x\}$ for all prime divisors w. Hence for the sum

$$\gamma = \sum_{c' \in E \setminus \{x\}} \sum_{w \in \mathrm{Supp}(c') \setminus (\tilde{I} \cup \{z\})} \gamma_{c',c'-w}$$

where

$$\gamma_{c',c'-w} \in e_{c,c-z} \Gamma_{c',c'-w}$$

the component in $\Delta_{x,S}$ is equal to zero.

The component in $\Delta_{x,S}$ of the right hand side of the equation (6.11.5) is then the component in $\Delta_{x,S}$ of the sum

$$e_{c,c-z} \sum_{i=1}^{n} K_{x,x-z_i}(\eta_{x,z_i}).$$

Hence the component of this equation (6.11.5) in $\Delta_{x,S}$ is the equation

$$j_x = -e_{c,c-z} \sum_{i=1}^{n} \frac{|O^*_{x-z_i}|}{|A^*|} e_i \eta_{x,z_i} \tag{6.11.7}$$

where j_x is the component in $\Delta_{x,S}$ of j and where the element j_x lies in $J_{x,z,S}$.

Case 1. Suppose that z is inert in K/F and $z \notin \mathrm{Supp}(c - z)$.
In this case from the table 6.7.16 we have, as S is an infinitesimal trait,

$$J_{x,z,S} = \mathrm{Ann}_S(a_z \otimes 1) e_{c,c-z} \Delta_{x,S}.$$

Suppose first that $n = 1$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z} \frac{|O^*_{x-z_1}|}{|A^*|} e_1 \eta_{x,z_1}.$$

As $\frac{|O^*_{x-z_1}|}{|A^*|}$ is a unit of R and $j_x \in J_{x,z,S}$ we obtain

$$e_{c,c-z} e_1 \eta_{x,z_1} \in J_{x,z,S}.$$

That is to say, we have

$$e_{c,c-z} \eta_{x,z_1} \in J^{z_1}_{x,z,S}.$$

Putting

$$\theta = K_{x,x-z_1}(e_{c,c-z}\eta_{x,z_1})$$

we then have $\theta \in J_\Gamma(S)$. Hence we obtain from (6.11.5)

$$j = \theta + \gamma$$

where

$$\theta \in J_\Gamma(S), \quad \gamma \in L(E\backslash\{x\}, S) \cap J(S).$$

This proves the lemma in this case.

Assume now that $n \geq 2$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z}\sum_{i=1}^{n} e_i\eta_{x,z_i}, \quad e_i = e_{x,x-z_i}, \tag{6.11.8}$$

where we have

$$j_x \in J_{x,z,S} = \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S}.$$

The family of subgroups $\{G(x - z/x - z - z_i)\}_{i=1,\ldots,n}$ of $\mathrm{Pic}(O_{x-z})$ is R-admissible (proposition 5.8.4). As there is an isomorphism of $\Delta_{c,S}$-modules

$$\frac{e_{c,c-z}\Delta_{x,S}}{J_{x,z,S}} = \frac{e_{c,c-z}\Delta_{x,S}}{\mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S}} \cong \Delta_{x-z,S/\mathrm{Ann}_S(a_z\otimes 1)}$$

we may apply proposition 5.5.30 to the equation (6.11.8). We obtain that there are elements

$$u^{(i,j)} \in e_{c,c-z}\Delta_{x,S} \quad \text{for all } i \neq j \text{ and } 1 \leq i, j \leq n$$

such that

$$u^{(i,j)} = -u^{(j,i)} \quad \text{for all } i \neq j$$

and

$$e_{c,c-z}e_i\eta_{x,z_i} = e_i\theta_i + \sum_{\substack{j\neq i \\ 1\leq j\leq n}} e_{ij}u^{(i,j)} \quad \text{for all } i \geq 1 \tag{6.11.9}$$

where

$$e_{ij} = \sum_{h\in G_iG_j} h \quad \text{for all } i \neq j$$

and where

$$e_i\theta_i \in J_{x,z,S} = \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S}.$$

As $z_i \neq z$, we may select the element θ_i to be in $e_{c,c-z}\Delta_{x,S}$ and hence as $e_i\theta_i \in J_{x,z,S}$ we have in particular, $\theta_i \in J^{z_i}_{x,z,S}$ for all i (see (6.8.3)).

From lemma 5.10.1, this equation (6.11.9) then gives the equation

$$N\Big\{e_{c,c-z}\sum_{i=1}^{n}K_{x,x-z_i}(\eta_{x,z_i})-\sum_{i=1}^{n}K_{x,x-z_i}(\theta_i)\Big\}= \tag{6.11.10}$$

$$-\sum_{i=1}^{n}\sum_{1\le j\le n,j\ne i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}))$$

where

$$N=\frac{|O^*_{x-z_1-z_2}|}{|A^*|}$$

and where we have that $N=1$ unless $n=2$ and $x=z_1+z_2$; in particular, N is a unit in R, by the hypotheses (6.10.1).

We obtain from (6.11.10) and (6.11.5)

$$j=\sum_{i=1}^{n}K_{x,x-z_i}(\theta_i)+\gamma$$

$$-\frac{1}{N}\sum_{i=1}^{n}\sum_{1\le j\le n,j\ne i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}))$$

where, as $\theta_i\in J^{z_i}_{x,z,S}$ for all i,

$$\sum_{i=1}^{n}K_{x,x-z_i}(\theta_i)\in J_{\Gamma}(S)\ \text{ and }\ \gamma\in L(E\backslash\{x\},S)$$

and where

$$-\frac{1}{N}\sum_{i=1}^{n}\sum_{1\le j\le n,j\ne i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}))$$

also belongs to $L(E\backslash\{x\},S)$. We obtain

$$j=\sum_{i=1}^{n}K_{x,x-z_i}(\theta_i)+\delta$$

where $\delta\in L(E\backslash\{x\},S)$ and $\sum_{i=1}^{n}K_{x,x-z_i}(\theta_i)$ belongs to $J_{\Gamma}(S)$. As j belongs to $L(S)\cap J(S)$ we obtain that $\delta\in L(E\backslash\{x\},S)\cap J(S)$, which proves the lemma in the case where z is inert in K/F.

Case 2. Suppose that $z \notin \mathrm{Supp}(c-z)$, that z is ramified in K/F, and that $|P|$ is a unit of S.

Let $\mathfrak{m}_z$ be the ideal of A defining z. Let $\mathfrak{m}'_z$ be the prime ideal of O_{c-z} lying above $\mathfrak{m}_z$. Let P be the cyclic subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the ideal class of $\mathfrak{m}'_z$, where the order of P is assumed to be prime to the residue characteristic of S, that is to say the order has image in S which is a multiplicative unit. Let $\mathfrak{m}'_{z,x}$ be the prime ideal of O_{x-z} lying above $\mathfrak{m}_z$. Then $\mathfrak{m}'_z = \mathfrak{m}'_{z,x} \cap O_{c-z}$; hence the group P_x generated by the ideal class of $\mathfrak{m}'_{z,x}$ in $\mathrm{Pic}(O_{x-z})$ is a homomorphic image of the group P. Hence the order of P_x is also a unit of S.

By the table 6.7.16 we then have

$$J_{x,z,S} = I_{\chi_L}$$

where L is the smallest ideal of S for which there is a rank 1 character

$$\chi_L : P_x \to (S/L)^*$$

of P_x such that

$$a_z \otimes 1 \equiv \chi_L([[\mathfrak{m}'_{z,x}]]) \pmod{L}.$$

By definition we have

$$I_{\chi_L} = \{\delta \in \mathrm{Ann}_S(L) e_{x,x-z} \Delta_{x,S} |\ h\delta = \chi_L^{-1}(h)\delta \ \text{ for all } h \in P_x\}. \tag{6.11.11}$$

Fix an isomorphism of $\Delta_{c,S}$-modules

$$i : \Delta_{x-z,S/L} \xrightarrow{\sim} \mathrm{Ann}_S(L) e_{x,x-z} \Delta_{x,S}.$$

We have (see (6.7.10) and (6.10.3))

$$I_{\chi_L} = i(g_{\chi_L} \Delta_{x-z,S/L})$$

where

$$g_{\chi_L} = \sum_{g \in P_x} g\chi_L(g) \in \Delta_{x-z,S/L}.$$

Suppose first that $n = 1$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z} \frac{|O^*_{x-z_1}|}{|A^*|} e_1 \eta_{x,z_1}.$$

As $\frac{|O^*_{x-z_1}|}{|A^*|}$ is a unit of R and $j_x \in J_{x,z,S}$ we obtain

$$e_{c,c-z} e_1 \eta_{x,z_1} \in J_{x,z,S} = I_{\chi_L}.$$

Hence we have (see (6.8.3))

$$e_{c,c-z} \eta_{x,z_1} \in J^{z_1}_{x,z,S}.$$

Putting

$$\theta = K_{x,x-z_1}(e_{c,c-z}\eta_{x,z_1})$$

we then have $\theta \in J_\Gamma(S)$. Hence we obtain from (6.11.5)

$$j = \theta + \gamma$$

where

$$\theta \in J_\Gamma(S), \quad \gamma \in L(E\backslash\{x\}, S) \cap J(S).$$

This proves the lemma in this case.

Assume now that $n \geq 2$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z}\sum_{i=1}^{n} e_i\eta_{x,z_i}, \quad e_i = e_{x,x-z_i}, \tag{6.11.12}$$

where we have

$$j_x \in J_{x,z,S} = I_{\chi_L}.$$

We have by definition

$$g_{\chi_L} = \sum_{g\in P_x} g\chi_L(g) \in \Delta_{x-z,S/L}$$

and we have

$$g_{\chi_L}g_{\chi_L} = |P_x|g_{\chi_L}.$$

Put

$$g^*_{\chi_L} = g_{\chi_L}/|P_x| \ \in \ \Delta_{x-z,S/L}.$$

This is well defined as $|P_x|$ is a unit of S. The element $g^*_{\chi_L}$ acts on $\mathrm{Ann}_S(L)e_{c,c-z}\Delta_{x,S}$; in particular, $g^*_{\chi_L}$ acts on $I_{\chi_L} = J_{x,z,S}$ as we have $I_{\chi_L} \subset \mathrm{Ann}_S(L)e_{c,c-z}\Delta_{x,S}$. We have for any element $h \in I_{\chi_L}$

$$g^*_{\chi_L}h = h.$$

The family of subgroups $\{G(x - z/x - z - z_i)\}_{i=1,\ldots,n}$ of $\mathrm{Pic}(O_{x-z})$ is R-admissible (proposition 5.8.4). As there is an isomorphism of $\Delta_{c,S}$-modules

$$\mathrm{Ann}_S(L)e_{c,c-z}\Delta_{x,S} \cong \Delta_{x-z,S/L}$$

and as $j_x \in \mathrm{Ann}_S(L)e_{c,c-z}\Delta_{x,S}$, we may apply proposition 5.5.30 to the equation (6.11.12). We obtain that there are elements

$$u^{(i,j)} \in \Delta_{x,S} \ \text{ for all } i \neq j \text{ and } 1 \leq i, j \leq n$$

such that

$$u^{(i,j)} = -u^{(j,i)}, \ \text{ for all } i \neq j,$$

and elements

$$e_{c,c-z}e_i\theta_i \in e_i\mathrm{Ann}_S(L)e_{c,c-z}\Delta_{x,S}$$

where we have

$$e_{c,c-z}e_i\eta_{x,z_i} = e_{c,c-z}e_i\theta_i + e_{c,c-z}\sum_{\substack{j\neq i\\ 1\leq j\leq n}} e_{ij}u^{(i,j)} \quad \text{for all } i \geq 1 \tag{6.11.13}$$

and

$$e_{ij} = \sum_{h\in G_iG_j} h \quad \text{for all } i \neq j.$$

Summing the equations (6.11.13) over all i we obtain the equation

$$j_x = -e_{c,c-z}\sum_{i=1}^{n} e_i\theta_i \tag{6.11.14}$$

Multiplying the equation (6.11.14) by $g^*_{\chi_L}$ we obtain, as $g^*_{\chi_L}j_x = j_x$,

$$j_x = -e_{c,c-z}\sum_{i=1}^{n} g^*_{\chi_L}e_i\theta_i. \tag{6.11.15}$$

The difference between the equations (6.11.14) and (6.11.15) gives the equation

$$0 = -e_{c,c-z}\sum_{i=1}^{n} e_i(\theta_i - g^*_{\chi_L}\theta_i). \tag{6.11.16}$$

As we have an isomorphism of $\Delta_{c,S}$-modules

$$\mathrm{Ann}_S(L)e_{c,c-z}\Delta_{x,S} \cong \Delta_{x-z,S/L}$$

we may again apply 5.5.30 to the equation (6.11.16). We obtain that there are elements

$$v^{(i,j)} \in \mathrm{Ann}_S(L)\Delta_{x,S} \quad \text{for all } i \neq j \text{ and } 1 \leq i,j \leq n$$

such that

$$v^{(i,j)} = -v^{(j,i)} \quad \text{for all } i \neq j$$

and

$$e_{c,c-z}e_i\theta_i = g^*_{\chi_L}e_{c,c-z}e_i\theta_i + e_{c,c-z}\sum_{\substack{j\neq i\\ 1\leq j\leq n}} e_{ij}v^{(i,j)} \quad \text{for all } i \geq 1. \tag{6.11.17}$$

We then obtain from (6.11.17) and (6.11.13)

$$e_{c,c-z}e_i\eta_{x,z_i} = g^*_{\chi_L}e_{c,c-z}e_i\theta_i + e_{c,c-z}\sum_{\substack{j\neq i\\ 1\leq j\leq n}} e_{ij}(u^{(i,j)} + v^{(i,j)}) \quad \text{for all } i \geq 1. \tag{6.11.18}$$

We have here

$$g^*_{\chi_L}e_{c,c-z}e_i\theta_i \ \in \ e_iI_{\chi_L} = e_iJ_{x,z,S}$$

for all i, hence we have $g^*_{\chi_L}e_{c,c-z}\theta_i \in J^{z_i}_{x,z,S}$ for all i (see (6.8.3)).

From lemma 5.10.1, this equation (6.11.18) then gives the equation

$$N\Big\{e_{c,c-z}\sum_{i=1}^{n}K_{x,x-z_i}(\eta_{x,z_i})-\sum_{i=1}^{n}K_{x,x-z_i}(e_{c,c-z}g^*_{\chi_L}\theta_i)\Big\}= \tag{6.11.19}$$

$$-e_{c,c-z}\sum_{i=1}^{n}\sum_{1\le j\le n,j\ne i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}+v^{(i,j)}))$$

where

$$N=\frac{|O^*_{x-z_1-z_2}|}{|A^*|}$$

and where we have that $N=1$ unless $n=2$ and $x=z_1+z_2$; in particular, N is a unit in R, by the hypotheses (6.10.1).

We obtain from (6.11.19) and (6.11.5)

$$j=\sum_{i=1}^{n}K_{x,x-z_i}(e_{c,c-z}g^*_{\chi_L}\theta_i)+\gamma$$

$$-e_{c,c-z}\frac{1}{N}\sum_{i=1}^{n}\sum_{1\le j\le n,j\ne i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}+v^{(i,j)}))$$

where

$$\gamma\in L(E\backslash\{x\},S).$$

and where

$$-\frac{1}{N}e_{c,c-z}\sum_{i=1}^{n}\sum_{1\le j\le n,j\ne i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}+v^{(i,j)}))$$

also belongs to $L(E\backslash\{x\},S)$. We obtain

$$j=\sum_{i=1}^{n}K_{x,x-z_i}(e_{c,c-z}g^*_{\chi_L}\theta_i)+\delta$$

where $\delta\in L(E\backslash\{x\},S)$ and $\sum_{i=1}^{n}K_{x,x-z_i}(e_{c,c-z}g^*_{\chi_L}\theta_i)$ belongs to $J_\Gamma(S)$ as $g^*_{\chi_L}e_{c,c-z}\theta_i\in J^{z_i}_{x,z,S}$ for all i. As j belongs to $L(S)\cap J(S)$ we obtain that $\delta\in L(E\backslash\{x\},S)\cap J(S)$, which proves the lemma in the case where $z\notin\mathrm{Supp}(c-z)$, z is ramified in K/F, and $|P|$ is a unit in S.

Case 3. Suppose that $z \notin \mathrm{Supp}(c-z)$, z is split completely in K/F, and $|P|$ is a unit of S.

Let $\mathfrak{m}_z$ be the ideal of A defining z. Let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be the prime ideals of O_{x-z} lying over the prime ideal $\mathfrak{m}_z$ of A. We put

$$g =< [[\mathfrak{p}_1]]^{-1}, x-z >$$

$$h =< [[\mathfrak{p}_2]]^{-1}, x-z > .$$

Let P_x be the subgroup of $\mathrm{Pic}(O_{x-z})$ generated by g and h. The group P is, by definition, the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the classes of the prime ideals of O_{c-z} lying over $\mathfrak{m}_z$. There is an evident surjective group homomorphism $P \to P_x$. Hence the order of P_x is prime to the residue characteristic of S.

Let $\Delta(\chi)$ denote the χ-isotypical component of $e_{c,c-z}\Delta_{x,S}$ for any irreducible representation $\chi : P \to \mathrm{GL}_n(S/(\pi))$ where $S/(\pi)$ is the residue field of S. By (6.7.15), we have a decomposition of the group algebra $S[P_x]$ into its isotypical components $S(\chi)$, where the order of the group P_x is prime to the residue characteristic of S by hypothesis,

$$S[P_x] \cong \bigoplus_{\chi} S(\chi).$$

By the table 6.7.16 and (6.7.51), (6.7.52) we then have an equality of submodules of $\Delta_{x,S}$

$$J_{x,z,S} = \bigoplus_{\chi} \mathrm{Ann}_{\Delta(\chi)}(a_z \otimes 1 - g - h)$$

where the sum runs over the irreducible representations χ of P_x over $S/(\pi)$. We then have

$$J_{x,z,S} = \bigoplus_{\chi} \bigoplus_{w \in \mathrm{Pic}(O_{x-z})/P_x} w\mathrm{Ann}_{S(\chi)}(a_z \otimes 1 - g - h)$$

where the sum $\bigoplus_{w \in \mathrm{Pic}(O_{x-z})/P_x}$ runs over a set of coset representatives of P_x in $\mathrm{Pic}(O_{x-z})$.

As $S(\chi)$ is a finite étale S-algebra (see (6.7.15)) it is an infinitesimal trait with the same local parameter π as S. Hence we have

$$\mathrm{Ann}_{S(\chi)}(a_z \otimes 1 - g - h) = S(\chi)A_\chi$$

where A_χ is the ideal of S given by

$$A_\chi = \mathrm{Ann}_S(a_z \otimes 1 - g - h);$$

that is to say, A_χ is the ideal of S annihilated by the element $a_z \otimes 1 - [[\mathfrak{p}_1]]^{-1} - [[\mathfrak{p}_2]]^{-1}$ of the S-algebra $S(\chi)$. Hence we have isomorphisms of $\Delta_{c,S}$-modules

$$J_{x,z,S} \cong \bigoplus_{\chi} \bigoplus_{w \in \mathrm{Pic}(O_{x-z})/P_x} wA_\chi S(\chi) \cong \bigoplus_{\chi} A_\chi \Delta(\chi).$$

Suppose first that $n = 1$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z} \frac{|O^*_{x-z_1}|}{|A^*|} e_1 \eta_{x,z_1}.$$

As $\frac{|O^*_{x-z_1}|}{|A^*|}$ is a unit of R and $j_x \in J_{x,z,S}$ we obtain

$$e_{c,c-z} e_1 \eta_{x,z_1} \in J_{x,z,S}.$$

Hence we have (see (6.8.3))

$$e_{c,c-z} \eta_{x,z_1} \in J^{z_1}_{x,z,S}.$$

Putting

$$\theta = K_{x,x-z_1}(e_{c,c-z}\eta_{x,z_1})$$

we then have $\theta \in J_\Gamma(S)$. Hence we obtain from (6.11.5)

$$j = \theta + \gamma$$

where

$$\theta \in J_\Gamma(S), \quad \gamma \in L(E \backslash \{x\}, S) \cap J(S).$$

This proves the lemma in this case.

Assume now that $n \geq 2$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z} \sum_{i=1}^{n} e_i \eta_{x,z_i}, \quad e_i = e_{x,x-z_i}, \tag{6.11.20}$$

where we have

$$j_x \in J_{x,z,S}.$$

The family of subgroups $\{G(x - z/x - z - z_i)\}_{i=1,\ldots,n}$ of $\mathrm{Pic}(O_{x-z})$ is R-admissible (proposition 5.8.4). As there is an isomorphism of S-modules

$$S/\mathrm{Ann}_S(A_\chi) \cong A_\chi$$

and as j_x lies in the submodule $\bigoplus_\chi A_\chi \Delta(\chi)$ of $\Delta_{x,S}$, we may apply proposition 5.5.30 to the equation (6.11.20); for this proposition applies to each component $\Delta(\chi) \otimes_S S/L$ for any ideal L of S and for any χ. We obtain that there are elements

$$u^{(i,j)} \in e_{c,c-z} \Delta_{x,S} \quad \text{for all } i \neq j \text{ and } 1 \leq i, j \leq n$$

such that

$$u^{(i,j)} = -u^{(j,i)} \quad \text{for all } i \neq j$$

and elements

$$e_{c,c-z}e_i\theta_i \in e_i \bigoplus_{\chi} A_\chi \Delta(\chi) = e_i J_{x,z,S}$$

where we have

$$e_{c,c-z}e_i\eta_{x,z_i} = e_{c,c-z}e_i\theta_i + e_{c,c-z}\sum_{\substack{j\neq i\\ 1\leq j\leq n}} e_{ij}u^{(i,j)} \quad \text{for all } i \geq 1 \tag{6.11.21}$$

and

$$e_{ij} = \sum_{h\in G_iG_j} h \quad \text{for all } i \neq j.$$

We have here

$$e_{c,c-z}e_i\theta_i \ \in \ e_i J_{x,z,S}$$

for all i; hence $e_{c,c-z}\theta_i \in J^{z_i}_{x,z,S}$ for all i (see (6.8.3)).

From lemma 5.10.1, this equation (6.11.21) then gives the equation

$$N\left\{e_{c,c-z}\sum_{i=1}^{n} K_{x,x-z_i}(\eta_{x,z_i}) - \sum_{i=1}^{n} K_{x,x-z_i}(e_{c,c-z}\theta_i)\right\} = \tag{6.11.22}$$

$$-e_{c,c-z}\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i} - \epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)})).$$

where

$$N = \frac{|O^*_{x-z_1-z_2}|}{|A^*|}$$

and where we have that $N = 1$ unless $n = 2$ and $x = z_1 + z_2$; in particular, N is a unit in R, by the hypotheses (6.10.1).

We obtain from (6.11.22) and (6.11.5)

$$j = \sum_{i=1}^{n} K_{x,x-z_i}(e_{c,c-z}\theta_i) + \gamma$$

$$-e_{c,c-z}\frac{1}{N}\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i} - \epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}))$$

where

$$\gamma \in L(E\backslash\{x\}, S).$$

and where

$$-\frac{1}{N}e_{c,c-z}\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i} - \epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}))$$

also belongs to $L(E\backslash\{x\}, S)$. We obtain

$$j = \sum_{i=1}^{n} K_{x,x-z_i}(e_{c,c-z}\theta_i) + \delta$$

where $\delta \in L(E\backslash\{x\}, S)$ and $\sum_{i=1}^{n} K_{x,x-z_i}(e_{c,c-z}\theta_i)$ belongs to $J_\Gamma(S)$ as $e_{c,c-z}\theta_i \in J^{z_i}_{x,z,S}$ for all i. As j belongs to $L(S) \cap J(S)$ we obtain that $\delta \in L(E\backslash\{x\}, S) \cap J(S)$, which proves the lemma in the case where $z \notin \mathrm{Supp}(c - z)$, z is split completely in K/F, and $|P|$ is a unit in S.

Case 4. Suppose that $z \in \mathrm{Supp}(c - z)$.

By the table 6.7.16 we have

$$J_{x,z,S} = \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}I_{x,x-2z,S}.$$

That is to say, an element $e_{c,c-z}y$ of $e_{c,c-z}\Delta_{x,S}$, where $y \in \Delta_{x,S}$, lies in $J_{x,z,S}$ if and only if $(a_z \otimes 1)t^{\Delta}_{x,x-z}(y) = 0$ and $t^{\Delta}_{x,x-2z}(y) = 0$.

Suppose first that $n = 1$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z}\frac{|O^*_{x-z_1}|}{|A^*|}e_1\eta_{x,z_1}.$$

As $\frac{|O^*_{x-z_1}|}{|A^*|}$ is a unit of R and $j_x \in J_{x,z,S}$ we obtain

$$e_{c,c-z}e_1\eta_{x,z_1} \in J_{x,z,S}.$$

That is to say, we have

$$e_{c,c-z}\eta_{x,z_1} \in J^{z_1}_{x,z,S}.$$

Putting

$$\theta = e_{c,c-z}K_{x,x-z_1}(\eta_{x,z_1})$$

we then have $\theta \in J_\Gamma(S)$. Hence we obtain from (6.11.5)

$$j = \theta + \gamma$$

where

$$\theta \in J_\Gamma(S), \quad \gamma \in L(E\backslash\{x\}, S) \cap J(S).$$

This proves the lemma in this case.

Assume now that $n \geq 2$. Then the equation (6.11.7) becomes

$$j_x = -e_{c,c-z}\sum_{i=1}^{n} e_i\eta_{x,z_i} \tag{6.11.23}$$

where we have

$$j_x \in J_{x,z,S} = \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}I_{x,x-2z,S}.$$

The family of subgroups $\{G(x - z/x - z - z_i)\}_{i=1,\ldots,n}$ of $\mathrm{Pic}(O_{x-z})$ is R-admissible (proposition 5.8.4). As there is an isomorphism of $\Delta_{c,S}$-modules

$$e_{c,c-z}\Delta_{x,S}/\mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S} \;\cong\; \Delta_{x-z,S/\mathrm{Ann}_S(a_z\otimes 1)}$$

we may apply proposition 5.5.30 to the equation (6.11.23). We obtain that there are elements

$$u^{(i,j)} \in e_{c,c-z}\Delta_{x,S} \quad \text{for all } i \neq j \text{ and } 1 \leq i, j \leq n$$

such that

$$u^{(i,j)} = -u^{(j,i)}, \quad \text{for all } i \neq j,$$

and

$$e_{c,c-z}e_i\eta_{x,z_i} = e_i\theta_i + \sum_{\substack{j\neq i \\ 1\leq j\leq n}} e_{ij}u^{(i,j)} \quad \text{for all } i \geq 1 \tag{6.11.24}$$

where

$$e_{ij} = \sum_{h\in G_iG_j} h \quad \text{for all } i \neq j$$

and where

$$\theta_i \in \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S} \quad \text{for all } i.$$

Summing over all i we obtain from (6.11.24) and (6.11.23)

$$j_x = -\sum_{i=1}^{n} e_i\theta_i. \tag{6.11.25}$$

where

$$j_x \in \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}I_{x,x-2z,S}.$$

Applying the homomorphism $t^{\Delta}_{x,x-2z}$ to the equation (6.11.25), we obtain the equation in $\Delta_{x-2z,S}$

$$0 = -\sum_{i=1}^{n} e_i t^{\Delta}_{x,x-2z}(\theta_i). \tag{6.11.26}$$

There is an evident isomorphism of $\Delta_{c,S}$-modules

$$\mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S} \cong \Delta_{x-z,S/(a_z\otimes 1)S}.$$

Hence we may again apply 5.5.30 to the equation (6.11.26). We obtain that there are elements

$$v^{(i,j)} \in \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S} \quad \text{for all } i \neq j \text{ and } 1 \leq i, j \leq n$$

and elements

$$\xi_i \in \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S} \quad \text{for all } i$$

such that

$$v^{(i,j)} = -v^{(j,i)}, \quad \text{for all } i \neq j,$$

and

$$e_i\theta_i = e_i\xi_i + \sum_{\substack{j\neq i \\ 1\leq j\leq n}} e_{ij}v^{(i,j)} \quad \text{for all } i \geq 1 \tag{6.11.27}$$

where

$$t^{\Delta}_{x,x-2z}(e_i\xi_i) = 0.$$

Hence we have

$$e_i\xi_i \in I_{x,x-2z,S} \cap \mathrm{Ann}_S(a_z \otimes 1)e_{c,c-z}\Delta_{x,S} = J_{x,z,S}.$$

It follows that (see (6.8.3))

$$\xi_i \in J^{z_i}_{x,z,S} \quad \text{for all } i.$$

From lemma 5.10.1, the equations (6.11.24) and (6.11.27) then give the equation

$$N\left\{e_{c,c-z}\sum_{i=1}^{n} K_{x,x-z_i}(\eta_{x,z_i}) - \sum_{i=1}^{n} K_{x,x-z_i}(\xi_i)\right\} = \tag{6.11.28}$$

$$-\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i} - \epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)} + v^{(i,j)}))$$

where

$$N = \frac{|O^*_{x-z_1-z_2}|}{|A^*|}$$

and where we have that $N = 1$ unless $n = 2$ and $x = z_1 + z_2$; in particular, N is a unit in R, by the hypotheses (6.10.1).

We obtain from (6.11.28) and (6.11.5)

$$j = \sum_{i=1}^{n} K_{x,x-z_i}(\xi_i) + \gamma$$

$$-\frac{1}{N}\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i} - \epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)} + v^{(i,j)}))$$

where

$$\gamma \in L(E\backslash\{x\}, S)$$

and where

$$-\frac{1}{N}\sum_{i=1}^{n}\sum_{1\leq j\leq n, j\neq i}(a_{z_i}-\epsilon(x,z_i))K_{x-z_i,x-z_i-z_j}(t^{\Delta}_{x,x-z_i}(u^{(i,j)}+v^{(i,j)}))$$

also belongs to $L(E\backslash\{x\},S)$ as $u^{(i,j)}, v^{(i,j)} \in e_{c,c-z}\Delta_{x,S}$ for all i,j. We obtain

$$j=\sum_{i=1}^{n}K_{x,x-z_i}(\xi_i)+\delta$$

where $\delta \in L(E\backslash\{x\},S)$ and $\sum_{i=1}^{n}K_{x,x-z_i}(\xi_i)$ belongs to $J_{\Gamma}(S)$ as $\xi_i \in J^{z_i}_{x,z,S}$ for all i. As j belongs to $L(S)\cap J(S)$ we obtain that $\delta \in L(E\backslash\{x\},S)\cap J(S)$. This completes the proof of lemma 6.11.3 and of proposition 6.11.1.□

End of proof of theorem 6.10.7.

Put $S'=S/\exp(G)S$. By corollary 6.8.11 we have the exact sequence of $\Delta_{c,S}$-modules

$$0\longrightarrow H^1(G,L(S')\cap J(S'))\longrightarrow J(H^1(G,S))\xrightarrow{\Xi}\frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))}\longrightarrow 0.$$

In the case where $z\notin \mathrm{Supp}(c-z)$ and either z is ramified or z is split completely in K/F then it is assumed that $|P|$ is prime to the residue characteristic of the infinitesimal trait S; this corresponds to the cases (2) and (3) of table 6.10.7.

By proposition 6.11.1, we then have the equality

$$L(S')\cap J(S')=J_{\Gamma}(S').$$

Hence we obtain the exact sequence of $\Delta_{c,S}$-modules
(6.11.29)

$$0\longrightarrow H^1(G,J_{\Gamma}(S'))\longrightarrow J(H^1(G,S))\xrightarrow{\Xi}\frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))}\longrightarrow 0.$$

By lemma 6.9.7, the group $H^1(G,S)$ is a finite free S'-module; by remarks 6.8.4(i) and (ii), we then have an isomorphism of $\Delta_{c,S}$-modules

$$J(H^1(G,S))\cong J(S')\otimes_S H^1(G,S).$$

As G acts trivially on $J_{\Gamma}(S')$, lemma 6.9.9 (or the universal coefficient theorem; see (6.9.8)) shows that there is a non-canonical isomorphism of $\Delta_{c,S}$-modules

$$H^1(G,J_{\Gamma}(S'))\cong J_{\Gamma}(S')\otimes_S H^1(G,S).$$

Hence we obtain from (6.11.29) the exact sequence of $\Delta_{c,S}$-modules (6.11.30)

$$0 \to J_\Gamma(S') \otimes_S H^1(G,S) \to J(S') \otimes_S H^1(G,S) \xrightarrow{\Xi} \frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))} \to 0$$

where the first arrow is induced by the inclusion $J_\Gamma(S') \subseteq J(S')$.

Case 1. Suppose that z is inert in K/F and $z \notin \mathrm{Supp}(c-z)$.
From table 6.7.16 we have

$$J(S') = \mathrm{Ann}_{S'}(a_z \otimes 1) \bigoplus_{c' \le c,\ c' \not\le c-z} e_{c',c'-z}\Delta_{c',S'}. \tag{6.11.31}$$

From proposition 5.7.8(i), we have the equation

$$e_{c,c-z}\delta = \frac{|O^*_{c'-z}|}{|A^*|} e_{c',c'-z}\delta \quad \text{for all } c' < c, c' \not\le c-z \text{ and } \delta \in \Delta_{c',S}. \tag{6.11.32}$$

We obtain from the equation (6.11.31) and as the integer $|B^*|/|A^*|$ is assumed to be a multiplicative unit of R,

$$J(S') = \mathrm{Ann}_{S'}(a_z \otimes 1) e_{c,c-z} \bigoplus_{c' \le c,\ c' \not\le c-z} \Delta_{c',S'}. \tag{6.11.33}$$

We obtain from (6.11.31) for any prime divisor w, where $w \in \mathrm{Supp}(c')$ and $w \neq z$,

$$J^w_{c',z,S}(S') = \mathrm{Ann}_{S'}(a_z \otimes 1) e_{c',c'-z}\Delta_{c',S'} + e_{c',c'-z} I_{c',c'-w,S'}$$

where $I_{c',c'-w,S'}$ is the augmentation ideal of $\Delta_{c',S'}$ with respect to the subgroup $\ker(t_{c',c'-w})$ of $\mathrm{Pic}(O_{c'})$. Hence we have

$$\begin{aligned} K_{c',c'-w}(J^w_{c',z,S'}) &= \mathrm{Ann}_{S'}(a_z \otimes 1) K_{c',c'-w}(e_{c',c'-z}\Delta_{c',S'}) \\ &= \mathrm{Ann}_{S'}(a_z \otimes 1) e_{c',c'-z}\Gamma_{c',c'-w,S'}. \end{aligned} \tag{6.11.34}$$

From this we have

$$J_\Gamma(S') = \mathrm{Ann}_{S'}(a_z \otimes 1) \sum_{\substack{c' \le c \\ \text{such that } c' \not\le c-z}} \sum_{\substack{w \in \mathrm{Supp}(c') \\ w \notin \bar{I} \cup \{z\}}} e_{c',c'-z}\Gamma_{c',c'-w,S'}. \tag{6.11.35}$$

We obtain from (6.11.32) and (6.11.35)

$$\begin{aligned} J_\Gamma(S') &= \mathrm{Ann}_{S'}(a_z \otimes 1) e_{c,c-z} \sum_{\substack{c' \le c \\ \text{such that } c' \not\le c-z}} \sum_{\substack{w \in \mathrm{Supp}(c') \\ w \notin \bar{I} \cup \{z\}}} \Gamma_{c',c'-w,S'} \\ &= \mathrm{Ann}_{S'}(a_z \otimes 1) L(S') \end{aligned} \tag{6.11.36}$$

where $L(S')$ is defined in (6.8.8).

We have the commutative diagram of $\Delta_{c,S}$-modules

$$\begin{array}{ccc} & \Delta_{c',S'} & \\ {\scriptstyle t^{\Delta}_{c',c'-z}}\swarrow & & \searrow{\scriptstyle e_{c,c-z}} \\ \Delta_{c'-z,S'} & \longrightarrow & e_{c,c-z}\Delta_{c',S'} \\ & {\scriptstyle i_{c',c'-z}} & \end{array} \tag{6.11.37}$$

where the right hand arrow $e_{c,c-z} : \Delta_{c',S'} \to e_{c,c-z}\Delta_{c',S'}$ is multiplication by $e_{c,c-z}$. The horizontal homomorphism

$$i_{c',c'-z} : \Delta_{c'-z,S'} \to e_{c,c-z}\Delta_{c',S'}$$

given by

$$1_{\Delta_{c'-z,S'}} \mapsto e_{c,c-z}.1_{\Delta_{c',S'}}$$

is an isomorphism of $\Delta_{c,S}$-modules. We have for all prime divisors $w \neq z$

$$t^{\Delta}_{w} \circ i_{c',c'-z} = i_{c'-w,c'-z-w} \circ t^{\Delta}_{w}.$$

We write

$$i_z = \bigoplus_{c' \leq c, c' \not\leq c-z} i_{c',c'-z}$$

where the sum runs over all $c' \in \mathrm{Div}_+(A)$ with $c' \leq c$ and $c' \not\leq c - z$. Thus i_z is an isomorphism, as $z \notin \mathrm{Supp}(c - z)$,

$$i_z : \Delta_{\leq c-z,S'} \to \bigoplus_{c' \leq c, c' \not\leq c-z} e_{c,c-z}\Delta_{c',S'}$$

given by $i_{c',c'-z}$ on each component of the graded $\Delta_{c,S}$-module $\Delta_{\leq c-z,S'}$.

We have (by proposition 5.7.8(iii)) for all $w \neq z$, where $w, z \notin \tilde{I}$ are prime divisors,

$$t^{\Delta}_{z} \circ K_{c',c'-w} = K_{c'-z,c'-z-w} \circ t^{\Delta}_{z}.$$

Hence we have

$$i_z \circ t^{\Delta}_{z} \circ K_{c',c'-w} = i_z \circ K_{c'-z,c'-z-w} \circ t^{\Delta}_{z}.$$

From the commutative diagram (6.11.37) above, the action of $i_z \circ t^{\Delta}_{z}$ on $\bigoplus_{c' \leq c, c' \not\leq c-z} \Delta_{c',S}$ is multiplication by $e_{c,c-z}$. Hence we obtain for all $\delta \in \Delta_{c',S'}$

$$e_{c,c-z}K_{c',c'-w}(\delta) = i_z K_{c'-z,c'-z-w}(t^{\Delta}_{z}(\delta)).$$

Hence the isomorphism $i_z : \Delta_{\leq c-z,S'} \to \bigoplus_{c'\leq c, c'\not\leq c-z} e_{c,c-z}\Delta_{c',S'}$ induces an isomorphism of $\Delta_{c,S'}$-modules, where $J(S')$ is considered a submodule of $\Delta_{\leq c,S'}$,

$$i_z^{-1}|_{J(S')} : J(S') \cong \mathrm{Ann}_{S'}(a_z \otimes 1) \bigoplus_{d\leq c-z} \Delta_{d,S'}$$

given by

$$\bigoplus_{c'\leq c,\ c'\not\leq c-z} \delta_{c',S} \mapsto \bigoplus_{d\leq c-z} i_z^{-1}(\delta_{d+z,S'}).$$

Hence we obtain an isomorphism of $\Delta_{c,S}$-modules induced by i_z

$$J(S') \cong \mathrm{Ann}_{S'}(a_z \otimes 1)\Delta_{\leq c-z,S'}$$

and we have a commutative diagram where the vertical maps are inclusions (6.11.38)

$$\begin{array}{ccccc} & & i_z & & \\ \Delta_{\leq c-z,S'} & \to & \bigoplus_{c'\leq c,c'\not\leq c-z} e_{c,c-z}\Delta_{c',S'} & \subseteq & \Delta_{\leq c,S'} \\ \uparrow & & & & \uparrow \\ \mathrm{Ann}_{S'}(a_z\otimes 1)\Delta_{\leq c-z,S'} & & \cong & & J(S') \end{array}$$

Futhermore, we have from (6.11.32) and (6.11.34)

$$K_{c',c'-w}(J^w_{c',z,S'}) = \mathrm{Ann}_{S'}(a_z \otimes 1)e_{c,c-z}\Gamma_{c',c'-w,S'}.$$

From the equality

$$e_{c,c-z}K_{c',c'-w}(\delta) = i_z K_{c'-z,c'-z-w}(t_z^{\Delta}(\delta)), \quad \text{for all } \delta,$$

the isomorphism i_z then gives an isomorphism (proposition 5.7.8(iii))

$$K_{c',c'-w}(J^w_{c',z,S'}) \cong \mathrm{Ann}_{S'}(a_z \otimes 1)\Gamma_{c'-z,c'-z-w,S'}.$$

Hence by (6.11.36) the map i_z^{-1} restricts to an isomorphism of $\Delta_{c,S'}$-modules

$$i_z^{-1}|_{J_\Gamma(S')} : J_\Gamma(S') \cong \mathrm{Ann}_{S'}(a_z \otimes 1)\Gamma_{\leq c-z,S'}.$$

The commutative diagram (6.11.38) may then be extended to a commutative diagram where the vertical arrows are the obvious inclusions

$$\begin{array}{ccc} \Delta_{\leq c-z,S'} & \to & \Delta_{\leq c,S'} \\ \uparrow & & \uparrow \\ \mathrm{Ann}_{S'}(a_z\otimes 1)\Delta_{\leq c-z,S'} & \cong & J(S') \\ \uparrow & & \uparrow \\ \mathrm{Ann}_{S'}(a_z\otimes 1)\Gamma_{\leq c-z,S'} & \cong & J_\Gamma(S') \end{array} \tag{6.11.39}$$

The inclusion $\mathrm{Ann}_{S'}(a_z \otimes 1)\Gamma_{\leq c-z,S'} \subseteq \mathrm{Ann}_{S'}(a_z \otimes 1)\Delta_{\leq c-z,S'}$ fits into the commutative diagram with an exact top row, where the vertical arrows are the evident inclusions,

$$\begin{array}{ccccccc} 0 & \to & \Gamma_{\leq c-z,S'} & \to & \Delta_{\leq c-z,S'} & \to & \mathcal{H}_{c-z,S'} \to 0 \\ & & \uparrow & & \uparrow & & \\ & & \mathrm{Ann}_{S'}(a_z \otimes 1)\Gamma_{\leq c-z,S'} & \subseteq & \mathrm{Ann}_{S'}(a_z \otimes 1)\Delta_{\leq c-z,S'} & & \end{array}$$

The top row here is the standard presentation of the Heegner module $\mathcal{H}_{c-z,S'}$. As the modules $\Gamma_{\leq c-z,S'}$, $\Delta_{\leq c-z,S'}$, $\mathcal{H}_{c-z,S'}$ are finite flat S'-modules and as there is an isomorphism of $\Delta_{c,S}$-modules (see proposition 5.9.2 and corollaries 5.9.5, 5.9.6)

$$\mathrm{Ann}_{S'}(a_z \otimes 1)\mathcal{H}_{c-z,S'} \cong \mathcal{H}_{c-z,S'/(a_z \otimes 1)S'} \tag{6.11.40}$$

we obtain that the cokernel of the inclusion

$$\mathrm{Ann}_{S'}(a_z \otimes 1)\Gamma_{\leq c-z,S'} \subseteq \mathrm{Ann}_{S'}(a_z \otimes 1)\Delta_{\leq c-z,S'}$$

is $\Delta_{c,S}$-isomorphic to $\mathrm{Ann}_{S'}(a_z \otimes 1)\mathcal{H}_{c-z,S'}$. From the diagram (6.11.39) we obtain the exact sequence of $\Delta_{c,S}$-modules

$$0 \to J_\Gamma(S') \to J(S') \to \mathrm{Ann}_{S'}(a_z \otimes 1)\mathcal{H}_{c-z,S'} \to 0.$$

From the exact sequence (6.11.30), we obtain that tensoring this sequence with $- \otimes_S H^1(G,S)$ it remains exact. Hence we obtain an isomorphism of $\Delta_{c,S}$-modules

$$\frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))} \cong H^1(G,S) \otimes_S \mathrm{Ann}_{S'}(a_z \otimes 1)\mathcal{H}_{c-z,S'}.$$

As there is an isomorphism of S-modules

$$S'/(a_z \otimes 1)S' \cong (S/(a_z \otimes 1)S) \otimes_S S'$$

and $H^1(G,S)$ is a finite free S'-module (lemma 6.9.7) we obtain from corollary 5.9.5 and (6.11.40) the isomorphisms of $\Delta_{c,S}$-modules

$$\begin{aligned} \frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))} &\cong H^1(G,S) \otimes_S \mathcal{H}_{c-z,S'/(a_z \otimes 1)S'} \\ &\cong H^1(G,S) \otimes_S \mathcal{H}_{c-z,S/(a_z \otimes 1)S} \\ &\cong H^1(G,S) \otimes_S \mathrm{Ann}_S(a_z \otimes 1)\mathcal{H}_{c-z,S} \end{aligned}$$

as required.

Cases 2 and 3. Suppose one of the following:

a) $z \notin \mathrm{Supp}(c-z)$ and z is ramified in K/F;

b) $z \notin \mathrm{Supp}(c-z)$ and z is split completely in K/F.

Suppose further in both these cases that $|P|$ is a unit of S.

We treat these two cases simultaneously. Let $\mathfrak{m}_z$ be the ideal of A defining z.

Let $c' \leq c$ be a divisor of $\mathrm{Div}_+(A)$ such that $c' \not\leq c-z$. If z is ramified in K/F, let $\mathfrak{m}'_z$ be the prime ideal of $O_{c'-z}$ lying above $\mathfrak{m}_z$. We put

$$f =< [[\mathfrak{m}'_z]]^{-1}, c'-z > .$$

Let $P_{c'}$ be the cyclic subgroup of $\mathrm{Pic}(O_{c'-z})$ generated by f. The group $P = P_c$ is, by definition, the cyclic subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the class of the ideal of O_{c-z} lying over $\mathfrak{m}'_z$. There is an evident surjective group homomorphism $P \to P_{c'}$ for all $c' \leq c$. Hence the order of the group $P_{c'}$ is prime to the residue characteristic of S.

Similarly, if z is split completely in K/F, let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be the prime ideals of $O_{c'-z}$ lying over the prime ideal $\mathfrak{m}_z$ of A. We put

$$g =< [[\mathfrak{p}_1]]^{-1}, c'-z >$$

$$h =< [[\mathfrak{p}_2]]^{-1}, c'-z > .$$

Let $P_{c'}$ be the subgroup of $\mathrm{Pic}(O_{c'-z})$ generated by g and h. The group $P = P_c$ is, by definition, the subgroup of $\mathrm{Pic}(O_{c-z})$ generated by the classes of the prime ideals of O_{c-z} lying over $\mathfrak{m}_z$. There is an evident surjective group homomorphism $P \to P_{c'}$ for all $c' \leq c$. Hence the order of $P_{c'}$ is prime to the residue characteristic of S.

Let δ be the element of $\Delta_{c'-z,S}$ defined by

$$\delta = \begin{cases} a_z \otimes 1 - f, & \text{if } z \text{ is ramified in } K/F \\ a_z \otimes 1 - g - h, & \text{if } z \text{ is split completely in } K/F. \end{cases}$$

By definition of $J_{c',z,S}$ (definition 6.7.3; see also theorem 6.7.16) we have

$$J_{c',z,S} = \mathrm{Ann}_{e_{c,c-z}\Delta_{c',S}}(\delta).$$

Let κ be the residue field of S' and let π be a local parameter of S'. As in (6.7.51) and (6.7.52), we have in both instances (a) and (b) above that $J_{c',z,S'}$ is $\Delta_{c,S}$-isomorphic to

$$\bigoplus_{\chi} \mathrm{Ann}_{\Delta_{c'-z,S'}(\chi)}(\delta) \tag{6.11.41}$$

where the sum runs over all the irreducible representations $\chi : P_{c'} \to \mathrm{GL}_n(\kappa)$ of $P_{c'}$ and where $\Delta_{c'-z,S'}(\chi)$ is the χ-isotypical component of $e_{c,c-z}\Delta_{c',S'}$ (see (6.7.15)). In case (a) where z is ramified in K/F and $\delta = a_z \otimes 1 - f$, the component $\mathrm{Ann}_{\Delta_{c'-z,S'}(\chi)}(\delta)$ is non-zero for at most one irreducible representation χ.

As any irreducible representation $\chi : P_{c'} \to \mathrm{GL}_n(\kappa)$ induces an irreducible representation $\chi : P \to \mathrm{GL}_n(\kappa)$ by composition with the homomorphism $P \to P_{c'}$, in the formula (6.11.41) the representations χ may be allowed to run over all irreducible representations of P over κ.

By (6.7.15) and (6.7.28) we have

$$S'[P_{c'}] \cong \bigoplus_{\chi} S'(\chi, c')$$

where $S'(\chi, c')$ is the χ-isotypical component of $S'[P_{c'}]$. The S'-algebra $S'(\chi, c')$ is an infinitesimal trait with the same local parameter as S' and whose residue field is a finite separable extension $\kappa(\chi)$ of the residue field κ of S'; in fact $S'(\chi, c')$ is a finite étale S'-algebra. For each irreducible representation χ of P over κ, there is a group homomorphism

$$\chi : P \to \kappa(\chi)^*$$

where $\kappa(\chi)$ is a finite separable extension field of κ and the character of this representation χ is a trace of the form $\mathrm{Tr}_{\kappa(\chi)/\kappa}(\chi)$.

The algebra $S'[P_{c'}]$ acts on the module $S'(\chi, c')$. We have that

$$\mathrm{Ann}_{S'(\chi,c')}(\delta)$$

is an ideal of the algebra $S'(\chi, c')$ and hence is of the form $\pi^m S'(\chi, c')$ for some integer $m \geq 0$ where π is a local parameter of S'; hence there is an ideal $I(\chi)$ of S' such that we have the equality of ideals of $S'(\chi, c')$

$$I(\chi)S'(\chi, c') = \mathrm{Ann}_{S'(\chi,c')}(\delta).$$

The ideal $I(\chi)$ of S' is independent of the divisor c' and depends only on the representation χ of P over κ. For if $\chi : P \to \mathrm{GL}_n(\kappa)$ is an irreducible representation of P over κ and $c' \leq c$, $c' \not\leq c - z$, is a divisor such that the homomorphism χ factors through the surjective homomorphism $P \to P_{c'}$ then the χ-isotypical component $S'(\chi, c')$ of $S'[P_{c'}]$ is $S[P]$-isomorphic to the χ-isotypical component $S'(\chi, c)$ of $S'[P]$. Hence there is an isomorphism of $S[P]$-modules, as required,

$$\mathrm{Ann}_{S'(\chi,c')}(\delta) \cong \mathrm{Ann}_{S'(\chi,c)}(\delta).$$

The module $\Delta_{c'-z,S'}(\chi)$ is a direct sum of copies of $S'(\chi, c')$; more precisely, we obtain an isomorphism of $\Delta_{c,S}$-modules

$$\Delta_{c'-z,S'}(\chi) \cong \bigoplus_{h \in \mathrm{Pic}(O_{c'-z})/P_{c'}} hS'(\chi, c')$$

where the sum $\bigoplus_{h \in \mathrm{Pic}(O_{c'-z})/P_{c'}}$ runs over a set of coset representatives of $P_{c'}$ in $\mathrm{Pic}(O_{c'-z})$. We then obtain

$$\mathrm{Ann}_{\Delta_{c'-z,S'}(\chi)}(\delta) = I(\chi)\Delta_{c'-z,S'}(\chi).$$

As there is a decomposition of $\Delta_{c,S}$-modules

$$e_{c,c-z}\Delta_{c',S'} \cong \bigoplus_{\chi} \Delta_{c'-z,S'}(\chi)$$

we then have an isomorphism of $\Delta_{c,S}$-modules

$$J_{c',z,S'} \cong \bigoplus_{\chi} I(\chi)\Delta_{c'-z,S'}(\chi) \tag{6.11.42}$$

where the sum runs over the irreducible representations $\chi : P \to \mathrm{GL}_n(\kappa)$ of P and where $I(\chi)$ is an ideal of S' for all χ which is independent of c'. We have $\Delta_{c'-z,S'}(\chi) = 0$ unless χ factors through the homomorphism $P \to P_{c'}$.

Let w be a prime divisor in $\mathrm{Supp}(c') \setminus \tilde{I}$ distinct from z. Each component $\Delta_{c'-z,S'}(\chi)$ is a finite free S'-module, as is also $e_{c,c-w}\Delta_{c'-z,S'}(\chi)$. We then have, as $I(\chi)$ is an S'-ideal

$$e_{c,c-w}\Delta_{c'-z,S'}(\chi) \cap I(\chi)\Delta_{c'-z,S'}(\chi) = e_{c,c-w}I(\chi)\Delta_{c'-z,S'}(\chi). \tag{6.11.43}$$

To prove this equality, $\Delta_{c'-z,S'}(\chi)$ is a direct summand of $\Delta_{c'-z,S'}$ and hence it is a cohomologically trivial $G(c'-z, c'-z-w)$-module. Hence $e_{c,c-w}\Delta_{c'-z,S'}(\chi)$ is the $G(c'-z, c'-z-w)$-invariant submodule of $\Delta_{c'-z,S'}(\chi)$. Hence $e_{c,c-w}\Delta_{c'-z,S'}(\chi) \cap I(\chi)\Delta_{c'-z,S'}(\chi)$ is the $G(c'-z, c'-z-w)$-invariant submodule of $I(\chi)\Delta_{c'-z,S'}(\chi)$. But we have an isomorphism of $\Delta_{c,S}$-modules

$$I(\chi)\Delta_{c'-z,S'}(\chi) \cong \Delta_{c'-z,S'/\mathrm{Ann}_{S'}(I(\chi))}(\chi);$$

hence the $G(c'-z, c'-z-w)$-invariant submodule of $I(\chi)\Delta_{c'-z,S'}(\chi)$ is equal to $e_{c,c-w}I(\chi)\Delta_{c'-z,S'}(\chi)$; this proves (6.11.43).

We have by definition of $J^w_{c',z,S'}$ for any prime divisor $w \neq z$ in $\mathrm{Supp}(c')$

$$J^w_{c',z,S'} = \{x \in e_{c,c-z}\Delta_{c',S'} \mid \ e_{c',c'-w}x \in J_{c',z,S'} \ \}.$$

It follows from (6.11.42) and (6.11.43) that if $w \neq z$

$$J^w_{c',z,S'} = e_{c,c-z}I_{c',c'-w,S'} + \bigoplus_{\chi} e_{c,c-z}I(\chi)\Delta_{c',S'}(\chi)$$

where $I_{c',c'-w,S'}$ is the augmentation ideal $\ker(t^{\Delta}_{c',c'-w,S'})$. Hence we obtain

$$K_{c',c'-w}(J^w_{c',z,S'}) = K_{c',c'-w}(\bigoplus_{\chi} I(\chi)e_{c,c-z}\Delta_{c',S'}(\chi)) \tag{6.11.44}$$

$$= \bigoplus_{\chi} I(\chi)e_{c,c-z}K_{c',c'-w}(\Delta_{c',S'}(\chi)).$$

We obtain from (6.11.42) and (6.11.44) the formulae

$$J_{\Gamma}(S') = \bigoplus_{\chi} \sum_{\substack{c'\le c \\ \text{such that } c'\not\le c-z}} \sum_{w\in \mathrm{Supp}(c')\setminus(\tilde{I}\cup\{z\}} I(\chi)e_{c,c-z}K_{c',c'-w}(\Delta_{c',S'}(\chi)) \tag{6.11.45}$$

$$\cong \bigoplus_{\chi} I(\chi)\Gamma_{\le c-z,S'}(\chi)$$

$$J(S') \cong \bigoplus_{\chi} \bigoplus_{\substack{c'\le c \\ \text{such that } c'\not\le c-z}} I(\chi)\Delta_{c'-z,S'}(\chi) \cong \bigoplus_{\chi} I(\chi)\Delta_{\le c-z,S'}(\chi) \tag{6.11.46}$$

where the sums run over the irreducible representations $\chi : P \to \mathrm{GL}_n(\kappa)$ of P over κ and where $I(\chi)$ is an ideal of S' for all χ.

The Heegner module $\mathcal{H}_{c-z,S'}$ is defined by the exact sequence

$$0 \longrightarrow \Gamma_{\le c-z,S'} \longrightarrow \Delta_{\le c-z,S'} \longrightarrow \mathcal{H}_{c-z,S'} \longrightarrow 0.$$

The group P acts on each element of this exact sequence and as $|P|$ is prime to the residue characteristic of S' we have the decomposition into isotypical components

$$0 \longrightarrow \bigoplus_{\chi} \Gamma_{\le c-z,S'}(\chi) \longrightarrow \bigoplus_{\chi} \Delta_{\le c-z,S'}(\chi) \longrightarrow \bigoplus_{\chi} \mathcal{H}_{c-z,S'}(\chi) \longrightarrow 0$$

where the sums run over the irreducible representations $\chi : P \to \mathrm{GL}_n(\kappa)$ of P. As $\Gamma_{\le c-z,S'}$, $\Delta_{\le c-z,S'}$, $\mathcal{H}_{c-z,S'}$ are flat S'-modules it follows that the χ-isotypical components $\Gamma_{\le c-z,S'}(\chi)$, $\Delta_{\le c-z,S'}(\chi)$, $\mathcal{H}_{c-z,S'}(\chi)$ are also flat S'-modules. Hence we may tensor this last exact sequence with $- \otimes_S H^1(G,S)$ and obtain the exact sequence (using lemma 6.9.7(ii)) for all χ where we write H^1 for $H^1(G,S)$

$$0 \to \Gamma_{\le c-z,S'}(\chi) \otimes_S H^1 \to \Delta_{\le c-z,S'}(\chi) \otimes_S H^1 \to \mathcal{H}_{c-z,S'}(\chi) \otimes_S H^1 \to 0. \tag{6.11.47}$$

From (6.11.30), (6.11.45) and (6.11.46), we obtain a commutative diagram of $\Delta_{c,S}$-modules with exact rows

$$\begin{array}{ccccccc} 0 \to & & J_\Gamma(S') \otimes_S H^1 & \to & J(S') \otimes_S H^1 & \stackrel{\Xi}{\to} & H^0 \to 0 \\ & & \uparrow\cong & & \uparrow\cong & & \\ 0 \to & \bigoplus_\chi I(\chi)\Gamma_{\leq c-z,S'}(\chi) \otimes_S H^1 & \to & \bigoplus_\chi I(\chi)\Delta_{\leq c-z,S'}(\chi) \otimes_S H^1 & & & \end{array}$$

where we write

$$H^1 = H^1(G, S)$$

and

$$H^0 = \frac{H^0(G, \mathcal{H}_{c,S})}{t(H^0(G, \mathcal{H}_{c-z,S}))}.$$

Comparing this diagram with the exact sequence (6.11.47) we obtain the isomorphism of $\Delta_{c,S}$-modules

$$\frac{H^0(G, \mathcal{H}_{c,S})}{t(H^0(G, \mathcal{H}_{c-z,S}))} \cong \bigoplus_\chi I(\chi)\mathcal{H}_{c-z,S'}(\chi) \otimes_S H^1(G, S). \tag{6.11.48}$$

By lemma 6.9.7(ii), the group $H^1(G, S)$ is a finite free S'-module. Furthermore, we have the decomposition of $\Delta_{c,S}$-modules

$$\mathcal{H}_{c-z,S} \cong \bigoplus_\chi \mathcal{H}_{c-z,S}(\chi)$$

hence we have by corollary 5.9.5 the isomorphism of $\Delta_{c,S}$-modules

$$\mathcal{H}_{c-z,S}(\chi) \otimes_S S' \cong \mathcal{H}_{c-z,S'}(\chi).$$

Hence we obtain from (6.11.48) the isomorphism of $\Delta_{c,S}$-modules

$$\frac{H^0(G, \mathcal{H}_{c,S})}{t(H^0(G, \mathcal{H}_{c-z,S}))} \cong \bigoplus_\chi I(\chi)\mathcal{H}_{c-z,S}(\chi) \otimes_S H^1(G, S)$$

as required.

Case 4. Suppose that $z \in \mathrm{Supp}(c - z)$.

Let c' be an effective divisor such that $c' \leq c$ and $c' \not\leq c - z$. By table 6.7.16 we have

$$J_{c',z,S'} = \mathrm{Ann}_{S'}(a_z \otimes 1)e_{c',c'-z}I_{c',c'-2z,S'}.$$

Let $x \in J^w_{c',z,S'}$ where $w \in \mathrm{Supp}(c')$ and $w \neq z$. Then we have

$$x \in e_{c,c-z}\Delta_{c',S'}$$

where

$$e_{c',c'-w}(a_z \otimes 1)x = 0 \quad \text{and} \quad e_{c',c'-w}t^{\Delta}_{c',c'-2z}(x) = 0.$$

We obtain

$$(a_z \otimes 1)x \in I_{c',c'-w,S'} \quad \text{and} \quad t^{\Delta}_{c',c'-2z}(x) \in I_{c'-2z,c'-2z-w,S'}$$

where $I_{c',c'-w,S'}$ is the augmentation ideal in $\Delta_{c',S'}$ of the subgroup $\ker(t_{c',c'-w})$; that is to say

$$I_{c',c'-w,S'} = \mathrm{Ann}_{\Delta_{c',S'}}(e_{c',c'-w}).$$

The kernel of the map of multiplication by $e_{c',c'-w}$

$$e_{c,c-z}\Delta_{c',S'} \to e_{c,c-z}\Delta_{c',S'}, \quad e_{c,c-z} \mapsto e_{c',c'-w}e_{c,c-z}$$

is equal to $e_{c,c-z}I_{c',c'-w,S'}$. The condition $(a_z \otimes 1)x \in I_{c',c'-w,S'}$, where $x \in e_{c,c-z}\Delta_{c',S}$, is then equivalent to

$$x \in e_{c',c'-z}I_{c',c'-w,S'} + \mathrm{Ann}_{S'}(a_z \otimes 1)e_{c',c'-z}\Delta_{c',S'}.$$

We then obtain

$$\begin{aligned} J^w_{c',z,S'} &= e_{c',c'-z}I_{c',c'-w,S'} + \mathrm{Ann}_{S'}(a_z \otimes 1)e_{c',c'-z}I_{c',c'-2z,S'} \\ &= e_{c',c'-z}I_{c',c'-w,S'} + J_{c',z,S'}. \end{aligned}$$

We have by definition (see (5.3.6))

$$K_{c',c'-w}(x) = (a_w - \epsilon(c',w))t^{\Delta}_{c',c'-w}(x) - \frac{|O^*_{c'-w}|}{|A^*|}e_{c',c'-w}x.$$

Hence we have

$$K_{c',c'-w}(e_{c',c'-z}I_{c',c'-w,S'}) = 0$$

and therefore we obtain

$$\begin{aligned} K_{c',c'-w}(J^w_{c',z,S'}) &= K_{c',c'-w}(J_{c',z,S'}) \\ &= I_{c',c'-2z,S'}\mathrm{Ann}_{S'}(a_z \otimes 1)e_{c',c'-z}\Gamma_{c',c'-w,S'}. \end{aligned}$$

As we have

$$I_{c,c-2z,S'}\Delta_{c',S'} = I_{c',c'-2z,S'} \quad \text{for } c' \not\leq c - z,$$

we then obtain the equalities of submodules of $\Delta_{\leq c,S'}$

(6.11.49)

$$J_\Gamma(S') = I_{c,c-2z,S'}\mathrm{Ann}_{S'}(a_z \otimes 1)e_{c,c-z} \sum_{\substack{c'\leq c \\ \text{such that } c'\not\leq c-z}} \sum_{\substack{w\in \mathrm{Supp}(c')\setminus \tilde{I} \\ w\neq z}} \Gamma_{c',c'-w,S'}$$

and

$$J(S') = I_{c,c-2z,S'}\mathrm{Ann}_{S'}(a_z \otimes 1)e_{c,c-z} \sum_{\substack{c'\leq c \\ \text{such that } c'\not\leq c-z}} \Delta_{c',S'}. \tag{6.11.50}$$

The family of isomorphisms, which are compatible with all restriction maps $t^{\Delta}_{c',c'-w}$,

$$e_{c,c-z}\Delta_{c',S'} \cong \Delta_{c'-z,S'}$$

induces by restriction a family of isomorphisms of $\Delta_{c,S'}$-modules, for $w \neq z$,

$$e_{c,c-z}\Gamma_{c',c'-w,S'} \cong \Gamma_{c'-z,c'-z-w,S'}$$

which are compatible with the restriction maps $t^{\Delta}_{c',c'-w}$, for all w and c'. Hence we obtain an isomorphism of $\Delta_{c,S'}$-modules

$$J_\Gamma(S') \cong I_{c,c-2z,S'}\mathrm{Ann}_{S'}(a_z \otimes 1) \sum_{\substack{c'\leq c-z \\ \text{such that } c'\not\leq c-2z}} \sum_{\substack{w\in \mathrm{Supp}(c')\setminus \tilde{I} \\ w\neq z}} \Gamma_{c',c'-w,S'}.$$

Put

$$S'' = S'/(a_z \otimes 1).$$

We further obtain that the isomorphism

$$\mathrm{Ann}_{S'}(a_z \otimes 1)\Delta_{c',S'} \cong \Delta_{c',S''}$$

induces by restriction an isomorphism of $\Delta_{c,S'}$-modules

$$\mathrm{Ann}_{S'}(a_z \otimes 1)\Gamma_{c',c'-w,S'} \cong \Gamma_{c',c'-w,S''}.$$

Hence we have a commutative diagram of $\Delta_{c,S}$-modules compatible with the obvious inclusions in $\Delta_{\leq c,S'}$ and in $\Delta_{\leq c,S''}$, where the horizontal maps are isomorphisms and the vertical maps are inclusions,

(6.11.51)

$$\begin{array}{ccc} J_\Gamma(S') & \cong & I_{c,c-2z,S''} \sum_{\substack{c'\leq c-z \\ \text{such that } c'\not\leq c-2z}} \sum_{\substack{w\in \mathrm{Supp}(c')\setminus \tilde{I} \\ w\neq z}} \Gamma_{c',c'-w,S''} \\ \downarrow & & \downarrow \\ J(S') & \cong & I_{c,c-2z,S''} \sum_{\substack{c'\leq c-z \\ \text{such that } c'\not\leq c-2z}} \Delta_{c',S''} \end{array}$$

As in (6.1.1), let $\mathcal{H}_c$ be the Heegner module attached to

$$\rho : \Sigma_F \setminus \tilde{I} \quad \to \quad R, \quad v \mapsto a_v,$$

with coefficients in R. Let

$$\rho^* : \Sigma_F \setminus (\tilde{I} \cup \{z\}) \quad \to \quad R, \ v \mapsto a_v,$$

be the restriction of ρ to the subset $\Sigma_F \setminus (\tilde{I} \cup \{z\})$. Let $\mathcal{H}_c^*$ be the Heegner module attached to ρ^* with coefficients in R. Let $\mathit{\Gamma}^*_{\leq c-z}$ be the module $\mathit{\Gamma}_{\leq c-z}$ where the exceptional set of primes is taken to be $\tilde{I} \cup \{z\}$ in place of $\tilde{I}$ (see (5.3.7)).

Put

$$\tilde{\mathit{\Gamma}}_{c,S''} = \sum_{\substack{c' \leq c \\ \text{such that } c' \not\leq c-z}} \ \sum_{\substack{w \in \mathrm{Supp}(c') \setminus \tilde{I} \\ w \neq z}} \mathit{\Gamma}_{c',c'-w,S''}.$$

We obtain an equality of $\mathit{\Delta}_{c,S}$-modules

$$\mathit{\Gamma}^*_{\leq c-z,S''} = \bigoplus_{n=1}^{t} \tilde{\mathit{\Gamma}}_{c-nz,S''} \quad \text{where } t = \mathrm{ord}_z(c).$$

Let

$$\pi_{c-z} : \mathit{\Delta}_{\leq c-z,S} \to \bigoplus_{c' \leq c-z, \ c' \not\leq c-2z} \mathit{\Delta}_{c',S}$$

be the projection homomorphism onto the submodule $\bigoplus_{c' \leq c-z, \ c' \not\leq c-2z} \mathit{\Delta}_{c',S}$ of $\mathit{\Delta}_{\leq c-z,S}$ with kernel $\mathit{\Delta}_{\leq c-2z,S}$. Then π_{c-z} induces a projection homomorphism denoted by the same symbol

$$\pi_{c-z} : \mathit{\Gamma}^*_{\leq c-z,S''} \to \tilde{\mathit{\Gamma}}_{c-z,S''}.$$

We then obtain (from (6.11.51)) an isomorphism of $\mathit{\Delta}_{c,S}$-modules

$$J_{\mathit{\Gamma}}(S') \cong I_{c,c-2z,S'} \pi_{c-z}(\mathit{\Gamma}^*_{\leq c-z,S''}). \tag{6.11.52}$$

As above, the projection homomorphism

$$\pi_{c-z} : \mathit{\Delta}_{\leq c-z,S} \to \bigoplus_{c' \leq c-z, \ c' \not\leq c-2z} \mathit{\Delta}_{c',S}$$

induces a projection homomorphism denoted by the same symbol

$$\pi_{c-z} : \mathcal{H}^*_{c-z,S''} \to \mathcal{H}^*_{c-z,S''}.$$

By proposition 6.11.1, we have the equality

$$L(S'') \cap J(S'') = J_{\mathit{\Gamma}}(S'') \tag{6.11.53}$$

where

$$L(S'') = \sum_{c' \leq c, c' \not\leq c-z} \ \sum_{\substack{w \in \mathrm{Supp}(c') \setminus \tilde{I} \\ w \neq z}} e_{c,c-z} \mathit{\Gamma}_{c',c'-w,S''} \ \cong \ \tilde{\mathit{\Gamma}}_{c-z,S''}.$$

We have the commutative diagram of $\Delta_{c,S}$-modules with exact rows (see the isomorphisms (6.11.49))

(6.11.54)

$$\begin{array}{ccccccc} 0 \to \tilde{\Gamma}_{c-z,S''} & \to & \sum_{\substack{c' \leq c-z \\ \text{such that } c' \not\leq c-2z}} \Delta_{c',S''} & \to & \pi_{c-z}(\mathcal{H}^*_{c-z,S''}) \to 0 \\ f_\Gamma \uparrow & & f \uparrow & & \\ 0 \to J_\Gamma(S') & \to & J(S') & & \end{array}$$

where the vertical homomorphisms f_Γ, f are the natural injections induced by

$$J(S') \cong I_{c,c-2z,S'} \sum_{\substack{c' \leq c-z \\ \text{such that } c' \not\leq c-2z}} \Delta_{c',S''} \subseteq \sum_{\substack{c' \leq c-z \\ \text{such that } c' \not\leq c-2z}} \Delta_{c',S''}.$$

From (6.11.53), we obtain

$$\tilde{\Gamma}_{c-z,S''} \cap f(J(S')) = f_\Gamma(J_\Gamma(S')).$$

Hence from the above commutative diagram (6.11.54) we obtain that the kernel of the composite homomorphism

$$J(S') \to \pi_{c-z}(\mathcal{H}^*_{c-z,S''})$$

is equal to $J_\Gamma(S')$; furthermore, the image of this latter homomorphism is evidently equal to $I_{c,c-2z,S'}\pi_{c-z}(\mathcal{H}^*_{c-z,S''})$ (from the isomorphisms (6.11.51)). Hence we obtain the exact sequence

$$0 \to J_\Gamma(S') \to J(S') \to I_{c,c-2z,S'}\pi_{c-z}(\mathcal{H}^*_{c-z,S''}) \to 0.$$

By (6.11.30), tensoring this previous exact sequence with $- \otimes_S H^1(G,S)$ it remains exact and we obtain the exact sequence, where $H^1 = H^1(G,S)$,

$$0 \to J_\Gamma(S') \otimes_S H^1 \to J(S') \otimes_S H^1 \to I_{c,c-2z,S'}\pi_{c-z}(\mathcal{H}^*_{c-z,S''}) \otimes_S H^1 \to 0.$$

From this and (6.11.30), we obtain the isomorphism of $\Delta_{c,S}$-modules

$$\frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))} \cong I_{c,c-2z,S'}\pi_{c-z}(\mathcal{H}^*_{c-z,S''}) \otimes_S H^1(G,S).$$

As we have isomorphisms of $\Delta_{c,S}$-modules (corollary 5.9.5)

$$\mathcal{H}^*_{c-z,S''} \cong \mathrm{Ann}_S(a_z \otimes 1)\mathcal{H}^*_{c-z,S} \otimes_S S', \quad I_{c,c-2z,S'} \cong I_{c,c-2z,S}\Delta_{c,S'}$$

we obtain the isomorphism of $\Delta_{c,S}$-modules in this case where $z \in \mathrm{Supp}(c-z)$

$$\frac{H^0(G,\mathcal{H}_{c,S})}{t(H^0(G,\mathcal{H}_{c-z,S}))} \cong I_{c,c-2z,S}\mathrm{Ann}_S(a_z \otimes 1)\pi_{c-z}(\mathcal{H}^*_{c-z,S}) \otimes_S H^1(G,S).$$

This completes the proof of theorem 6.10.7.□

7

Finiteness of Tate-Shafarevich groups

Let E/F be an elliptic curve with split multiplicative reduction at ∞, with the notation of §2.1 of Chapter 2. In this chapter we extend the main result on the Tate conjecture for the elliptic surface corresponding to E proved in [Br2] to general global fields of positive characteristic; we also eliminate some of the technical hypotheses contained therein.

The point is to prove the finiteness of the l-primary component of the Tate-Shafarevich group $Ш(E/F)$ of the elliptic curve E/F for at least one prime number l; this then implies both the finiteness of the group $Ш(E/F)$ and the Tate conjecture for the corresponding elliptic surface by known results on étale cohomology (due to Artin, Tate, and Milne).

The contents of this chapter are the following. After some preliminaries on quasi-groups in §7.1, Igusa's determination of the galois action on torsion points of an elliptic curve over a global field of positive characteristic is presented in §§7.2-7.4, as well as some of its consequences. Further preliminaries are given in §§7.5-7.12 on the Tate conjecture.

The Heegner module $\mathcal{H}_{c,S}$ of the elliptic curve E/F is introduced in §7.12; in §7.13 the determination of the galois invariants of the Heegner module (theorem 6.10.7) provides a homomorphism

$$\eta : \mathcal{H}_{c,S} \otimes_S M(c) \to (\mathcal{H}_{c,S})^{G(c/0)}$$

(see proposition 7.13.4 for the notation) for the case where the primes components of c are distinct, inert, and unramified in K/F and where $S = \mathbb{Z}/l^n\mathbb{Z}$ for a suitable prime number l. The parametrisation of the elliptic curve E by the Drinfeld modular curve $X_0^{\mathrm{Drin}}(I)$, where I is the conductor of E without the component at ∞, provides the homomorphism

$$(\mathcal{H}_{c,S}^{(0)})^{G(c/0)} \to H^1(K, E)$$

M.L. Brown: LNM 1849, pp. 329–434, 2004.

whose domain is the galois invariant part of the Heegner module. If c is prime to the conductor I, composing this map with η gives a homomorphism

$$\mathcal{H}_{c,S} \otimes_S M(c) \to H^1(K, E)$$

whose image is a principal S-module generated by a cohomology class $\delta(c)$ in $H^1(K, E)$ (lemma 7.14.9, notation 7.14.10). It is these cohomology classes $\delta(c)$, whose properties are considered in §7.14, that provide annihilators by duality (Tate-Poitou duality §§7.15-7.16 and Pontrjagin duality §7.17) of the Tate-Shafarevich group $\text{Ш}(E/F)$ in §7.18; this suffices to prove the finiteness of the l-primary component of the Tate-Shafarevich groups for a set of prime numbers l of positive Dirichlet density.

7.1 Quasi-modules

In this section we introduce quasi-modules, trival quasi-modules, and quasi-isomorphisms.

Partially ordered sets and quasi-modules

(7.1.1) Let Λ be a set equipped with a partial order written $\succeq$, that is to say $\succeq$ is reflexive, transitive, and verifies the condition: if $x \succeq y$ and $y \succeq x$ then $x = y$.

Let Λ_{cat} be the category associated to Λ; that is, there is a bijection between Λ and the objects of Λ_{cat} noted

$$\Lambda \to \text{Ob}(\Lambda_{\text{cat}}), \quad x \to [x],$$

and there is a unique arrow $[x] \to [y]$ between two objects $[x], [y]$ of Λ_{cat} if and only if $x \succeq y$.

7.1.2. Examples. The main examples of partially ordered sets Λ that we consider are these.
(i) Let R be a commutative ring. Let $\{I_\lambda\}_{\lambda \in \Lambda}$ be a family of ideals of R partially ordered by inclusion; that is to say, for $\lambda_1, \lambda_2 \in \Lambda$ we have $\lambda_1 \succeq \lambda_0$ if and only if $I_{\lambda_1} \subseteq I_{\lambda_0}$.

(ii) Let Λ be the set

$$\mathcal{P} = \{p^n |\ p \text{ is a prime number and } n \in \mathbb{N}\}$$

the set of all prime powers of $\mathbb{N}$ where the partial order is given by divisibility: $p^a \succeq q^b$ if and only if $q^b | p^a$.

This is a special case of the example of (i), where we identify a prime power p^n with the ideal $p^n\mathbb{Z}$ of the ring $\mathbb{Z}$. The partially ordered set $\mathcal{P}$ is isomorphic to the partially ordered set of non-zero primary ideals of $\mathbb{Z}$ ordered by inclusion.

(iii) Let Λ be the set $\mathbb{N}^*$ of all non-zero natural numbers where the partial order is given by divisibility.

This is also a special case of the example of (i), where we identify a positive integer n with the ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$. The partially ordered set $\mathbb{N}^*$ is then isomorphic to the partially ordered set of non-zero ideals of $\mathbb{Z}$ ordered by inclusion.

7.1.3. Definition. Let R be a commutative ring and $\{I_\lambda\}_{\lambda\in\Lambda}$ be a family of ideals of R which are partially ordered by inclusion (as in example 7.1.2(i)). A *quasi-module G over R with respect to* $\{I_\lambda\}_{\lambda\in\Lambda}$ is a family

$$G = \{G_\lambda\}_{\lambda\in\Lambda}$$

of R-modules G_λ indexed by Λ such that for each pair of comparable elements $\lambda_1 \succeq \lambda_0$ there is an R-module *transition homomorphism*

$$f_{\lambda_1\lambda_0} : G_{\lambda_1} \to G_{\lambda_0}$$

and each module G_λ is annihilated by the ideal I_λ:

$$I_\lambda G_\lambda = 0 \quad \text{for all } \lambda \in \Lambda.$$

Furthermore, the maps $f_{\lambda_1\lambda_0}$ satisfy the compatibility condition that if $\lambda_2 \succeq \lambda_1 \succeq \lambda_0$ are elements of Λ then the diagram

$$\begin{array}{ccc} G_{\lambda_1} & \overset{f_{\lambda_1\lambda_0}}{\longrightarrow} & G_{\lambda_0} \\ {\scriptstyle f_{\lambda_2\lambda_1}}\nwarrow & & \nearrow{\scriptstyle f_{\lambda_2\lambda_0}} \\ & G_{\lambda_2} & \end{array}$$

is commutative.

If $R = \mathbb{Z}$ we speak of a *quasi-group* instead of a quasi-module over $\mathbb{Z}$.

7.1.4. Definition. A *homomorphism $h : G \to H$ of quasi-modules over R*, with respect to $\{I_\lambda\}_{\lambda\in\Lambda}$, is a family of R-module homomorphisms

$$h_\lambda : G_\lambda \to H_\lambda, \text{ for all } \lambda \in \Lambda$$

such that for every pair of comparable elements $\lambda_1 \succeq \lambda_0$ there is a commutative diagram of R-module homomorphisms

$$\begin{array}{ccc} & {\scriptstyle f_{\lambda_1\lambda_0}} & \\ G_{\lambda_1} & \to & G_{\lambda_0} \\ {\scriptstyle h_{\lambda_1}}\downarrow & & \downarrow{\scriptstyle h_{\lambda_0}} \\ H_{\lambda_1} & \to & H_{\lambda_0} \\ & {\scriptstyle g_{\lambda_1\lambda_0}} & \end{array}$$

The homomorphism h is an *isomorphism* of quasi-modules if the h_λ are isomorphisms for all $\lambda \in \Lambda$. The quasi-modules over R with respect to $\{I_\lambda\}_{\lambda\in\Lambda}$ form a category noted $[\{I_\lambda\}_{\lambda\in\Lambda}]_R$ or more simply $[\Lambda]_R$.

(7.1.5) Let $h : G \to H$ be a homomorphism of quasi-R-modules in $[\Lambda]_R$.

The *kernel* of h is defined as a quasi-module in the evident way, namely

$$\ker(h) = \{\ker(h_\lambda)\}_{\lambda\in\Lambda}$$

where the transition homomorphisms are given by restriction of the transition homomorphisms of G.

The *cokernel* of $h : G \to H$ is defined as a quasi-R-module by

$$\mathrm{coker}(h) = \{\mathrm{coker}(h_\lambda)\}_{\lambda\in\Lambda}$$

where the transition homomorphisms are the quotients of the transition homomorphisms of H.

One may check that $[\Lambda]_R$ is an abelian category.

(7.1.6) Let $R-\mathbf{mod}$ be the category of R-modules. Then the category of quasi-R-modules $[\{I_\lambda\}_{\lambda\in\Lambda}]_R$ is equivalent to the category of covariant functors

$$\mathcal{F} : \Lambda_{\mathrm{cat}} \to R - \mathbf{mod}$$

such that for all $\lambda \in \Lambda$ we have

$$I_\lambda \mathcal{F}(\lambda) = 0.$$

7.1.7. Examples. (1) Consider the category $[\Lambda]_{\mathbb{Z}}$ of quasi-groups where Λ is a subset of $\mathbb{N}^*$ with the partial order given by divisibility, and in particular the categories $[\mathbb{N}^*]_{\mathbb{Z}}$, $[\mathcal{P}]_{\mathbb{Z}}$.

An element of $[\Lambda]_{\mathbb{Z}}$ is a family

$$G = \{G_n\}_{n\in\Lambda}$$

of abelian groups G_n indexed by the elements of Λ such that for each pair of integers $m, n \in \Lambda$ such that $m|n$ there is a homomorphism of abelian groups

$$f_{nm} : G_n \to G_m$$

and each abelian group G_n is annihilated by n for all $n \in \Lambda$. Furthermore, the transition homomorphisms satisfy the compatibility condition

$$f_{nm} \circ f_{pn} = f_{pm}$$

whenever $m|n$ and $n|p$.

(2) Let Λ be a subset of $\mathbb{N}^*$ and $[\Lambda]_{\mathbb{Z}}$ the corresponding category of quasi-groups. Let A be an abelian group and for each $n \in \Lambda$ put

$$ {}_nA = A \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} $$

$$ A_n = \ker(A \xrightarrow{n} A) $$

where A_n denotes the subgroup of A of elements annihilated by n. Then

$$ {}_*A = \{{}_nA\}_{n\in\Lambda} $$

$$ A_* = \{A_n\}_{n\in\Lambda} $$

are quasi-groups associated to A which are denoted ${}_*A$ and A_* respectively.

If A, B, C are abelian groups fitting into an exact sequence

$$ 0 \to A \to B \to C \to 0 $$

then the snake lemma gives an exact sequence of quasi-groups in $[\Lambda]_{\mathbb{Z}}$, where the index runs over the integers in Λ,

$$ 0 \to A_* \to B_* \to C_* \to {}_*A \to {}_*B \to {}_*C \to 0. $$

(3) Let E/L be an elliptic curve over a field L and let Λ be a subset of $\mathbb{N}^*$. If the characteristic p of L is positive, we assume that the integral powers of p are excluded from Λ. Let $\mathcal{E}$ denote the sheaf of abelian groups for the étale topology on Spec L induced by E.

Then we have these quasi-groups attached to E:

$$ \{E(L)_n\}_{n\in\Lambda} $$

$$ \{E(L)/nE(L)\}_{n\in\Lambda} $$

$$ \{H^1_{\text{ét}}(\mathrm{Spec}(L), \mathcal{E})_n\}_{n\in\Lambda} $$

$$ \{H^1_{\text{ét}}(\mathrm{Spec}(L), \mathcal{E})/nH^1_{\text{ét}}(\mathrm{Spec}(L), \mathcal{E})\}_{n\in\Lambda} $$

$$ \{H^1_{\text{ét}}(\mathrm{Spec}(L), \mathcal{E}_n)\}_{n\in\Lambda}. $$

Quasi-constants

7.1.8. Definition. Let Λ be a partially ordered subset of $\mathbb{N}^*$, which is ordered by divisibility; this partial order is written $\succeq$. A function

$$ \gamma : \Lambda \to \mathbb{N} $$

is called *quasi-constant* if

(i) $\gamma(\Lambda)$ is a finite subset of $\mathbb{N}$;

(ii) for some finite set $\mathcal{S}$ of prime numbers and for all $n \in \Lambda$ coprime to all elements of $\mathcal{S}$ we have $\gamma(n) \leq 1$.

7.1.9. Remarks. (i) It is evident that a function $\gamma : \Lambda \to \mathbb{N}$ is quasi-constant if and only if there is a quasi-constant $\Gamma : \mathbb{N}^* \to \mathbb{N}$ which extends γ, that is to say $\Gamma|_\Lambda = \gamma$.

(ii) Let $\gamma, \delta : \mathbb{N}^* \to \mathbb{N}$ be functions such that $0 \leq \gamma \leq \delta$ and δ is quasi-constant. Then γ is quasi-constant.

(iii) A function $\gamma : \mathbb{N}^* \to \mathbb{N}$ is quasi-constant if and only if there is a function $\delta : \mathbb{N}^* \to \mathbb{N}$ such that

(a) $0 \leq \gamma \leq \delta$;

(b) δ is multiplicative: $\delta(mn) = \delta(m)\delta(n)$ whenever the integers m, n are coprime;

(c) $\delta(p^n) = 1$ for all $n \in \mathbb{N}$ and for all except finitely many prime numbers p;

(d) for all prime numbers p, $\delta(p^n)$ is bounded as $n \to +\infty$.

Clearly, a function δ satisfying these conditions is also quasi-constant.

(iv) A function $\delta : \mathbb{N}^* \to \mathbb{N}$ satisfies conditions (b),(c), and (d) of the remark (iii) above if and only if δ is multiplicative and bounded.

Hence a map $\gamma : \mathbb{N}^* \to \mathbb{N}$ is quasi-constant if and only if it is majorised by a bounded multiplicative function.

Trivial quasi-groups. Quasi-isomorphisms.

Let Λ be a partially ordered subset of $\mathbb{N}^*$.

7.1.10. Definition. A quasi-group G of $[\Lambda]_{\mathbb{Z}}$ is *finite* if all G_n, for all $n \in \Lambda$, are finite abelian groups and their order is bounded independently of n.

7.1.11. Definition. A quasi-group G of $[\Lambda]_{\mathbb{Z}}$ is *trivial* if G is finite and the map $n \mapsto |G_n|$, $\Lambda \to \mathbb{N}$, is quasi-constant.

7.1.12. Remarks. (i) A quasi-group G of $[\Lambda]_{\mathbb{Z}}$ is trivial if and only if there is a bounded multiplicative function $\gamma : \Lambda \to \mathbb{Z}$ such that

$$|G_n| \leq \gamma(n) \quad \text{for all } n \in \Lambda.$$

[See remarks 7.1.9 (ii), (iii), (iv).]

(ii) A quasi-group G of $[\Lambda]_{\mathbb{Z}}$ is trivial if and only if these conditions hold:

(a) there is a finite set $\mathcal{S}$ of prime numbers such that for all $n \in \Lambda$ coprime to all elements of $\mathcal{S}$ the group G_n is trivial;
(b) G is finite.

7.1.13. Definition. A homomorphism of quasi-groups $f : G \to H$ of $[\Lambda]_{\mathbb{Z}}$ is a *quasi-isomorphism* if the kernel and cokernel of f are trivial quasi-groups of $[\Lambda]_{\mathbb{Z}}$.

7.1.14. Examples. (1) For any finitely generated $\mathbb{Z}$-module A let $m(A)$ denote the minimal number of generators of A. Let M be a finitely generated $\mathbb{Z}[G]$-module where G is a finite group. Then the order of the finite Tate cohomology group $\hat{H}^i(G, M)$ is bounded by

$$|\hat{H}^i(G, M)| \leq |G|^{m(M)|G|^{|i|}} \quad \text{for all } i \ \in \mathbb{Z}.$$

[We prove this by induction on i. We have that $\hat{H}^0(G, M)$ is a quotient of M^G which is annihilated by $|G|$. Hence $\hat{H}^0(G, M)$ has at most $|G|^{m(M)}$ elements, which proves the result for $i = 0$.

Assume the result has been proved for all M and for an index $i \geq 0$. The G-module M is a submodule of the coinduced module $N = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$; the action of G on N is given by: if $\phi \in N$ then $g.\phi$ is the homomorphism

$$g' \mapsto \phi(g'g), \quad \mathbb{Z}[G] \to M.$$

We have the short exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to M \to N \to M' \to 0$$

which is split exact as a sequence of $\mathbb{Z}$-modules and where the injection $M \to N$ is given by

$$m \mapsto \{\phi_m : g \mapsto gm\}.$$

The long exact sequence of cohomology of this sequence provides isomorphisms

$$\hat{H}^i(G, M') \cong \hat{H}^{i+1}(G, M)$$

for all $i \in \mathbb{Z}$, as $\hat{H}^i(G, N) = 0$ for all i by Shapiro's lemma. Evidently, we have

$$m(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)) \leq m(M)|G|.$$

Hence we have

$$m(M') \leq m(M)|G|.$$

But we then have

$$|\hat{H}^{i+1}(G, M)| = |\hat{H}^i(G, M')| \leq |G|^{m(M')|G|^i} \leq |G|^{m(M)|G|^{i+1}}.$$

This proves the result for all $i \geq 0$ by ascending induction on $i \geq 0$.

Assume now that the result has been proved for an index $i \leq 0$. Then we may argue similarly as follows. The G-module M is a quotient module of the induced module $N' = \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$; the action of G on N' is given by: $g(a \otimes m) = (ga) \otimes m$, for $a \in \mathbb{Z}[G], m \in M$. In fact the $\mathbb{Z}[G]$-modules N, N' are isomorphic where the isomorphism is given by

$$N \to N', \quad \phi \mapsto \sum_{g \in G} g \otimes \phi(g).$$

We have the short exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to M'' \to N' \to M \to 0$$

where the surjection $N' \to M$ is given by

$$\sum_j a_j \otimes m_j \mapsto \sum a_j m.$$

The long exact sequence of cohomology of this sequence provides isomorphisms

$$\hat{H}^i(G, M'') \cong \hat{H}^{i-1}(G, M)$$

for all $i \in \mathbb{Z}$, as $\hat{H}^i(G, N') = 0$ for all i. As $m(N') \leq m(M)|G|$ we have

$$m(M'') \leq m(M)|G|.$$

As $i \leq 0$ we then obtain

$$|\hat{H}^{i-1}(G, M)| = |\hat{H}^i(G, M'')| \leq |G|^{m(M'')|G|^{|i|}} \leq |G|^{m(M)|G|^{|i|+1}}.$$

This proves the result for all $i \leq 0$ by descending induction on $i \leq 0$.]

(2) Let M be a finitely generated $\mathbb{Z}[G]$-module where G is a finite group. Then for all $i \geq 1$

$$\{H^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z})\}_{n \in \mathbb{N}^*}$$

and

$$\{H^i(G, M_n)\}_{n\in\mathbb{N}^*}$$

are trivial quasi-groups.

[With the notation of example (1) above, we have evidently

$$m(M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \leq m(M)$$

and

$$m(M_n) \leq m(M)$$

for all integers $n \geq 1$. The cohomology groups $H^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z})$, $H^i(G, M_n)$ coincide with the Tate cohomology groups $\hat{H}^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z})$, $\hat{H}^i(G, M_n)$ for all $i \geq 1$. Hence by example (1) above, we have that the orders of the groups $H^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z})$, $H^i(G, M_n)$, are for all $n \geq 1$ bounded by $|G|^{m(M)|G|^i}$ which is independent of n. Furthermore, $H^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z})$ and $H^i(G, M_n)$ are both annihilated by $|G|$ for all $i \geq 1$; hence we have for all $i \geq 1$

$$H^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) = H^i(G, M_n) = 0$$

for all non-zero integers n prime to $|G|$. Hence, for $i \geq 1$, $\{H^i(G, M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z})\}_{n\in\mathbb{N}^*}$ and $\{H^i(G, M_n)\}_{n\in\mathbb{N}^*}$ are trivial quasi-groups, as required.]

(3) Let E be an elliptic curve defined over a finite field k of characteristic $p > 0$. Let $\mathbb{N}^{(p)}$ be the set of positive integers prime to p. Then $\{H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), E_n)\}_{n\in\mathbb{N}^{(p)}}$ is a trivial quasi-group.

[For the proof, we have the exact sequence of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-modules obtained by multiplication by n

$$0 \to E_n(k^{\mathrm{sep}}) \to E(k^{\mathrm{sep}}) \xrightarrow{n} E(k^{\mathrm{sep}}) \to 0$$

where $E_n(k^{\mathrm{sep}})$ is the submodule of n-torsion points of $E(k^{\mathrm{sep}})$. The associated long exact sequence of cohomology gives the isomorphism

$$H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), E_n) \cong E(k)/nE(k)$$

because

$$H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), E) = 0$$

by the theorem of Lang. As $E(k)$ is a finite abelian group the result immediately follows.]

(4) Let

$$0 \to H_1 \to H_2 \to H_3 \to 0$$

be a short exact sequence of quasi-groups in $[\mathbb{N}^*]_{\mathbb{Z}}$.

(i) If two of these quasi-groups are trivial then so is the third.

(ii) If H_2 is a trivial quasi-group then so are H_1 and H_3.

(5) Suppose that Λ is a subset of $\mathbb{N}^*$ with its usual partial order by divisibility. Let $\{E_{2,n}^{i,j}\}_{n\in\Lambda}$ for all integers $i, j \geq 0$ be quasi-groups. Suppose for each $n \in \Lambda$ there is a (convergent first quadrant) spectral sequence of abelian groups

$$E_{2,n}^{i,j} \Rightarrow E_n^{i+j}.$$

If E_n^i is annihilated by n for all i, then we have:

(i) the $\{E_n^i\}_{n\in\Lambda}$ are quasi-groups in $[\Lambda]_{\mathbb{Z}}$;

(ii) if $\{E_{2,n}^{i,j}\}_{n\in\Lambda}$ are trivial quasi-groups for all integers i, j then for all i the quasi-group $\{E_n^i\}_{n\in\Lambda}$ is trivial in $[\Lambda]_{\mathbb{Z}}$.

[For the proof, part (i) follows immediately. For part (ii), the differentials of the spectral sequence

$$E_{2,n}^{i,j} \Rightarrow E_n^{i+j}.$$

are given by

$$d_{r,n}^{p,q} : E_{r,n}^{p,q} \to E_{r,n}^{p+r,q-r+1}$$

and where we put for all $p, q \geq 0$

$$E_{r+1,n}^{p,q} = \frac{\ker(d_{r,n}^{p,q})}{\mathrm{Im}(d_{r,n}^{p-r,q+r-1})}.$$

We put $E_{\infty,n}^{p,q}$ to be the stationary group $E_{r,n}^{p,q}$ for all r sufficiently large.

We have that $E_{r,n}^{p,q}$ is a sub-quotient of $E_{2,n}^{p,q}$ for all p, q, n hence $E_{r,n}^{p,q}$ is annihilated by n for all p, q, r. Hence $E_{\infty,n}^{p,q}$ is annihilated by n for all p, q, r.

The quasi-group $\{E_{2,n}^{p,q}\}_{n\in\Lambda}$ is trivial for all $p, q \geq 0$, by hypothesis, and the abelian group $E_{2,n}^{p,q}$ is zero unless $p \geq 0$ and $q \geq 0$. Hence for all $p, q \geq 0$ there are bounded multiplicative functions

$$\phi^{p,q} : \mathbb{N}^* \to \mathbb{N}$$

such that

$$|E_{2,n}^{p,q}| \leq \phi^{p,q}(n) \text{ for all } p, q, n.$$

Hence we have

$$|E_{r,n}^{p,q}| \leq \phi^{p,q}(n) \text{ for all } p, q, r, n.$$

Hence we have $|E^{p,q}_{\infty,n}| \leq \phi^{p,q}(n)$ for all p, q, r, n. Hence $\{E^{p,q}_{\infty,n}\}_{n\in\Lambda}$ is a trivial quasi-group for all p, q.

The abutment E^r_n of the spectral sequence is equipped with a filtration

$$E^r_n = E^r_{0,n} \supset E^r_{1,n} \supset \ldots \supset E^r_{r,n} \supset 0$$

such that

$$E^r_{p,n}/E^r_{p+1,n} \cong E^{p,r-p}_{\infty,n}.$$

As $\{E^{p,q}_{\infty,n}\}_{n\in\Lambda}$ is a trivial quasi-group for all p, q and E^i_n is annihilated by n for all i, it follows that $\{E^r_n\}_{n\in\Lambda}$ is a trivial quasi-group for all $r \geq 0$.]

7.1.15. Remark. As in the preceding example 7.1.14(5), assume we are given the quasi-groups $\{E^{i,j}_{2,n}\}_{n\in\Lambda}$ for all integers $i, j \geq 0$ and the first quadrant convergent spectral sequences of abelian groups for all $n \in \Lambda$

$$E^{i,j}_{2,n} \Rightarrow E^{i+j}_n.$$

Assume that E^i_n is annihilated by n so that $\{E^i_n\}_{n\in\Lambda}$ is a quasi-group in $[\Lambda]_{\mathbb{Z}}$. Then we have a first quadrant spectral sequence of quasi-groups in the abelian category $[\Lambda]_{\mathbb{Z}}$

$$\mathcal{E}^{i,j}_2 = \{E^{i,j}_{2,n}\}_{n\in\Lambda} \Rightarrow \mathcal{E}^{i+j} = \{E^{i+j}_n\}_{n\in\Lambda}.$$

For we have, with the notation of the preceding example, that the intermediate convergent $E^{i,j}_{r,n}$ is annihilated by n for all $n \in \Lambda$ hence $\{E^{i,j}_{r,n}\}_{n\in\Lambda}$ is a quasi-group of $[\Lambda]_{\mathbb{Z}}$ for all i, j, r.

This spectral sequence $\mathcal{E}^{i,j}_2 \Rightarrow \mathcal{E}^{i+j}$ of $[\Lambda]_{\mathbb{Z}}$ is not convergent in general because the sequence of quasi-groups

$$\mathcal{E}^{i,j}_r = \{E^{i,j}_{r,n}\}_{n\in\Lambda} \quad \text{for } r = 2, 3, \ldots$$

need not stabilise. We therefore say that this spectral sequence of quasi-groups $\mathcal{E}^{i,j}_2 \Rightarrow \mathcal{E}^{i+j}$ is *semi-convergent* in the abelian category $[\Lambda]_{\mathbb{Z}}$.

The conclusion of the preceding example 7.1.14(5) may be stated as follows. If $\mathcal{E}^{i,j}_2$ are trivial quasi-groups for all i, j and the E^i_n are annihilated by n for all i and n then the first quadrant spectral sequence of quasi-groups in $[\Lambda]_{\mathbb{Z}}$

$$\mathcal{E}^{i,j}_2 = \{E^{i,j}_{2,n}\}_{n\in\Lambda} \Rightarrow \mathcal{E}^{i+j} = \{E^{i+j}_n\}_{n\in\Lambda}$$

is semi-convergent and $\mathcal{E}^i$ is a trivial quasi-group for all i.

7.2 Igusa's theorem

We shall summarise the results of Igusa for the Galois action on torsion points of elliptic curves over global fields of positive characteristic.

(7.2.1) Let F be a global field of positive characteristic p. Let E/F be an elliptic curve with modular invariant $j \in F$. Assume that the finite field k is the exact field of constants of F. Let

$G = \mathrm{Gal}(F^{\mathrm{sep}}/F)$, where F^{sep} is the separable closure of F;
n be an integer prime to p;
E_n be the finite F-group scheme of n-torsion points of E;
E_∞ be the torsion subgroup of $E(F^{\mathrm{sep}})$ of order prime to p.

The elliptic curve is said to be *isotrivial* if there is a finite galois extension field F' of F such that the curve $E \times_F F'$ is definable over a finite subfield of F'; otherwise, the curve E is said to be *not isotrivial*.

(7.2.2) The action of the galois group G on E_n provides a homomophism

$$\rho_n : G \to \mathrm{Aut}(E_n) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

The determinant

$$\det : \mathrm{Aut}(E_n) \to (\mathbb{Z}/n\mathbb{Z})^*$$

induces a homomorphism

$$G \to (\mathbb{Z}/n\mathbb{Z})^*.$$

Let H_n be the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ generated by the powers of $q = |k|$ modulo n. Then H_n is naturally isomorphic to the Galois group of the field of nth roots of unity over k. Let Γ_n be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ defined by the exact sequence of finite groups

(7.2.3)
$$0 \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \Gamma_n \xrightarrow{\det} H_n \to 0.$$

(7.2.4) Passing to the projective limit of the previous exact sequence over all integers n prime to p we obtain the exact sequence of profinite groups

$$0 \to \mathrm{SL}_2(\hat{\mathbb{Z}}^{(p)}) \to \hat{\Gamma} \to \hat{H} \to 0$$

where $\hat{H}$ is the subgroup of $\hat{\mathbb{Z}}^{(p)*}$ topologically generated by q, where

$$\hat{\mathbb{Z}}^{(p)} = \prod_{l \neq p} \mathbb{Z}_l$$

is the profinite prime-to-p completion of $\mathbb{Z}$, and $\hat{\Gamma}$ is a closed subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}}^{(p)})$.

(7.2.5) Passing to the projective limit of the exact sequence (7.2.3) where n runs over all powers of a prime number l where $l \neq p$, we obtain the exact sequence

$$0 \to \mathrm{SL}_2(\mathbb{Z}_l) \to \hat{\Gamma}_l \to \hat{H}_l \to 0.$$

7.2.6. Theorem. (Igusa [I]). *Suppose that E/F is not isotrivial. Then the profinite group* $\mathrm{Gal}(F(E_\infty)/F)$ *is an open subgroup of* $\hat{\Gamma}$. □

This result may be restated as follows.

7.2.7. Theorem. *Suppose that E/F is not isotrivial. Then for all prime numbers $l \neq p$ the profinite group* $\mathrm{Gal}(F(E_{l^\infty})/F)$ *is an open subgroup of* $\hat{\Gamma}_l$ *and is equal to* $\hat{\Gamma}_l$ *for all but finitely many l.* □

7.2.8. Remarks. (1) Suppose that the curve E/F is isotrivial. Then it is easy to show that the group $\mathrm{Gal}(F(E_\infty)/F)$ is an extension of a finite group by the abelian profinite group $\hat{\mathbb{Z}}^{(p)}$.
(2) Let E be an elliptic curve defined over a number field L. Let E_∞ be the torsion subgroup of $E(\overline{L})$, where $\overline{L}$ denotes the algebraic closure of L. Then the nature of the galois group $\mathrm{Gal}(L(E_\infty)/L)$ is as follows.

Let P be the set of all prime numbers. For any prime number l, let $T_l(E)$ be the Tate module of E and let $\mathbb{Z}_l$ be the l-adic completion of $\mathbb{Z}$. Then the galois action of $G = \mathrm{Gal}(\overline{L}/L)$ provides a continuous homomorphism $\rho_l : G \to \mathrm{GL}(T_l(E))$.

(a) Suppose that E has complex multiplication. Put $R = \mathrm{End}_{\overline{L}}(E)$, which is an order of an imaginary quadratic extension of $\mathbb{Q}$. Assume that the elements of R are defined over L. Put $R_l = R \otimes_{\mathbb{Z}} \mathbb{Z}_l$. Then $T_l(E)$ is a free R_l-module of rank 1. The image of $G = \mathrm{Gal}(\overline{L}/L)$ by $\rho_l : G \to \mathrm{GL}(T_l(E))$ commutes with the elements of R_l and is therefore contained in R_l^*. The image of G by $\rho = \prod_{l \in P} \rho_l$ is an open subgroup of the product $\prod_{l \in P} R_l^*$.
[See [S5, §4.5] for more details.]

(b) If E does not have complex multiplication then the image of $G = \mathrm{Gal}(\overline{L}/L)$ by $\rho = \prod_{l \in P} \rho_l$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ (see [S5]).

7.3 Consequences of Igusa's theorem

For a finite group G and a $\mathbb{Z}[G]$-module M, let $H^i(G, M)$ denote the standard cohomology groups of G acting on M (see §5.6 or [CF, Chap. IV]). Let $\hat{H}^i(G, M)$ denote the Tate cohomology groups of G acting on M (see [CF, Chap. IV]).

7.3.1. Proposition. *Let E/F be an elliptic curve and let $\mathbb{N}^{(p)}$ be the set of positive integers prime to p, where p is the characteristic of F. Write G_n for the group $\mathrm{Gal}(F(E_n)/F)$.*
(i) *Let $i = 0$ or 1. Then*

$$\{H^i(G_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group.
(ii) *There is a finite set $\mathcal{N}$ of prime numbers including p such that for all prime numbers $l \notin \mathcal{N}$ we have*

$$H^i(G_{l^n}, E_{l^n}) = 0 \quad \textit{for all} \quad n \geq 1 \quad \textit{and all} \quad i \geq 0.$$

7.3.2. Remark. The proof below of this proposition shows that if E/F is isotrivial then for all integers $i \geq 0$

$$\{H^i(G_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group. Does this also hold if E/F is not isotrivial?

Proof of proposition 7.3.1. Case 1. Suppose that E/F is not isotrivial.

With the notation of §7.2, for any integer $n \geq 1$ prime to p, let H_n be the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ generated by the powers of $q = |k|$ modulo n. As in §7.2, let Γ_n be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ defined by the exact sequence (7.2.1) namely

$$0 \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \Gamma_n \xrightarrow{\det} H_n \to 0. \tag{7.3.3}$$

The group $\mathrm{Gal}(F(E_\infty)/F)$ is a subgroup of finite index s, say, of the profinite group $\hat{\Gamma} = \varprojlim \Gamma_n$ by Igusa's theorem 7.2.2. The homotheties λI_2, where $\lambda \in H_n$ and I_2 is the identity of GL_2, are contained in the centre of the group Γ_n. Identifying G_n with a subgroup of Γ_n, we obtain that

$$Z_n = \{\lambda^s I_2 \mid \lambda \in H_n\}$$

is a subgroup of G_n contained in its centre.

By definition of Z_n, we have

$$H^0(Z_n, E_n) = \{P \in E_n \mid q^s P = P\}.$$

If the exact order of $P \in E_n$ is m then we have $q^s P = P$ if and only if m divides $q^s - 1$. Hence we have an isomorphism of G_n-modules

$$H^0(Z_n, E_n) \cong E_{\gcd(q^s-1,n)}.$$

It follows that $\{H^0(Z_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$ and $\{\hat{H}^0(Z_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$ are trivial quasi-groups. The group Z_n is cyclic and the group E_n is finite hence its herbrand

quotient $h(Z_n, E_n)$ is equal to 1. Hence for a fixed integer n, the groups $\hat{H}^i(Z_n, E_n)$ have the same order for all i. As $\hat{H}^i(Z_n, E_n) \cong H^i(Z_n, E_n)$ for all $i \geq 1$, it follows that for all integers $i \geq 0$

$$\{H^i(Z_n, E_n)\}_{n \in \mathbb{N}^{(p)}}$$

is a trivial quasi-group.

The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by 2 elements namely the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The natural homomorphisms

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$$

are surjective for all integers $n \geq 1$. Hence the group $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is generated by at most 2 elements for all n.

The subgroup Γ_n of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ defined by the exact sequence (7.3.3) is finitely generated with a set of at most 3 generators, as H_n is generated by 1 element. The group G_n is a subgroup of Γ_n of index $\leq s$. Hence by Schreier's formula [S4, p.43], we have that G_n is generated by at most $2s + 1$ elements for all n prime to p. We then have that the group

$$H^1(G_n/Z_n, H^0(Z_n, E_n)) \cong H^1(G_n/Z_n, E_{\gcd(q^s-1,n)})$$

has order bounded by

$$\gcd(q^s - 1, n)^{2(2s+1)}.$$

This holds as a 1-cocycle in $\mathrm{Cocy}^1(G_n/Z_n, E_{\gcd(q^s-1,n)})$ is uniquely determined by its values on a set of generators of G_n/Z_n. It follows that the quasi-group

$$\{H^1(G_n/Z_n, H^0(Z_n, E_n))\}_{n \in \mathbb{N}^{(p)}}$$

is trivial.

We have the Hochschild-Serre spectral sequence

$$H^i(G_n/Z_n, H^j(Z_n, E_n)) \Rightarrow H^{i+j}(G_n, E_n).$$

The short exact sequence of low degree terms of this spectral sequence begins with the sequence

$$(7.3.4) \quad 0 \to H^1(\frac{G_n}{Z_n}, H^0(Z_n, E_n)) \to H^1(G_n, E_n) \to H^0(\frac{G_n}{Z_n}, H^1(Z_n, E_n)).$$

As $\{H^1(Z_n, E_n)\}_{n \in \mathbb{N}^{(p)}}$ is a trivial quasi-group we obtain that

$$\{H^0(G_n/Z_n, H^1(Z_n, E_n))\}_{n \in \mathbb{N}^{(p)}}$$

is as well. As $\{H^1(G_n/Z_n, H^0(Z_n, E_n))\}_{n\in\mathbb{N}^{(p)}}$ is also a trivial quasi-group, from the exact sequence (7.3.4) we obtain that

$$\{H^1(G_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group. It is obvious that

$$\{H^0(G_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group and this proves part (i) of the proposition in this case.

For all integers $n \geq 1$ prime to p and to $q^s - 1$ we have

$$H^i(Z_n, E_n) = 0 \quad \text{for all } i \geq 0.$$

Hence the Hochschild-Serre spectral sequence

$$H^i(G_n/Z_n, H^j(Z_n, E_n)) \Rightarrow H^{i+j}(G_n, E_n)$$

degenerates and we obtain for all $n \geq 1$ prime to p and to $q^s - 1$

$$H^i(G_n, E_n) = 0 \quad \text{for all } i \geq 0.$$

This proves part (ii) of the proposition in this case where E/F is not isotrivial.

Case 2. Suppose that E/F is isotrivial.

Then there is a finite galois extension field L/F such that $E \times_F L$ is definable over a finite subfield $\mathbb{F}$ of L; that is to say, there is an elliptic curve $E'/\mathbb{F}$ and an isomorphism

$$E' \times_{\mathbb{F}} L \cong E \times_F L$$

of elliptic curves over L. By enlarging $\mathbb{F}$ if necessary, we may take $\mathbb{F}$ to be the largest finite subfield of L, that is to say we may assume that $\mathbb{F}$ is algebraically closed in L. Let $L(E_n)$ be the join of the fields L and $F(E_n)$. We write U_n for the galois group

$$U_n = \mathrm{Gal}(F(E_n)/F(E_n) \cap L).$$

Then U_n is a normal subgroup of G_n such that the quotient group is a homomorphic image of $\mathrm{Gal}(L/F)$.

We have isomorphisms of galois groups

$$U_n \cong \mathrm{Gal}(L(E_n)/L) \cong \mathrm{Gal}(\mathbb{F}(E'_n)/\mathbb{F}(E'_n) \cap L).$$

As $\mathbb{F}$ is algebraically closed in L, we have $\mathbb{F}(E'_n) \cap L = \mathbb{F}$ for all integers n prime to p. Hence we have isomorphisms for all n prime to p

$$U_n \quad \cong \quad \mathrm{Gal}(\mathbb{F}(E'_n)/\mathbb{F})\,.$$

In particular, U_n is a finite cyclic group.

We obtain the commutative diagram of fields

$$
\begin{array}{ccccc}
 & & L(E_n) & \leftarrow & F(E_n) \\
 & \nearrow & U_n\Big\{\uparrow & & \uparrow\Big\}U_n \\
\mathbb{F}(E'_n) & & L & \leftarrow & F(E_n)\cap L \\
U_n\Big\{\uparrow & \nearrow & & \nwarrow & \uparrow \\
\mathbb{F} & & & & F
\end{array}
\Bigg\} G_n \tag{7.3.5}
$$

where each vertical arrow denotes a galois field extension.

The quasi-group $\{\hat{H}^0(U_n, E'_n)\}_{n\in\mathbb{N}^{(p)}}$ is a trivial because $E'(\mathbb{F})$ is a finite group. As E'_n is a finite group and U_n is a finite cyclic group, its Herbrand quotient as a U_n-module is equal to 1; hence $\hat{H}^i(U_n, E'_n)$ has the same order as $\hat{H}^0(U_n, E'_n)$ for all $i \geq 0$. Hence $\{\ \hat{H}^i(U_n, E'_n)\ \}_{n\in\mathbb{N}^{(p)}}$ is a trivial quasi-group for all $i \geq 0$. It follows that for all $i \geq 1$

$$\{\ H^i(U_n, E'_n)\ \}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group. We obtain from the diagram (7.3.5) that for all $i \geq 1$

$$\{\ H^i(U_n, E_n)\ \}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group.

We have

$$H^0(U_n, E_n) = E_n(F(E_n)\cap L).$$

In particular, $H^0(U_n, E_n)$ is a subgroup of $E_n(L)$. As $\{E_n(L)\}_{n\in\mathbb{N}^{(p)}}$ is a trivial quasi-group by the Mordell-Weil theorem, we have that

$$\{H^0(U_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group. Hence

$$\{H^j(U_n, E_n)\}_{n\in\mathbb{N}^{(p)}}, \quad \text{for all } j \geq 0,$$

are trivial quasi-groups.

We have the Hochschild-Serre spectral sequence

$$H^i(G_n/U_n, H^j(U_n, E_n)) \Rightarrow H^{i+j}(G_n, E_n).$$

For all $i, j \geq 0$, let $\mathcal{E}_2^{i,j}$ denote the quasi-group in $[\mathbb{N}^{(p)}]_{\mathbb{Z}}$

$$\mathcal{E}_2^{i,j} = \{H^i(G_n/U_n, H^j(U_n, E_n))\}_{n\in\mathbb{N}^{(p)}}$$

.

We have already shown that

$$\{H^j(U_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$$

is a trivial quasi-group for all $j \geq 0$. The galois group G_n/U_n is a quotient group of $\mathrm{Gal}(L/F)$ which is independent of n. Furthermore, for $i \geq 1$ by the example 7.1.14(1) we have that the order of

$$H^i = H^i(G_n/U_n, H^j(U_n, E_n))$$

is bounded by

$$N^{m(H^j(U_n,E_n))N^i}$$

where N is the order of the group $\mathrm{Gal}(L/F)$ and $m(H^j(U_n, E_n))$ is the minimal number of generators of the abelian group $H^j(U_n, E_n)$. Furthemore, this cohomology group H^i is annihilated by n and is zero for all n prime to a certain finite set of prime numbers as $\{H^j(U_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$ is a trivial quasi-group for all j. Hence $\mathcal{E}_2^{i,j}$ is a trivial quasi-group for all $i \geq 1$ and all $j \geq 0$.

We have that $\mathcal{E}_2^{0,j}$ is a sub-quasi-group of the trivial quasi-group $\{H^j(U_n, E_n)\}_{n\in\mathbb{N}^{(p)}}$ for all $j \geq 0$ hence $\mathcal{E}_2^{0,j}$ is a trivial quasi-group for all j. We conclude that $\mathcal{E}_2^{i,j}$ is a trivial quasi-group for all $i \geq 0$ and all $j \geq 0$.

The Hochschild-Serre spectral sequence above then provides a semi-convergent first quadrant spectral sequence of quasi-groups in $[\mathbb{N}^{(p)}]_{\mathbb{Z}}$ (see remark 7.1.15)

$$\mathcal{E}_2^{i,j} \Rightarrow \mathcal{E}^i$$

where

$$\mathcal{E}^i = \{H^i(G_n, E_n)\}_{n\in\mathbb{N}^{(p)}}.$$

As the $\mathcal{E}_2^{i,j}$ are trivial quasi-groups we have by example 7.1.14(5) and remark 7.1.15 that $\mathcal{E}^i$ is a trivial quasi-group for all $i \geq 0$; this proves both parts (i) and (ii) in this case where E/F is isotrivial.□

The following group-theoretic result is proved in the next section §7.4.

7.3.6. Proposition. *Let $l \geq 5$ be a prime number. Let*

$$\phi : \mathrm{SL}_2(\mathbb{Z}_l) \to G$$

be a continuous surjective homomorphism where G is a non-trivial discrete finite simple group and $\mathrm{SL}_2(\mathbb{Z}_l)$ is an l-adic group. Then G is isomorphic to the finite simple group $\mathrm{PSL}_2(\mathbb{Z}/l\mathbb{Z})$.

7.3.7. Corollary. *Let E/F be an elliptic curve which is not isotrivial. Then for all except finitely prime numbers l and for all integers $n \geq 1$ the only intermediate fields of $F(E_{l^n})/F$ which are solvable over F are those obtained from F by adjoining lth power roots of unity.*

Proof. This follows from Igusa's theorem 7.2.2 and the preceding proposition 7.3.6.□

7.3.8. Proposition. *Under the hypotheses of (6.1.1), let*

$$K[A] = \bigcup_{c \in \mathrm{Div}_+(A)} K[c]$$

which is an infinite abelian extension of K composed of ring class fields. Let E/F be an elliptic curve. Then the quasi-group

$$\{E(K[A])_n\}_{n \in \mathbb{N}^{(p)}}$$

is trivial.

Proof. 1st argument. Let n be a positive integer prime to p. Let $M(n,c) = K[c] \cap K(E_n)$ which is a galois extension of K. Then as $F(E_n)$ is an unramified extension of F we have that $M(n,c)/K$ is unramified. As $K[c]/K$ is an abelian extension which is split completely at the place of K above ∞ we have that $M(n,c)/K$ is also an abelian extension which is split completely at ∞. But then we have $M(n,c) \subseteq K[0]$ for $K[0]/K$ is the maximal abelian unramified extension of K which is split completely at ∞. Hence we obtain the inclusion for all $c \in \mathrm{Div}_+(A)$ and all $n \in \mathbb{N}^{(p)}$

$$E(M(n,c))_n \subseteq E(K[0])_n.$$

But $E(K[0])$ is a finitely generated abelian group by the Mordell-Weil theorem hence $\{E(K[A])_n\}_{n \in \mathbb{N}^{(p)}}$ is a trivial quasi-group.

2nd argument. We shall prove using proposition 7.3.6 the weaker statement that if E/F is not isotrivial then for all prime numbers l, except finitely many, and for any effective divisor c on Spec A we have

$$E(K[c])_{l^\infty} = 0.$$

Let l be a prime number distinct from p. Let $M_l = K[c] \cap F(E_{l^\infty})$ which is a finite galois extension of F. Let $\hat{H}_l$ be the closed subgroup of $\hat{\mathbb{Z}}_l^*$ which is topologically generated by the powers of $q = |k|$. Then $\hat{H}_l$ is naturally isomorphic to the Galois group of the cyclotomic field $F(\zeta_{l^\infty})$ of all lth power roots of unity over F.

For all except finitely many prime numbers l, we then have a commutative diagram of groups with an exact row (see theorem 7.2.2) and where α, β are surjective homomorphisms

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{SL}(2,\mathbb{Z}_l) & \xrightarrow{\gamma} & \mathrm{Gal}(F(E_{l^\infty})/F) & \to & \hat{H}_l & \to & 0 \\ & & & & \downarrow \alpha & & & & \\ & & \mathrm{Gal}(K[c]/F) & \xrightarrow{\beta} & \mathrm{Gal}(M_l/F) & & & & \end{array}$$

The surjection $\mathrm{Gal}(F(E_{l^\infty})/F) \to \hat{H}_l$ corresponds to an inclusion of fields $F(\zeta_{l^\infty}) \subseteq F(E_{l^\infty})$. As $\mathrm{Gal}(K[c]/F)$ is a generalised dihedral group (proposition 2.5.6), we have that $\mathrm{Gal}(M_l/F)$, which is a homomorphic image of $\mathrm{Gal}(K[c]/F)$, is either abelian or generalised dihedral. But then the composite homomorphism

$$\alpha \circ \gamma : \mathrm{SL}(2, \mathbb{Z}_l) \to \mathrm{Gal}(M_l/F)$$

is zero for all prime numbers $l \geq 5$ by proposition 7.3.6. Hence the map α factors through $\hat{H}_l$ which is the galois group of $F(\zeta_{l^\infty})$ over F. It follows that, for all except finitely many prime numbers l the field extension M_l/F is abelian, unramified, and is a subfield of a cyclotomic field $F(\zeta_{l^m})$ for some $m \geq 1$, where ζ_{l^m} is a primitive l^mth root of unity.

The extension $K[c]/K[0]$ is ramified at all places in the support of c (see (2.3.13)) and we have $M_l \subseteq K[c]$. Therefore we have $M_l \subseteq K[0]$ for all except finitely many prime numbers l. We obtain that for all except finitely many prime numbers l

$$E(K[c])_{l^\infty} \subseteq E(K[0]).$$

As $E(K[0])$ is a finitely generated abelian group, by the Mordell-Weil theorem, we have that for all except finitely many prime numbers l and for all divisors $c \geq 0$

$$E(K[c])_{l^\infty} = 0$$

where the finite exceptional set of prime numbers is independent of c. □

7.3.9. Remark. A variant of the 2nd argument in the previous proof also holds for elliptic curves over number fields. For example it shows the following. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let K be an imaginary quadratic extension of $\mathbb{Q}$. Denote by K_n the ring class field of K of conductor $n \in \mathbb{N}$. Then for all except finitely many prime numbers l we have $E(K_n)_{l^\infty} = 0$ for all n.

7.3.10. Proposition. *Let E/F be an elliptic curve which is not isotrivial. Let L be a finite extension field of F in which k is algebraically closed. Then there is an infinite set S of prime numbers of positive Dirichlet density such that for all $l \in S$ we have*
(a) *the fields $F(E_{l^\infty})$ and L are linearly disjoint over F;*
(b) *$E(L)_{l^\infty} = 0$;*
(c) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{Gal}(F(E_{l^\infty})/F)$.

Proof. For any prime number l distinct from p, let H_{l^n} denote the subgroup of $(\mathbb{Z}/l^n\mathbb{Z})^*$ generated by the powers of q modulo l^n. Put

$$\hat{H}_l = \varprojlim_n H_{l^n}$$

which is the closed subgroup of $\mathbb{Z}_l^*$ topologically generated by q.

For any positive integer s let $\zeta_{2^s} \in \mathbb{C}$ be a primitive 2^sth root of unity. Put

$$K_s = \mathbb{Q}(\zeta_{2^s}),\ K'_s = \mathbb{Q}(\zeta_{2^s}, q^{1/2^s}).$$

Then $K_s/\mathbb{Q}$ and K'_s/K_s are Galois field extensions

Step 1. Let $l > 2$ be an odd prime number distinct from p. Let 2^s be the exact power of 2 which divides $l-1$. Then we have $-1 \in \hat{H}_l$ if and only if q is a 2^sth-power non-residue modulo l.

For we have by Hensel's lemma that $-1 \in \hat{H}_l$ if and only if the congruence

$$x^{2^s} \equiv q \pmod{l} \tag{7.3.11}$$

has no solution for $x \in \mathbb{Z}$. This latter condition is equivalent to q being a 2^sth-power non-residue modulo l, as required.

Step 2. Put for any integer $s \geq 0$

$$T_s = \left\{ \begin{array}{c} \text{prime numbers which split completely in } K_{s+1}/\mathbb{Q} \text{ and in } K'_s/\mathbb{Q} \\ \text{but do not split completely in } K'_{s+1}/\mathbb{Q} \end{array} \right\}$$

$$T = \bigcup_{s \geq 0} T_s.$$

Let $l > 2$ be an odd prime number distinct from p. Then we have

$$-1 \in \hat{H}_l \text{ if and only if } l \in T. \tag{7.3.12}$$

For the galois field extensions $K_s/\mathbb{Q}$ and K'_s/K_s we have these inclusions for all integers $s \geq 0$

$$\begin{array}{ccccc} \mathbb{Q} & \subset & K_s & \subset & K'_s \\ & & \cap & & \cap \\ & & K_{s+1} & \subset & K'_{s+1} \end{array}$$

Furthermore, for any prime number $l > 2$ we have that 2^s divides $l-1$ if and only if l splits completely in the field extension $K_s/\mathbb{Q}$. If 2^s divides $l-1$, we then have that the congruence (7.3.11) above has no solution for x if and only if l does not split completely in the field extension $K'_s/\mathbb{Q}$. Then we have from the above discussion that

$$-1 \in \hat{H}_l \text{ if and only if } l \in T.$$

Here T is the disjoint union of the sets T_s of prime numbers.

Step 3. The set T of prime numbers has non-zero Dirichlet density.

Write q as $q = p^m$ where p is the characteristic of F and $m \geq 1$ is an integer. Let 2^r be the highest power of 2 which divides the integer m. Suppose first that $p > 2$. Then the the field extensions $K_s/\mathbb{Q}, K'_s/K_s$ have degrees given by

$$\begin{aligned} [K_s : \mathbb{Q}] &= 2^{s-1}, \quad \text{if } s \geq 1, \\ [K'_s : K_s] &= 2^{s-r}. \quad \text{if } s \geq r. \end{aligned}$$

as the field extensions K_s and $\mathbb{Q}(q^{1/2^r})$ are linearly disjoint for all $r, s \geq 0$. In particular, if $p \neq 2$ then K'_s is distinct from K_s for all $s > r$; by the Chebotarev density theorem we then have that T_s has non-zero Dirichlet density for all integers s such that $s \geq r$ if $p \neq 2$. On the other hand, we have

$$T_s = \emptyset \text{ for } s \leq r - 1$$

because for $s \leq r$ we have

$$K'_s = \mathbb{Q}(\zeta_{2^s}, q^{1/2^s}) = \mathbb{Q}(\zeta_{2^s}, p^{2^{r-s}}) = K_s.$$

Suppose now that $p = 2$. These field extensions are no longer linearly disjoint as we have $\sqrt{2} \in K_3$. We assert that

$$\mathbb{Q}(2^{1/2^t}) \cap K_s = \begin{cases} \mathbb{Q}(2^{1/2}), & \text{if } t \geq 1 \text{ and } s \geq 3 \\ \mathbb{Q}, & \text{otherwise.} \end{cases} \tag{7.3.13}$$

On the one hand, if $t = 0$ or if $s \leq 2$ then we have

$$\mathbb{Q}(2^{1/2^t}) \cap K_s = \mathbb{Q}.$$

On the other hand, if $t \geq 1$ and $s \geq 3$ then we clearly have

$$\mathbb{Q}(2^{1/2^t}) \cap K_s \supset \mathbb{Q}(2^{1/2}).$$

If equality did not always hold here then for some $s \geq 3$ and $t \geq 2$ we would have

$$\mathbb{Q}(2^{1/2^t}) \cap K_s \supset \mathbb{Q}(2^{1/4}).$$

This would imply that the field K_s contained $\mathbb{Q}(i, 2^{1/4})$; this is impossible as $\mathbb{Q}(i, 2^{1/4})$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to the non-abelian dihedral group with 8 elements and $K_s/\mathbb{Q}$ is an abelian Galois extension. This proves the statement (7.3.13).

We obtain from (7.3.13) that

$$[K'_s : K_s] = 2^{s-r-1} \text{ for all } s \geq \max(3, r+1).$$

It follows from this that K'_{s+1} is a quadratic extension of the compositum $K_{s+1}.K'_s$ for all $s \geq \max(3, r+1)$. Hence by the Chebotarev density theorem, the set T_s of prime numbers has non-zero Dirichlet density for all $s \geq \max(3, r+1)$.

In résumé, for any $s \geq r$ the set T_s consists of all prime numbers which split completely in the join $K_{s+1}.K'_s$ over $\mathbb{Q}$ but the prime ideals lying over these prime numbers do not split completely in the Galois extension $K'_{s+1}/K_{s+1}.K'_s$; it follows from the preceding discussion that for all prime numbers $p \geq 2$, the set T_s has non-zero Dirichlet density for all $s \geq \max(3, r+1)$. As T is the disjoint union of the sets T_s, for $s \geq 0$, we obtain that T has non-zero Dirichlet density and, in particular, contains infinitely many prime numbers, as required.

Step 4. End of proof.

Let E_∞ denote the prime-to-p torsion subgroup of E. We now apply Igusa's theorem theorem 7.2.3 on the structure of the Galois group $\mathrm{Gal}(F(E_\infty)/F)$; we have that for all except finitely many prime numbers $l \neq p$, the group $\mathrm{Gal}(F(E_{l^\infty})/F)$ is the subgroup of $\mathrm{GL}_2(\mathbb{Z}_l)$ determined by the exact sequence

$$0 \quad \to \quad \mathrm{SL}_2(\mathbb{Z}_l) \quad \to \quad \mathrm{Gal}(F(E_{l^\infty})/F) \quad \overset{\det}{\to} \quad \hat{H}_l \quad \to \quad 0.$$

Here the map det is the restriction of the determinant homomorphism. We then obtain that for all prime numbers $l \in T$, except for finitely many, the group $\mathrm{Gal}(F(E_{l^\infty})/F)$ contains all elements of $\mathrm{GL}_2(\mathbb{Z}_l)$ with determinant equal to -1, in particular, this group for all prime numbers $l \in T$, except finitely many, contains the semi-simple element

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let k be the exact field of constants of the global field F, that is to say k is the largest finite field contained in F. Let L be a finite extension field of F in which k is algebraically closed, as in the statement of the proposition. Then for all prime numbers $l \in T$ except for finitely many we have

$$E(L)_{l^\infty} = 0$$

by the Mordell-Weil theorem.

Let k^{sep} be the algebraic closure of k. Let $j \in F$ be the j-invariant of the elliptic curve E/F. Then j is transcendental over k as E/F is not isotrivial. Let F_1 be the subfield $k(j)$ of F. Then the curve E is definable over F_1 and the fields $k^{\mathrm{sep}}F_1(E_{l^\infty})$ are linearly disjoint over $k^{\mathrm{sep}}F_1$ for distinct prime numbers l, as shown by Igusa. It follows that $F(E_{l^\infty}) \cap L$ is equal to F for all except finitely many prime numbers l. In particular, for all except finitely prime numbers $l \in T$ the fields $F(E_{l^\infty})$ and L are linearly disjoint.

The set S of prime numbers in the statement of the proposition may therefore be obtained from the set T by deleting a finite set of elements.□

7.3.14. Remarks. (1) The set S of prime numbers of this proposition 7.3.10 consists of all but finitely many prime numbers l of the form $2^s n + 1$ where $s \geq 1$ and n is odd such that $q = |k|$ is a 2^sth power non-residue modulo l.

(2) The Dirichlet density of the set S of prime numbers may be computed; for the case where $p > 2$ the density is equal to $\frac{1}{7.3^{r-1}}$ where 2^r is the highest power of 2 which divides m and where $q = p^m$. If $p = 2$ the density is equal to 1.
(3) The cohomological vanishing proposition 7.3.1 for the Galois action is a refinement of [Br2, Cor. 3.3]. Proposition 7.3.10 is a refinement of [Br2, Cor. 3.4], where the hypothesis that q be a square has been eliminated.

7.4 Proof of proposition 7.3.6.

This proof is entirely group theoretic.

(7.4.1) For any commutative ring Λ let

$E(\Lambda)$ be the subgroup of $\mathrm{SL}_2(\Lambda)$ generated by elementary matrices i.e. matrices which coincide with the identity except for a single off-diagonal entry;
$D(\Lambda)$ be the subgroup of diagonal matrices of $\mathrm{SL}_2(\Lambda)$;
$N(\Lambda)$ be the normal subgroup of $\mathrm{SL}_2(\Lambda)$ generated by $E(\Lambda)$;
$\mathrm{SL}_2(\Lambda)/N(\Lambda)$ denote the group of cosets of $N(\Lambda)$ in $\mathrm{SL}_2(\Lambda)$.

(7.4.2) Let P be the set of pairs (a, b) of elements of Λ such that $a\Lambda + b\Lambda = \Lambda$ i.e. the ideal generated by a, b equals Λ. Define a map of sets

$$f : P \to \mathrm{SL}_2(\Lambda)/N(\Lambda)$$
$$(a, b) \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N(\Lambda)}.$$

where $b, d \in \Lambda$ are any elements such that $ad - bc = 1$. This map f is well defined as the image $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N(\Lambda)}$ is independent of the choice of coset representative $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $N(\Lambda)$; for if $ad' - bc' = 1$ then we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c' & d' \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ cd' - dc' & 1 \end{pmatrix}.$$

This map f is clearly surjective. Let $\mathcal{P}$ be the quotient of P by the equivalence relation $(a, b) \sim (a', b')$ if and only if $f(a, b) = f(a', b')$; we write $[a, b]$ for the equivalence class of the pair (a, b).

(7.4.3) We have a symbol which is a bijective map

$$\begin{aligned} \mathrm{SL}_2(\Lambda)/N(\Lambda) \quad &\to \mathcal{P} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N(\Lambda)} &\mapsto [a,b]. \end{aligned}$$

This symbol is closely related to the Mennicke symbol on on the K-group $\mathrm{SK}_1(\Lambda)$ [Mi, pp.124-125]. Unlike the Mennicke symbol, this symbol $[a,b]$ is not bi-multiplicative. But like the Mennicke symbol it satisfies these conditions:

(A) $[a,b] = [a, b+\lambda a]$ and $[a,b] = [a+\lambda b, b]$ for all $\lambda \in \Lambda$, since elementary column operations on a matrix correspond to multiplication on the right by elementary matrices.

(B) $[a,b] = [b,-a]$, as follows from (A).

7.4.4. Lemma. *Let Λ be a local ring. Then we have $N(\Lambda)D(\Lambda) = \mathrm{SL}_2(\Lambda)$.*

Proof of lemma 7.4.4. Let $[a,b]$ be a symbol of $\mathcal{P}$. Then either b or a is a unit of Λ, as this symbol represents a unimodular matrix. If a is a unit then we have

$$[a,b] = [a, b - a\frac{b}{a}] = [a,0].$$

Furthermore, the symbol $[a,0]$ is represented by the unimodular matrix $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ which lies in $D(\Lambda)$. On the other hand, if b is a unit then by (B) we have $[a,b] = [b,-a]$ and the preceding argument applies to show that $[a,b]$ is represented by a diagonal matrix in $D(\Lambda)$. We have shown that the elements of $\mathrm{SL}_2(\Lambda)/N(\Lambda)$ are represented by elements of $D(\Lambda)$, as required.

[This result $N(\Lambda)D(\Lambda) = \mathrm{SL}_2(\Lambda)$ also holds when Λ is a euclidean domain.] □

7.4.5. Lemma. *If Λ is a local ring then $N(\Lambda) = \mathrm{SL}_2(\Lambda)$.*

Proof of lemma 7.4.5. By lemma 7.4.4, it suffices to show that $N(\Lambda)$ contains $D(\Lambda)$. Suppose then that $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in D(\Lambda)$. Then $ad = 1$ and a, d are both units of Λ. The matrix $S = \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix}$ is unimodular. We have the identity

$$S^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} S = \begin{pmatrix} a & 1 \\ -(1-a)^2 & 2-a \end{pmatrix}.$$

Hence the symbol corresponding to $M = S^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} S$ is $[a, 1]$; but $[a, 1] = [a, 0]$ as a is a unit (see (A) above). Furthermore, M lies in $N(\Lambda)$ and the matrices M and $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ have the same symbol namely $[a, 0]$. It follows that $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ lies in $N(\Lambda)$, as required.□

7.4.6. Lemma. *Let D be a discrete topological group and $\mathbb{Z}_l$ be the l-adic completion of $\mathbb{Z}$ where l is a prime number. A continuous homomorphism $\psi : \mathrm{SL}_2(\mathbb{Z}_l) \to D$ factors through the surjective homomorphism ψ_n of reduction modulo l^n, for some integer $n \geq 1$,*

$$\psi_n : \mathrm{SL}_2(\mathbb{Z}_l) \to \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z}).$$

Proof. The homomorphisms ψ_n are surjective for all n as SL_2 is a smooth group scheme over $\mathbb{Z}$. That ψ factors through some ψ_n follows immediately from the continuity of ψ: the kernel of ψ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_l)$. □

7.4.7. Lemma. *Let $M = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ be an element of $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ such that c is a unit of $\mathbb{Z}/l^n\mathbb{Z}$. Then the normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ generated by M is equal to $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$.*

Proof of lemma 7.4.7. Suppose that P is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ containing $M = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$. As $M^m = \begin{pmatrix} 1 & 0 \\ mc & 1 \end{pmatrix}$ for all integers $m \geq 1$, then P also contains all matrices of the form $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ for all $x \in \mathbb{Z}/l^n\mathbb{Z}$. Hence P also contains all matrices of the form, where $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$,

$$T\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} T^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}.$$

Hence P contains the normal subgroup $N(\mathbb{Z}/l^n\mathbb{Z})$ generated by the elementary matrices. The equality $P = \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ now follows from lemma 7.4.5.□

End of proof of proposition 7.3.6. Let $l \geq 5$ be a prime number. By lemma 7.4.6, the homomorphism $\phi : \mathrm{SL}_2(\mathbb{Z}_l) \to G$ factors though ψ_n for some $n \geq 1$

$$\psi_n : \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z}) \to G.$$

Let I be the kernel of ψ_n. Then I is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$.

Suppose first that all elements M of the subgroup I where

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

satisfy the condition

$$b \in l\mathbb{Z}/l^n\mathbb{Z}. \tag{7.4.8}$$

The element

$$T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

lies in $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ and we have, where $M \in I$ is the matrix above,

$$T^{-1}MT = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

But $T^{-1}MT$ lies in I and hence the preceding condition (7.4.8) shows that $c \in l\mathbb{Z}/l^n\mathbb{Z}$ for all elements M of I; that is to say

$$b \equiv c \equiv 0 \pmod{l} \text{ for all } M \in I. \tag{7.4.9}$$

Suppose that the matrix $M \in I$ satisfies

$$a \not\equiv d \pmod{l}.$$

Then as b, c are non-units of $\mathbb{Z}/l^n\mathbb{Z}$, we have that a, d are units of this ring. We have, where $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$,

$$U \begin{pmatrix} a & b \\ c & d \end{pmatrix} U^{-1} = \begin{pmatrix} a-b & b \\ a+c-b-d & b+d \end{pmatrix}.$$

But $a + c - b - d$ is not then divisible by l and this matrix UMU^{-1} lies in I. This contradicts the condition (7.4.9). Therefore we must have $a \equiv d \pmod{l}$ and $b \equiv c \equiv 0 \pmod{l}$ for all $M \in I$. That is to say I is contained in the kernel of the surjective homomorphism, where Z is the centre of $\mathrm{SL}_2(\mathbb{Z}/l\mathbb{Z})$,

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z}) &\to \mathrm{SL}_2(\mathbb{Z}/l\mathbb{Z})/Z \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{lZ}. \end{aligned}$$

It follows that we have the diagram of homomorphisms

$$G \xrightarrow{\cong} \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})/I \longrightarrow \mathrm{SL}_2(\mathbb{Z}/l\mathbb{Z})/Z$$

where the first arrow is an isomorphism and the second is surjective. This shows that the finite simple group G is isomorphic to $\mathrm{SL}_2(\mathbb{Z}/l\mathbb{Z})/Z$ and this proves the result in this case.

Suppose now that the condition (7.4.8) does not hold for some matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of I that is to say b is a unit of $\mathbb{Z}/l^n\mathbb{Z}$ for some $M \in I$.

The next paragraphs largely follow W. Burnside, Theory of Finite Groups, §311, 1911. Let $\alpha \in (\mathbb{Z}/l^n\mathbb{Z})^*$. Then $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ contains the element

$$S = \begin{pmatrix} \alpha a & \alpha b \\ -(1+\alpha^2 a^2)/(\alpha b) & -\alpha a \end{pmatrix}.$$

The element S satisfies

$$S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad MS = \begin{pmatrix} -\frac{1}{\alpha} & 0 \\ \alpha a c - d(1+\alpha^2 a^2)/(\alpha b) & -\alpha \end{pmatrix}.$$

Hence I contains the element $MS^{-1}MS$ which is equal to

$$S' = MS^{-1}MS = \begin{pmatrix} -\alpha^{-2} & 0 \\ -(1+\alpha^2)(d+\alpha^2 a)/(\alpha^2 b) & -\alpha^2 \end{pmatrix}.$$

The group $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ contains the matrix

$$U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Hence I contains the element $S'U^{-1}S'^{-1}U$ which is equal to

$$\begin{pmatrix} 1 & 0 \\ 1-\alpha^4 & 1 \end{pmatrix}.$$

Suppose now that $l > 5$. Then we may choose $\alpha \in (\mathbb{Z}/l^n\mathbb{Z})^*$ such that

$$1 - \alpha^4$$

is a unit of $\mathbb{Z}/l^n\mathbb{Z}$. Then by lemma 7.4.7 we obtain $I = \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$, which completes the proof in this case.

Suppose finally that $l = 5$. Then the matrix $S' = MS^{-1}MS$ as above where we put $\alpha = 1$ satisfies

$$S'^2 = \begin{pmatrix} 1 & 0 \\ \frac{4}{b}(d+a) & 1 \end{pmatrix}.$$

and $S'^2 \in I$. If $d + a = \mathrm{Tr}(M)$ is not divisible by l then this implies by lemma 7.4.7 that $I = \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$. Suppose on the other hand $\mathrm{Tr}(M)$ is divisible by

l. Then the matrix $M' = UMU^{-1}M^{-1}$ is equal to

$$M' = \begin{pmatrix} 1-bd & b^2 \\ 1-bd-d^2 & 1+b^2+bd \end{pmatrix}.$$

This matrix M' belongs to I and the top right hand element b^2 is a unit of $\mathbb{Z}/l^n\mathbb{Z}$. Furthermore, we have

$$\mathrm{Tr}(M') = b^2 + 2.$$

But then $\mathrm{Tr}(M') \not\equiv 0$ modulo 5 because -2 is a quadratic non-residue modulo 5. Hence the element $S'' = M'S^{-1}M'S$ satisfies

$$S''^2 = \begin{pmatrix} 1 & 0 \\ \frac{4}{b^2}\mathrm{Tr}(M') & 1 \end{pmatrix}$$

and S''^2 lies in I. Hence we again have that $I = \mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ by lemma 7.4.7. □

7.5 Preliminaries

(7.5.1) The notation we use is the same as that of chapters 1 and 2:

k is a finite field with $q = p^m$ elements;
θ is the Frobenius $x \mapsto x^p$;
C/k is an integral smooth 1-dimensional projective k-scheme, where k is the exact field of constants;
∞ is a closed point of C/k;
C_{aff} is the affine curve $C - \{\infty\}$;
A is the coordinate ring $H^0(C_{\mathrm{aff}}, \mathcal{O}_{C_{\mathrm{aff}}})$ of the affine curve C_{aff};
F is the fraction field of A (that is, the function field of C/k);
K is an imaginary quadratic field extension of F, with respect to ∞;
B is the integral closure of A in K.

(7.5.2) If L'/L is a Galois field extension, we shall write $H^i(L, M)$ for the Galois cohomology group $H^i(\mathrm{Gal}(L^{\mathrm{sep}}/L), M)$, where L^{sep} is the separable closure of L, and we write $H^i(L'/L, M)$ for $H^i(\mathrm{Gal}(L'/L), M)$.

7.6 Statement of the main result and historical remarks

(7.6.1) Let E/F be an elliptic curve equipped with an origin, that is to say E/F is a 1-dimensional abelian variety. Let I be the ideal of A which is the

conductor of E/F without the component at ∞. Let $\epsilon = \pm 1$ be the sign in the functional equation of the L-function of the elliptic curve E/F. Assume that:

(a) ∞ is a place of F with residue field equal to k;
(b) E/F has split multiplicative reduction at ∞ (see §4.7);
(c) K is an imaginary quadratic field extension of F, with respect to ∞, such that all primes dividing the conductor I split completely in K and $K \neq F \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$.

These hypotheses (a),(b),(c) are assumed for the remainder §§7.6-7.18 of this chapter.

(7.6.2) Let l be any prime number distinct from the characteristic of F. Let ρ be the 2-dimensional l-adic representation of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ corresponding to E where F^{sep} is the separable closure of F; that is to say ρ is the continuous homomorphism

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \otimes_F F^{\mathrm{sep}}, \mathbb{Q}_l)).$$

For each place v of F put

$$a_v = \mathrm{Tr}(\rho(\mathrm{Frob}_v) |\ H^1_{\text{ét}}(E \otimes_F F^{\mathrm{sep}}, \mathbb{Q}_l)^{I_v})$$

where I_v is the inertia subgroup of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ over v. The representation ρ satisfies

$$a_v \in \mathbb{Z} \text{ for all } v \in \Sigma_F$$

(see example 5.3.18).

(7.6.3) Let $\mathcal{H}(\rho)$ be the Heegner module of ρ and K/F with exceptional set of primes those dividing I and the place ∞ with coefficients in $\mathbb{Z}$ (see §5.3). By §4.7, there is a finite surjective morphism of curves over F

$$\pi : X_0^{\mathrm{Drin}}(I) \to E.$$

By example 5.3.18 there is a homomorphism of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\begin{aligned} \mathcal{H}(\pi) : \quad \mathcal{H}(\rho)^{(0)} &\to E(F^{\mathrm{sep}}) \\ < b, c > &\mapsto (b, I_1, c, \pi) \end{aligned}$$

for all $c \in \mathrm{Div}_+(A)$, $b \in \mathrm{Pic}(O_c)$. Here I_1 denotes a fixed ideal of B such that $I_1 I_1^\tau = IB$ and τ is the non-trivial element of $\mathrm{Gal}(K/F)$. The image of

this homomorphism $\mathcal{H}(\pi)$ consists of the $\mathbb{Z}$-linear combinations of Drinfeld-Heegner points of E rational over all the ring class fields $K[c]$ for all c.

(7.6.4) Let $< 0, 0 >$ be the element of the Heegner module $\mathcal{H}(\rho)^{(0)}$ given by the principal class of $\mathrm{Pic}(B)$, where B is the integral closure of A in K. Let

$$< 0, I_1, 0, \pi >= \mathcal{H}(\pi)(< 0, 0 >)$$

be the corresponding Drinfeld-Heegner point of $E(K[0])$ (see (4.8.2)). Let

$$x_0 = \mathrm{Tr}_{K[0]/K} < 0, I_1, 0, \pi > \in E(K).$$

7.6.5. Main Theorem. *Suppose that x_0 has infinite order in the group $E(K)$. Let $\mathcal{E}/k$ (resp. $\mathcal{E}'/k$) be a proper smooth model of the Néron model of the elliptic curve E/F (resp. $E \times_F K/K$). Then we have:*
(i) *$E(F)$ is a finite abelian group if $\epsilon = +1$, and is an abelian group of rank 1 if $\epsilon = -1$;*
(ii) *$E(K)$ is an abelian group of rank 1;*
(iii) *The Tate conjecture holds for the elliptic surfaces $\mathcal{E}/k$ and $\mathcal{E}'/k$ (see §1.1);*
(iv) *The Birch and Swinnerton-Dyer conjecture holds for the elliptic curves E/F and $E \times_F K/K$ (see* [Br2, Introduction]*);*
(v) *The Artin-Tate conjecture holds for the elliptic surfaces $\mathcal{E}/k$ and $\mathcal{E}'/k$ provided that* char.$(F) \neq 2$ *(see* [Br2, Introduction]*).*

Historical remarks on the Tate conjecture for surfaces over finite fields

(7.6.6) The special case of this theorem 7.6.5 where F is the rational field $\mathbb{F}_q(T)$, q is not a square, and $p \neq 2$, was proved in [Br2] by a similar method to that given here.

(7.6.7) The smooth projective surfaces X/k over the finite field k for which the Tate conjecture is also known are the following (for the exact references see [Br2, §1]):

(a) X/k is a product of 2 curves (Tate and Milne);
(b) X/k is a rational surface (Milne);
(c) X/k is a $K3$ surface equipped with a pencil of elliptic curves (Artin and Swinnerton-Dyer);
(d) X/k is a $K3$ surface of finite height and $p \geq 5$ (Nygaard and Ogus);
(e) Fermat surfaces $X_0^n + X_1^n + X_2^n + X_3^n = 0$ in $\mathbb{P}_k^3$ (Tate, Katsura and Shioda [SK]);
(f) X/k is birationally equivalent to a surface for which the Tate conjecture holds;

(g) X/k has a finite covering for which the Tate conjecture holds.

In particular, from (f) the main theorem 4.6.5 implies that the Tate conjecture holds for any projective surface in the birational equivalence classes of the surfaces $\mathcal{E}, \mathcal{E}'$ under the stated hypotheses.

There appears to be little in common in the proofs of the various results (a) to (e) above.

(7.6.8) For the case of elliptic surfaces over finite fields, the conjectures of Tate, Artin-Tate, and Birch Swinnerton-Dyer are known to be equivalent if the characteristic of the ground field is different from 2.

[For further details see §7.8 below.]

Kolyvagin's work on the Birch and Swinnerton-Dyer conjecture for elliptic curves over number fields

(7.6.9) Our proof of theorem 7.6.5 is close to Kolyvagin's method of proving the Birch and Swinnerton-Dyer conjecture for a class of elliptic curves over $\mathbb{Q}$.

(7.6.10) Kolyvagin's proof of the Birch and Swinnerton-Dyer conjecture for a class of elliptic curves over $\mathbb{Q}$ is contained in the papers [K1], [K2], [K4]; the paper [K2] is also an exposition of Kolyvagin's method of Euler systems, which with further amplification is also given in the book of Rubin [R1].

(7.6.11) To state one of the main results of Kolyvagin, let E be an elliptic curve over $\mathbb{Q}$ with conductor $N \in \mathbb{N}$. Let

$$\gamma : X_0(N) \to E$$

be a Weil parametrisation of E, where $X_0(N)$ is the modular curve over $\mathbb{Q}$ which classifies isomorphism classes of isogenies of elliptic curves $E' \to E''$ with cyclic kernel of order N.

[That such parametrisations exist is known for all semi-stable elliptic curves over $\mathbb{Q}$ by the results of Wiles [W].]

(7.6.12) Suppose that $L = \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field extension of $\mathbb{Q}$ where $D < 0$ satisfies that D is a quadratic residue modulo $4N$ and that $D \neq -3$ and $\neq -4$.

Let O_1 be the ring of integers of L and let I_1 be an ideal of O_1 such that

$$O_1/I_1 \cong \mathbb{Z}/N\mathbb{Z};$$

that such an ideal exists follows from the hypotheses imposed on D. If λ is a positive integer, denote by $L[\lambda]$ the ring class field of L with conductor λ. If

λ is a positive integer coprime to N, O_λ is the order

$$\mathbb{Z} + \lambda O_1$$

of L, and $I_\lambda = I_1 \cap O_\lambda$ is the corresponding ideal of O_λ, let z_λ be the Heegner point of $X_0(N)$ rational over $L[\lambda]$ corresponding to the isogeny of elliptic curves

$$\mathbb{C}/O_\lambda \to \mathbb{C}/I_\lambda^{-1}.$$

Put

$$y_\lambda = \gamma(z_\lambda) \in E(L[\lambda])$$

and put

$$P_1 = \sum_{g \in \mathrm{Gal}(L[1]/L)} g y_1.$$

Here $L[1]$ is the Hilbert class field of L, that is to say the maximal unramified abelian extension of L.

(7.6.13) Let O be the ring of endomorphisms of E and let Q be the fraction field of O. Let l be a rational prime number and let $T_l(E)$ be the l-adic Tate module of E. Let $B(E)$ denote the set of all odd rational prime numbers l which do not divide the discriminant of O and for which the homomorphism of continuous groups

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_O(T_l(E))$$

is surjective. It follows from the known galois action (see remark 7.2.8(2)) that $B(E)$ contains all but finitely many prime numbers; in particular, if $O = \mathbb{Z}$ and N is square-free then according to Mazur, all prime numbers $l \geq 11$ belong to $B(E)$.

7.6.14. Theorem. (Kolyvagin) *Suppose that P_1 has infinite order in $E(L)$. Then the group $E(L)$ has rank 1, the index $[E(L) : \mathbb{Z}P_1]$ is finite, the Tate-Shafarevich group $Ш(E, \mathbb{Q})$ is finite and has order dividing $d[E(L) : \mathbb{Z}P_1]^2$ where d is an integer coprime to all elements of $B(E)$.* □

(7.6.15) Kolyvagin also determines the structure of the Tate-Shafarevich group $Ш(E, \mathbb{Q})$ in terms of Heegner points, under the stated hypotheses.

Kato [Ka] has given another proof of the finiteness of the Tate-Shafarevich group of the modular elliptic curve $E/\mathbb{Q}$ under the hypothesis that $L(E, 1) \neq 0$; Kato defines an Euler system for $E/\mathbb{Q}$ different from that obtained from Heegner points using Beilinson elements in the K-theory of modular curves.

Kolyvagin in [K3] generalised the argument used to prove theorem 7.6.14 to include the case where P_1 may have finite order and rank $(E(K)) > 1$ but the argument relies strongly on hypotheses. Furthermore, Kolyvagin [K3] states a hypothetical condition on Heegner points generalising the condition

that P_1 have infinite order of theorem 7.6.14; Kolyvagin conjectures that this generalised condition always holds

[See the end of §7.14 below for an analogue of this conjecture for the present case of elliptic curves over function fields.]

An important special case of Kolyvagin's work on the Birch and Swinnerton-Dyer conjecture is clearly explained in [GB2]. See also [PR] for more details.

(7.6.16) Bertolini and Darmon [BDa] made a further refinement of Kolyvagin's theorem 7.6.14 by considering isotypical components of Mordell-Weil groups. To state the result of Bertolini and Darmon, let $G = \mathrm{Gal}(L[1]/L)$. The group G acts naturally on the abelian group $E(L[1])$ and $E(L[1]) \otimes_{\mathbb{Z}} \mathbb{C}$ decomposes as a sum of eigenspaces under G

$$E(L[1]) \otimes_{\mathbb{Z}} \mathbb{C} \cong \bigoplus_{\chi} E(L[1])^{\chi}$$

where the sum runs over all irreducible complex characters $\chi : G \to \mathbb{C}^*$ of G. Put

$$e_{\chi} = \frac{1}{|G|} \sum_{g \in G} \chi^{-1}(g) g.$$

Then e_{χ} is an idempotent in the group ring $\mathbb{C}[G]$ giving the projection onto the χ-eigenspace.

7.6.17. Theorem. (Bertolini, Darmon [BDa]) *Suppose that E does not have complex multiplication and that $e_{\chi} y_1 \neq 0$ in $E(L[1])] \otimes_{\mathbb{Z}} \mathbb{C}$. Then we have* $\dim_{\mathbb{C}} E(L[1])^{\chi} = 1$. □

(7.6.18) Bertolini and Darmon [BDa] prove a more precise result under the stated hypotheses, namely that the p-component of the Tate-Shafarevich group of the curve $E \times L[1]/L[1]$ is trivial for infinitely many prime numbers p. The theorem 7.6.14 of Kolyvagin implies the special case of the theorem 7.6.17 of Bertolini and Darmon when χ is the trivial character.

(7.6.19) The method of Kolyvagin's Euler systems also applies to ideal class groups of number fields. In particular, Kolyvagin and Rubin [Ru4] prove by this method the "main conjecture" of Iwasawa theory first proved by Mazur and Wiles [MW].

Rubin's work on the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication over number fields

(7.6.20) Prior to the work of Kolyvagin, Rubin gave the first known examples of elliptic curves with finite Tate-Shafarevich groups. His method applies to elliptic curves over number fields with complex multiplication.

To state one of the main results of Rubin, let E be an elliptic curve defined over an imaginary quadratic extension L of $\mathbb{Q}$ and with complex multiplication. Let $L(E, s)$ be the L-function of E/L.

7.6.21. Theorem. (Rubin, [R2]) *Suppose that* $L(E, 1) \neq 0$. *Then we have*
(i) *the group* $E(L)$ *is finite;*
(ii) *the Tate-Shafarevich group* $Ш(E, K)$ *is finite;*
(iii) *for every prime number* $p > 7$ *such that* E *has good reduction above* p, *the* p*-part of the Tate-Shafarevich group* $Ш(E, K)$ *is finite and has the order predicted by the Birch and Swinnerton-Dyer conjecture.*□

(7.6.22) Part (i) of this theorem was already known and is due to Coates and Wiles [CW]. Rubin [Ru3] has also proved a stronger version of part (iii) of this theorem. See also [PR] for more details.

7.7 Tate-Shafarevich groups

For the rest of this chapter the notation is that of (7.5.1).

(7.7.1) Let E/F be an elliptic curve. Let $\mathcal{E}_0/C$ be the Néron model of E/F; then $\mathcal{E}_0/C$ may be considered as a sheaf of abelian groups on C for the étale topology. The *Tate-Shafarevich group of* E/F is defined to be

$$Ш(E, F) = H^1_{\text{ét}}(C, \mathcal{E}_0).$$

As k is a perfect field, this is equivalent to the usual definition that $Ш(E, F)$ is the group of principal homogeneous spaces of E/F which are everywhere locally trivial [Gro, Complément 4.9].

7.7.2. Remarks. (1) The Tate-Shafarevich group $Ш(E, F)$ is known to be a torsion group and is *conjectured* to be a finite group. This conjecture is almost identical with the conjectures of Tate, Artin-Tate, and Birch and Swinnerton-Dyer for the elliptic curve F/F and the corresponding elliptic surface over k.

[See [Gro], [T3], [M1], [M3], as well as remark 7.7.6(3) below, for the relations between these conjectures.]

(2) More precisely, $Ш(E,F)$ is known to be a torsion group of cofinite type: for every prime number l, there is an integer $r(l)$ such that there is an isomorphism of groups

$$Ш(E,F)_{l^\infty} \cong G_l \oplus \left(\frac{\mathbb{Q}_l}{\mathbb{Z}_l}\right)^{r(l)}.$$

where G_l is a finite l-group and G_l is trivial for all but finitely many prime numbers l. The conjecture that $Ш(E,F)$ be finite is then equivalent to the statement that $r(l) = 0$ for all prime numbers l.

That $Ш(E,F)$ is a torsion group of cofinite type follows from the known structure of the Tate-Shafarevich group $Ш(E \times_k \overline{k}, F \times_k \overline{k})$ for the elliptic curve $E \times_k \overline{k}$ over the field $F \times_k \overline{k}$, where $\overline{k}$ denotes the algebraic closure of the finite field k (formula of Grothendieck-Ogg-Shafarevich, see [Ra]).

(7.7.3) Assume the hypotheses (7.6.1) for the elliptic curve E/F hold. If the Drinfeld-Heegner point x_0 of (7.6.4) has infinite order of $E(K)$, for each prime number l let $t(l)$ be the greatest integer such that

$$x_0 \in l^{t(l)} E(K). \tag{7.7.4}$$

As $E(K)$ is a finitely generated abelian group (Mordell-Weil theorem), if x_0 has infinite order then the integer $t(l)$ exists for all l and is zero for all except finitely many prime numbers l.

7.7.5. Theorem. *Suppose that x_0 has infinite order in the group $E(K)$. Then x_0 generates a subgroup of finite index of $E(K)$ and there is an infinite set of prime numbers $\mathcal{P}_0$ such that*
(i) *the highest power of l dividing the index $[E(K) : \mathbb{Z}x_0]$ is at most $l^{6t(l)}$ for all $l \in \mathcal{P}_0$;*
(ii) $l^{2t(l)} Ш(E/F)_{l^\infty} = l^{2t(l)} Ш(E \times_F K/K)_{l^\infty} = 0$ *for all $l \in \mathcal{P}_0$.*

7.7.6. Remarks. (1) The set $\mathcal{P}_0$ of prime numbers is obtained from the set $\mathcal{P}$ of prime numbers of definition 7.10.3 below by deleting a finite set of primes. Hence (see remark 7.10.4 below) the set $\mathcal{P}_0$ consists of all but finitely many prime numbers l of the form $2^s n + 1$ where $s \geq 1$ and n is odd such that $q = |k|$ is a 2^sth power non-residue modulo l.

(2) The method of proof of theorem 7.7.5 given below should extend to all prime numbers and not just those primes in $\mathcal{P}_0$. For this it is necessary to consider the Heegner module $\mathcal{H}_c$ where c is a general divisor on Spec A. Below we only consider the Heegner module $\mathcal{H}_c$ where c is a divisor on Spec A which is a sum of prime divisors which are inert and unramified in K/F. This is precisely the reason for the restriction $l \in \mathcal{P}_0$ in theorem 7.7.5 above.

(3) Let $p > 0$ be the characteristic of the field F. Then it is known that if $Ш(E/F)_{l^\infty}$ is finite for one prime number l then the Tate-Shafarevich group $Ш(E/F)$ is a finite group. This is proved by Kato and Trihan in [KT] and refines earlier results of a similar kind due to Tate [T3, Theorem 5.2] and Milne [M1, Theorem 8.1].

Theorem 7.7.5(ii) above therefore shows that the Tate-Shafarevich groups in question are finite and gives explicit annihilators for the l-primary components for all $l \in \mathcal{P}_0$.

Note that for elliptic curves defined over number fields, the implication corresponding to that proved by Kato and Trihan (loc. cit.) is not known in general.

7.8 Proof that theorem 7.7.5 implies theorem 7.6.5

That theorem 7.7.5 implies the main theorem 7.6.5 is a consequence of known results on the relation between the conjectures of Tate, Artin-Tate, and Birch-Swinnerton Dyer (due to Artin, Tate, Milne, Kato and Trihan).

To be precise, let E_0/F_0 be an elliptic curve over a global field F_0 which is one of the following two possibilities

(a) $E_0 = E$ and $F_0 = F$;
(b) $E_0 = E \times_F K$ and $F_0 = K$.

Let C_0/k be the smooth projective curve whose function field is isomorphic to F_0. Let $\mathcal{E}_0/k$ denote the Néron model of the elliptic curve E_0/F_0. Then there is a smooth morphism of k-schemes

$$\mathcal{E}_0 \to C_0.$$

Let $\mathcal{E}/k$ denote the minimal proper smooth model of the surface $\mathcal{E}_0$. Then the corresponding morphism

$$\mathcal{E} \to C_0$$

admits a section and is proper with geometrically connected fibres. We then have isomorphisms between the Brauer group and Tate-Shafarevich group ([Gro, Proposition 4.3, Corollaire 4.4] or [T3, Proposition 3.1]), where $\mathrm{Br}(\mathcal{E}/k) = H^2_{\text{ét}}(X, \mathbb{G}_m)$,

$$\mathrm{Br}(\mathcal{E}/k) \cong Ш(E_0/F_0). \tag{7.8.1}$$

By theorem 7.7.5 and (7.8.1) we obtain that $\mathrm{Br}(\mathcal{E}/k)_{l^\infty}$ is finite for infinitely many prime numbers l. Therefore by [T3, Theorem 6.2] the Tate conjecture holds for the surface $\mathcal{E}/k$; by [M1, M3], the Artin-Tate conjecture then holds for $\mathcal{E}/k$ provided that char.$(F_0) \neq 2$. By [KT], the Birch and Swinnerton-Dyer conjecture then holds for the elliptic curve E_0/F_0. □

7.9 The Selmer group

(7.9.1) In this section the index set of all quasi-groups is $\mathbb{N}^{(p)}$ which is the set of positive integers prime to p, where p the characteristic of the global field F (see §7.1 for more details on quasi-groups).

(7.9.2) For a place v of the field F, we write F_v for the completion of F at the place v. We have a commutative diagram of quasi-groups, where the maps res_v are the restriction homomorphisms and the rows are exact sequences

$$\begin{array}{ccccccccc} 0 & \to & {}_*E(F) & \to & H^1(F, E(F^{\mathrm{sep}})_*) & \to & H^1(F, E(F^{\mathrm{sep}}))_* & \to & 0 \\ & & \downarrow & & \downarrow \mathrm{res}_v & & \downarrow \mathrm{res}_v & & \\ 0 & \to & {}_*E(F_v) & \to & H^1(F_v, E(F_v^{\mathrm{sep}})_*) & \to & H^1(F_v, E(F_v^{\mathrm{sep}}))_* & \to & 0 \end{array}$$

As in example 7.1.7(1), ${}_*E(F)$ denotes the quasi-group $\{E(F)/nE(F)\}_{n\in\mathbb{N}^{(p)}}$ and $E(F^{\mathrm{sep}})_*$ denotes the quasi-group $\{E(F^{\mathrm{sep}})_n\}_{n\in\mathbb{N}^{(p)}}$ given by the n-torsion subgroups associated to $E(F^{\mathrm{sep}})$ where n ranges over all positive integers prime to the characteristic of F.

(7.9.3) The Tate-Shafarevich group $Ш(E/F)$ of E/F is then given equivalently as [Gro, Complément 4.9]

$$Ш(E/F) = \ker\{H^1(F, E) \to \prod_{v\in\Sigma_F} H^1(F_v, E)\}.$$

The Selmer quasi-group is defined as

$$S^{(*)}(E/F) = \bigcap_{v\in\Sigma_F} \mathrm{res}_v^{-1}({}_*E(F_v)).$$

Thus $S^{(*)}(E/F)$ is a sub-quasi-group of $\{H^1(F, E(F^{\mathrm{sep}})_n)\}_{n\in\mathbb{N}^{(p)}}$. Each component $S^{(n)}(E/F)$ of the Selmer quasi-group is a finite abelian group. We then have the exact sequence of torsion abelian quasi-groups

$$0 \to {}_*E(F) \to S^{(*)}(E/F) \to Ш(E/F)_* \to 0.$$

For the imaginary quadratic extension field K of F we write $Ш(E/K)$ in place of $Ш(E\times_K K/K)$; similarly, for the Selmer quasi-group, we write $S^{(*)}(E/K)$ in place of $S^{(*)}(E\times_F K/K)$.

7.9.4. Proposition. *If n is an odd integer, the restriction homomorphism provides an isomorphism*

$$Ш(E/F)_n \xrightarrow{\text{res}}_{\cong} Ш(E/K)_n^{\mathrm{Gal}(K/F)}.$$

Proof. The definition of the Tate-Shafarevich groups provides a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \to & Ш(E/K)^{\mathrm{Gal}(K/F)} & \to & H^1(K,E)^{\mathrm{Gal}(K/F)} & \to & \Big(\prod_{v\in\Sigma_K} H^1(K_v,E)\Big)^{\mathrm{Gal}(K/F)} \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \to & Ш(E/F) & \to & H^1(F,E) & \to & \prod_{v\in\Sigma_F} H^1(F_v,E)
\end{array}$$

For any place v of F, the F_v-algebra $F_v \otimes_F K$ is étale and is the product of the completions of K at the places lying over v. The inflation restriction sequence provides isomorphisms because n is an odd integer and $\mathrm{Gal}(K/F)$ has order 2

$$\begin{aligned}
&H^1(F,E)_n \cong H^1(K,E)_n^{\mathrm{Gal}(K/F)} \\
&H^1(F_v,E)_n \cong H^1(F_v \otimes_F K,E)_n^{\mathrm{Gal}(K/F)} \text{ for all places } v \text{ of } F.
\end{aligned}$$

The isomorphism of the proposition now follows by a diagram chase.□

7.9.5. Remark. It may be shown that if the characteristic of F is not equal to 2 then the restriction homomorphism of Tate-Shafarevich groups

$$Ш(E/F) \longrightarrow Ш(E/K)^{\mathrm{Gal}(K/F)}$$

has finite kernel and cokernel which are elementary abelian 2-groups.

7.10 The set $\mathcal{P}$ of prime numbers

We define a set $\mathcal{P}$ of prime numbers by arithmetic conditions; the purpose of this definition is that for all but finitely any prime numbers l of $\mathcal{P}$ we shall prove that the l-primary component of the Tate-Shafarevich group $Ш(E/F)$ of E/F is finite and give an explicit annihilator, under the hypotheses of theorem 7.7.5.

(7.10.1) For a place v of F, let

F_v denote the completion of F at v;
F_v^{nr} denote the maximal unramified extension of the local field F_v (that is, F_v^{nr} is the field of fractions of the strict henselisation of the valuation ring of F_v);
O_v denote the discrete valuation ring of the local field F_v;
$\mathcal{E}$ denote the Néron model of the elliptic curve $E \times_F F_v/F_v$ over O_v;
$\mathcal{E}_0$ denote the closed fibre of $\mathcal{E}/O_v$;
$\pi_0(\mathcal{E}_0)$ be the group of connected components of $\mathcal{E}_0$ as a $\mathrm{Gal}(F_v^{\mathrm{nr}}/F_v)$-module.

7.10.2. Theorem. ([M4, Prop. 1.3.8]). *Write $G = \mathrm{Gal}(F_v^{\mathrm{nr}}/F_v)$. There is an isomorphism*

$$H^1(G, E(F_v^{\mathrm{nr}})) \cong H^1(G, \pi_0(\mathcal{E}_0)).$$

In particular, $H^1(G, E(F_v^{\mathrm{nr}}))$ is a finite group for all v and if E has good reduction at v then $H^1(G, E(F_v^{\mathrm{nr}})) = 0$. □

7.10.3. Definition. We may select an infinite set $\mathcal{P}$ of prime numbers (in fact $\mathcal{P}$ has positive Dirichlet density) such that for all $l \in \mathcal{P}$ we have

(a) p, 2, and the prime factors of $|B^*|/|A^*|$ are not in $\mathcal{P}$;
(b) $H^i(K(E_{l^n})/K, E_{l^n}) = 0$ for all integers $n \geq 1$ and for all $i \geq 0$ (see proposition 7.3.1);
(c) the natural map $\mathrm{Gal}(F(E_{l^\infty})/F) \to \hat{\Gamma}_l$ is an isomorphism (see §7.2 and Igusa's theorem 7.2.3);
(d) $H^1(K_z^{\mathrm{nr}}/K_z, E)_{l^\infty} = 0$ for all places z of K (see theorem 7.10.2 above);
(e) K and $F(E_{l^\infty})$ are linearly disjoint over F (see proposition 7.3.10);
(f) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{Gal}(F(E_{l^\infty})/F)$ (see proposition 7.3.10, which is a consequence of Igusa's theorem 7.2.2);

7.10.4. Remark. The first 5 conditions (a),(b),(c),(d),(e) of this definition hold for all except finitely many prime numbers l. Only the last condition (f) fails to hold in general for all but finitely many prime numbers.

The set $\mathcal{P}$ can therefore be obtained from the set S of prime numbers provided by proposition 7.3.10 by deleting a finite number of elements. That is to say (see remark 7.3.14(1)) the set $\mathcal{P}$ consists of all but finitely many prime numbers l of the form $2^s n + 1$ where $s \geq 1$ and n is odd such that $q = |k|$ is a 2^sth power non-residue modulo l.

7.11 Frobenius elements and the set $\mathcal{D}_{l^n}$ of divisors

The set $\mathcal{D}_{l^n}$ is defined for any prime number l in $\mathcal{P}$ and contains only effective divisors on Spec A consisting of sums of distinct prime divisors whose corresponding Frobenius conjugacy classes in $\mathrm{Gal}(K(E_{l^n})/F)$ are all the same. This unique Frobenius conjugacy class is of a special kind, in particular its elements have order 2.

(7.11.1) For each integer $n \geq 1$ and each $l \in \mathcal{P}$ let $\tau_\infty \in \mathrm{Gal}(K(E_{l^n})/F)$ be the unique element satisfying the two conditions:

(a) $\tau_\infty|_{F(E_{l^n})} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

(b) $\tau_\infty|_K$ is the non $-$ trivial element of $\mathrm{Gal}(K/F)$.

We write τ for the non-trivial element of $\mathrm{Gal}(K/F)$. The elements τ, τ_∞ have exact order 2.

(7.11.2) For any semi-simple $\mathbb{Z}[\mathrm{Gal}(K/F)]$-module M, we have a decomposition of M as a sum of eigenspaces

$$M \cong M^+ \oplus M^-$$

where M^ϵ, for $\epsilon = \pm$, is the submodule of M on which τ acts like $\epsilon 1$.

7.11.3. Definition. (i) For a prime divisor z in Spec A, unramified in $K(E_{l^n})$, let Frob_z denote the conjugacy class of $\mathrm{Gal}(K(E_{l^n})/F)$ containing the Frobenius substitutions of the prime factors of z.
(ii) For $l \in \mathcal{P}$, let $\mathcal{D}_{l^n}$ be the set of effective divisors on Spec A, of support prime to $\mathrm{Supp}(I)$ and the discriminant of K/F, all of whose prime components z have multiplicity 1 and satisfy

$$\mathrm{Frob}_z(K(E_{l^n})/F) = [\tau_\infty]$$

where $[\tau_\infty]$ denotes the conjugacy class of τ_∞. The prime divisors in $\mathcal{D}_{l^n}$ are infinite in number, by the Chebotarev density theorem, remain prime in the field extension K/F, and their liftings to K split completely in $K(E_{l^n})/K$. Furthermore, E has good reduction at all prime divisors of $\mathcal{D}_{l^n}$.

(7.11.4) For any prime number λ distinct from the characteristic of F, let

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}_{\mathbb{Q}_\lambda}(T_\lambda(E) \otimes_{\mathbb{Z}_\lambda} \mathbb{Q}_\lambda)$$

denote the galois representation on the λ-adic Tate module $T_\lambda(E)$ of the

elliptic curve E; that is to say

$$T_\lambda(E) \otimes_{\mathbb{Z}_\lambda} \mathbb{Q}_\lambda = H^1_{\text{ét}}(E \otimes_F F^{\text{sep}}, \mathbb{Q}_\lambda)^*$$

where $*$ denotes the dual $\mathbb{Q}_\lambda$-vector space.

If z is a prime of F let I_z be an inertia subgroup of $\text{Gal}(F^{\text{sep}}/F)$ at z; let

$$a_z = \text{Tr}(\rho(\text{Frob}_z) \mid (T_\lambda(E) \otimes_{\mathbb{Z}_\lambda} \mathbb{Q}_\lambda)^{I_z}).$$

That is to say, a_z is the trace of the Frobenius at z on the part of the Tate module invariant under I_z. Then we have $a_z \in \mathbb{Z}$ (see examples 5.3.18(1)).

7.11.5. Lemma. *Suppose that $z \in \mathcal{D}_{l^n}$ is a prime divisor, where $l \in \mathcal{P}$.*
(i) *We have $a_z \equiv |\kappa(z)| + 1 \equiv 0 \pmod{l^n}$.*
(ii) *If $\mathcal{E}_{0,z}$ denotes the reduction modulo z of the Néron model of E/F then we have group isomorphisms, for $\epsilon = +$ or $-$,*

$$\mathcal{E}_{0,z}(\kappa(z^\sharp))^\epsilon_{l^n} \cong \mathcal{E}_{0,z}(\kappa(z))_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}.$$

Proof. As a_z is the trace of a Frobenius above z we have by the trace formula, where $\kappa(z)$ is the residue field of A at z,

$$a_z = |\kappa(z)| + 1 - |\mathcal{E}_{0,z}(\kappa(z))|.$$

Let K' be the field $K(E_{l^n})$. As $z \in \mathcal{D}_{l^n}$, the prime z is a place of good reduction of E/F (see (7.11.3)). Hence the characteristic polynomial of the Frobenius $\text{Frob}_z(K'/F)$ above z acting on E_{l^n} is equal to

$$X^2 - a_z X + |\kappa(z)| \quad (\text{modulo } \ l^n).$$

Let σ be the element of $\text{Aut}(E_{l^n})$ given by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then the characteristic polynomial of the element σ is equal to

$$X^2 - 1.$$

Comparing these two polynomials modulo l^n proves part (i) of the lemma, as $\text{Frob}_z(K'/F) = [\tau_\infty]$ acts like σ on E_{l^n}.

For (ii), let $z^\sharp$ be the unique place of K lying over the place z of F where $z \in \mathcal{D}_{l^n}$. Then $\kappa(z^\sharp)$ is a quadratic extension of $\kappa(z)$. Furthermore, as $\text{Frob}_z(K'/F) = [\tau_\infty]$ where τ_∞ has order 2 (see (7.11.1), (7.11.3)), the prime $z^\sharp$ splits completely in the extension K'/K. The map of reduction modulo a prime of K' over z

$$E(K')_{l^n} \to \mathcal{E}_{0,z}(\kappa(z^\sharp))_{l^n}$$

is an isomorphism. Hence we have

$$\mathcal{E}_{0,z}(\kappa(z^\sharp))_{l^n} \cong \left(\frac{\mathbb{Z}}{l^n\mathbb{Z}}\right)^2.$$

The action of τ_∞ on $\mathcal{E}_{0,z}(\kappa(z^\sharp))$ decomposes into a sum over the eigenspaces corresponding to $\tau_\infty = \pm 1$. Hence we have for $\epsilon = \pm$, as the Frobenius $\mathrm{Frob}_z(K'/F) = [\tau_\infty]$ acts on $E(K')_{l^n}$ like the element σ,

$$\mathcal{E}_{0,z}(\kappa(z^\sharp))_{l^n}^{\tau_\infty=\epsilon} \cong \mathbb{Z}/l^n\mathbb{Z}.$$

On the other hand we have

$$\mathcal{E}_{0,z}(\kappa(z^\sharp))^{\tau_\infty=+1} = \mathcal{E}_{0,z}(\kappa(z)).$$

The result follows from this.□.

7.12 The Heegner module attached to E/F

(7.12.1) Let λ be a prime number distinct from the characteristic of the field F.

As in (7.11.4), let ρ be the representation of the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ given by the λ-adic Tate module $T_\lambda(E)$ of the elliptic curve E

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}_{\mathbb{Q}_\lambda}(T_\lambda(E) \otimes_{\mathbb{Z}_\lambda} \mathbb{Q}_\lambda).$$

The character of the representation ρ we denote by the same symbol ρ; as the character of this representation takes values in $\mathbb{Z}$, rather than $\mathbb{Z}_\lambda$, we have a map of sets

$$\rho : \Sigma_F \to \mathbb{Z}$$
$$v \mapsto a_v = \mathrm{Tr}(\rho(\mathrm{Frob}_v)|(T_\lambda(E) \otimes_{\mathbb{Z}_\lambda} \mathbb{Q}_\lambda)^{I_v}).$$

where I_v is an inertia subgroup of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ at v.

(7.12.2) Let

$$\pi : X_0^{\mathrm{Drin}}(I) \to E$$

be the surjective morphism of F-schemes given by §4.7 and example 5.3.18(1), where the ideal I of A is the conductor of the elliptic curve E/F without the component at ∞.

(7.12.3) Let K/F be an imaginary quadratic field extension in which all primes dividing the conductor of E, except the place ∞, split completely in K/F. Let $\mathcal{H}(\rho)$ be the Heegner module (see §5.3) of the character ρ

$$\rho : \Sigma_F \setminus (\mathrm{Supp}(I) \cup \{\infty\}) \to \mathbb{Z}, \quad v \mapsto a_v,$$

the imaginary quadratic extension K/F, with exceptional set the set of primes ∞ and those dividing the conductor I, and with coefficients in $\mathbb{Z}$. The morphism π induces a homomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules $\mathcal{H}(\pi)$ (see examples 5.3.18(1))

$$\begin{aligned}\mathcal{H}(\pi) : \mathcal{H}(\rho)^{(0)} &\to E(K^{\mathrm{sep}}) \\ < b, c > &\mapsto (b, I_1, c, \pi).\end{aligned}$$

Here I_1 denotes a fixed ideal of B such that $I_1 I_1^{\tau} = IB$ and τ is the non-trivial element of $\mathrm{Gal}(K/F)$.

(7.12.4) The module $\mathcal{H}(\rho)$ is a direct limit

$$\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$$

where the limit runs over all effective divisors c on Spec A. For each divisor c, we have a homomorphism of $\mathrm{Gal}(K[c]/K)$-modules

$$\mathcal{H}(\pi)_c : \mathcal{H}_c^{(0)} \to E(K[c])$$

which is obtained by composing the transition homomorphism $\mathcal{H}_c \to \mathcal{H}(\rho)$ with $\mathcal{H}(\pi)$.

7.13 Galois invariants of the Heegner module and the map η

The main result of this section, proposition 7.13.4, identifies part of $(\mathcal{H}_{c,S})^{G(c/0)}$, which is the submodule of the Heegner module $\mathcal{H}_{c,S}$ invariant under the action of the Galois group $G(c/0)$. This result is restricted to divisors c satisfying the conditions of the proposition, in particular that the prime components of c are inert and unramified in K/F. The proposition applies in particular to all divisors c in the set $\mathcal{D}_{l^n}$ for any prime number l in $\mathcal{P}$. That part of the module $(\mathcal{H}_{c,S})^{G(c/0)}$ given by the proposition corresponds to the "derivative" cohomology classes of Kolyvagin (see for example [Ru1, §4.4]).

(7.13.1) Let

$m \geq 1$ be a positive integer prime to the characteristic of F and prime to the order of the group B^*/A^*;
S be the ring $\frac{\mathbb{Z}}{m\mathbb{Z}}$;
$\rho : \Sigma_F \setminus (\mathrm{Supp}(I) \cup \{\infty\}) \to \mathbb{Z}$ the character of the l-adic representation attached to E/F (see (7.12.3));

$\mathcal{H}(\rho_S, S) = \varinjlim \mathcal{H}_{c,S}$ be the Heegner module of ρ, K/F and with coefficients in S where ρ_S is the composite of ρ with the natural surjection $\mathbb{Z} \to S$; $G(c/0) = \mathrm{Gal}(K[c]/K[0])$ for any divisor c of $\mathrm{Div}_+(A)$ (see §6.1).

The ring S is a direct product of infinitesimal traits corresponding to the prime factors of m. For an element $a \in \mathbb{Z}$ we write $a \otimes 1$ for its image in the algebra S.

(7.13.2) We have isomorphisms of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules as $|B^*/A^*|$ is a unit of S (see §5.9, corollary 5.9.5)

$$\mathcal{H}(\rho) \otimes_{\mathbb{Z}} S \cong \mathcal{H}(\rho_S, S), \quad \mathcal{H}_c \otimes_{\mathbb{Z}} S \cong \mathcal{H}_{c,S}.$$

The homomorphism

$$\mathcal{H}(\pi)_c : \mathcal{H}_c^{(0)} \to E(K[c])$$

then provides a homomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\pi)_c \otimes_{\mathbb{Z}} S : \mathcal{H}_{c,S}^{(0)} \to E(K[c]) \otimes_{\mathbb{Z}} S.$$

(7.13.3) If $h \in \mathcal{H}_{c,\mathbb{Z}}$ we write $[h]$ for its image in $\mathcal{H}_{c,S}$, that is to say $[h]$ is the reduction modulo m of h. Similarly, for an element $x \in E(K[c])$ we write $[x]$ for its image in $E(K[c]) \otimes_{\mathbb{Z}} S$.

7.13.4. Proposition. *Let $c \in \mathrm{Div}_+(A)$ where $c = \sum_{i=1}^r z_i$ is a sum of distinct prime divisors z_i such that z_i is unramified and inert in K/F and $z_i \notin \mathrm{Supp}(I)$ for all i. Let $M(c)$ be the S-module (where the tensor products are over S)*

$$M(c) = \bigotimes_i{}_S \ \mathrm{Hom}(G(c/c - z_i), S) \otimes_S \bigotimes_i{}_S \ \mathrm{Ann}_S(a_{z_i} \otimes 1).$$

Then there is commutative diagram of $\Delta_{c,S}$-modules

$$\begin{array}{ccc} (\mathcal{H}_{c,S})^{G(c/0)} & \xrightarrow{h} & \mathcal{H}_{0,S} \otimes_S M(c) \\ \eta \uparrow & & \uparrow e_{G(c/0)} \\ \mathcal{H}_{c,S} \otimes_S M(c) & \xrightarrow{\zeta} & \mathcal{H}'_{c,S} \otimes_S M(c) \end{array} \tag{7.13.5}$$

where $h, e_{G(c/0)}$ are surjective homomorphisms, ζ is induced from the natural surjection $\mathcal{H}_{c,S} \to \mathcal{H}'_{c,S}$ (see (5.7.4)), and η is obtained from Kolyvagin elements.

Proof. As $S = \mathbb{Z}/m\mathbb{Z}$ is a direct product of infinitesimal traits we may immediately reduce to the case where S itself is an infinitesimal trait of the form $\mathbb{Z}/q^r\mathbb{Z}$ where q is a prime number.

Definition of h. Let S be an infinitesimal trait where $|B^*/A^*|$ is a unit of S and let N be a S-module of finite type. Then we have an isomorphism of S-modules

$$N \cong \bigoplus_j S/I_j$$

where I_j are ideals of S. Hence we have

$$(\mathcal{H}_{c,S} \otimes_S N)^{G(c/c-z_i)} \cong \bigoplus_j (\mathcal{H}_{c,S/I_j})^{G(c/c-z_i)}.$$

By theorem 6.10.7 in view of the hypothesis on $c = \sum_i z_i$, we have the exact sequences for all i

$$0 \to \mathcal{H}_{c-z_i,S} \to (\mathcal{H}_{c,S})^{G(c/c-z_i)} \to H^1(G(c/c-z_i), S) \otimes_S \mathrm{Ann}_S(a_{z_i} \otimes 1)\mathcal{H}_{c-z_i,S} \to 0.$$

Hence we obtain a surjective homomorphism of $\Delta_{c-z_i,S}$-modules, as $\mathrm{Ann}_S(a_{z_i} \otimes 1) \otimes_S \frac{S}{I_j} \cong \mathrm{Ann}_{S/I_j}(a_{z_i} \otimes 1)$,

$$(\mathcal{H}_{c,S} \otimes_S N)^{G(c/c-z_i)} \to \bigoplus_j H^1(G(c/c-z_i), S/I_j) \otimes_S \mathrm{Ann}_{S/I_j}(a_{z_i} \otimes 1)\mathcal{H}_{c-z_i,S/I_j}$$

$$\cong \bigoplus_j \left\{ H^1(G(c/c-z_i), S) \otimes_S \frac{S}{I_j} \otimes_S \mathrm{Ann}_{S/I_j}(a_{z_i} \otimes 1)(\mathcal{H}_{c-z_i,S} \otimes_S \frac{S}{I_j}) \right\}$$

$$\cong \mathrm{Ann}_S(a_{z_i} \otimes 1)\mathcal{H}_{c-z_i,S} \otimes_S N \otimes_S H^1(G(c/c-z_i), S)$$

$$\cong \mathcal{H}_{c-z_i,S} \otimes_S N \otimes_S \left\{ H^1(G(c/c-z_i), S) \otimes_S \mathrm{Ann}_S(a_{z_i} \otimes 1) \right\}.$$

That is to say, we have a surjective homomorphism of $\Delta_{c-z_i,S}$-modules

$$h_i : (\mathcal{H}_{c,S} \otimes_S N)^{G(c/c-z_i)} \to \mathcal{H}_{c-z_i,S} \otimes_S N'$$

where

$$N' = N \otimes_S \left\{ \mathrm{Hom}(G(c/c-z_i), S) \otimes_S \mathrm{Ann}_S(a_{z_i} \otimes 1) \right\}$$

is also a S-module of finite type.

By induction on the number of components of c we obtain from h_i a surjective homomorphism, where the tensor products are over the artin ring S,

(7.13.6)

$$\mathcal{H}_{c,S}^{G(c/0)} \to \mathcal{H}_{0,S} \otimes_S \Big(\bigotimes_i \mathrm{Hom}(G(c - \sum_{j \le i} z_j / c - \sum_{j \le i+1} z_j), S) \Big) \otimes_S \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1).$$

For all $i \ge 0$, the restriction map provides a surjective homomorphism

$$G(c/c-z_i) \to G(c - \sum_{j \le i-1} z_j / c - \sum_{j \le i} z_j)$$

whose kernel has order dividing $|B^*|/|A^*|$ (see the isomorphisms (2.3.8) and (2.3.10)). As the group B^*/A^* has order which is a unit in S (7.13.1), we obtain the isomorphism of S-modules where the tensor products are over the algebra S

$$\bigotimes_i \mathrm{Hom}(G(c/c-z_i),S) \;\cong\; \bigotimes_i \mathrm{Hom}(G(c-\sum_{j\le i-1} z_j/c-\sum_{j\le i} z_j),S).$$

The homomorphism of (7.13.6) combined with this isomorphism defines the homomorphism h of the diagram (7.13.5)

$$h : (\mathcal{H}_{c,S})^{G(c/0)} \to \mathcal{H}_{0,S} \otimes_S M(c).$$

Definition of η. Let $\mathfrak{p}_i$ be the ideal of A corresponding to the prime divisor z_i. Then by (2.3.7) we have group isomorphisms

$$G(c/c-z_i) \cong (B/\mathfrak{p}_i B)^*/(A/\mathfrak{p}_i)^* \quad \text{if} \quad c \neq z_i$$

$$G(c/0) \cong \frac{\prod_i (B/\mathfrak{p}_i B)^*/(A/\mathfrak{p}_i)^*}{B^*/A^*}.$$

Hence there is a surjective group homomorphism

$$f : \prod_i G(c/c-z_i) \quad \to \quad G(c/0)$$

whose kernel has order dividing a power of $|B^*/A^*|$. Furthermore, the group $G(c/0)$ is the product of its subgroups $G(c/c-z_i)$ for all i.
Let ψ_i be group homomorphisms with values in the additive group of S where

$$\psi_i \in \mathrm{Hom}(G(c/c-z_i),S) \quad \text{for all } i.$$

Let ψ_0 be the multilinear map

$$\psi_0 : \prod_i G(c/c-z_i) \to S$$
$$(g_1,\ldots,g_m) \mapsto \prod_i \psi_i(g_i).$$

The kernel of the natural homomorphism $\prod_i G(c/c-z_i) \to G(c/0)$ has order which is a unit of S. It follows that if $h_1, h_2 \in \prod_i G(c/c-z_i)$ are such that $h_1 h_2^{-1}$ is in the kernel of $\prod_i G(c/c-z_i) \to G(c/0)$ then $\psi_0(h_1) = \psi_0(h_2)$; for we have

$$h_i = (g_1^{(i)},\ldots,g_r^{(i)}) \quad \text{for } i = 1,2;$$

hence we have

$$\psi_0(h_1) = \prod_j \psi_j(g_j^{(1)}) = \prod_j \psi_j(g_j^{(2)}) = \psi_0(h_2).$$

Hence the map ψ_0 factors though a map $\psi : G(c/0) \to S$ where the restriction of ψ to each subgroup $G(c/c - z_i)$ is equal to ψ_i for all i.

The map ψ is a 1-cochain in $\mathrm{Coch}^1(G(c/0), S)$. Let

$$E_\psi = \sum_{g \in G(c/0)} \psi(g) g^{-1}$$

be the Kolyvagin element of ψ (see §5.6, definition 5.6.11), where

$$E_\psi \in S[G(c/0)].$$

As the restriction of ψ to the subgroup $G(c/c - z_i)$ of $G(c/0)$ is the homomorphism ψ_i, it follows from proposition 5.6.12 that for some $x_i \in S[G(c/0)]$ and for all $g \in G(c/c - z_i)$ we have

$$(g-1)E_\psi = \psi_i(g) e_i x_i$$

where

$$e_i = \sum_{h \in G(c/c - z_i)} h.$$

We have the identity for any set of elements $g_1, \ldots, g_s \in G(c/0)$

$$\prod_{i=1}^{s} g_i - 1 = (g_1 - 1) \prod_{i \geq 2} g_i + (g_2 - 1) \prod_{i \geq 3} g_i + \ldots + (g_s - 1).$$

Taking $g_i \in G(c/c - z_i)$ for all i, we obtain that for all $g \in G$ (this is a variant of remark 5.6.13(iii))

$$(g-1)E_\psi \in \sum_i e_i S[G(c/0)].$$

For any element $g \in G(c/0)$ and $\delta \in \mathcal{H}_{c,S}$ we obtain

$$(g-1)E_\psi \delta \in \sum_i e_i \mathcal{H}_{c,S}.$$

For all $\delta \in \Delta_{c',S'}$ where $c' \leq c$ and all $z_i \in \mathrm{Supp}(c')$ and as z_i is inert and unramified in K/F, we have by definition (see (5.3.6))

$$K_{c',c'-z_i}(\delta) = (a_{z_i} \otimes 1) t^{\Delta}_{c',c'-z_i}(\delta) - \frac{|O^*_{c'-z_i}|}{|A^*|} e_{c',c'-z_i} \delta$$

where $\frac{|O^*_{c'-z_i}|}{|A^*|}$ is a unit of S. Hence we obtain

$$e_i\mathcal{H}_{c,S} \subseteq (a_{z_i} \otimes 1)\mathcal{H}_{c-z_i,S} \quad \text{for all } i.$$

Hence for any element

$$\delta \in \big(\bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1)\big) \otimes_S \mathcal{H}_{c,S}$$

we have for all $g \in G(c/0)$

$$(g-1)E_\psi\delta = 0.$$

Hence we have the inclusion of modules

$$E_\psi\big(\mathcal{H}_{c,S} \otimes_S \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1)\big) \ \subseteq (\mathcal{H}_{c,S})^{G(c/0)}.$$

We then define the S-module homomorphism

$$\eta : \mathcal{H}_{c,S} \otimes_S \big(\bigotimes_i \mathrm{Hom}(G(c/c-z_i), S)\big) \otimes_S \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1) \to (\mathcal{H}_{c,S})^{G(c/0)}$$

by

$$\delta \otimes (\psi_i)_i \otimes a \mapsto E_\psi(a\delta)$$

where $\delta \in \mathcal{H}_{c,S}$, $(\psi_i)_i \in \bigotimes_i \mathrm{Hom}(G(c/c-z_i), S)$, $\psi \in \mathrm{Coch}^1(G(c/0), S)$, and $a \in \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1)$ where E_ψ is the Kolyvagin element of ψ; here ψ is the multilinear map attached to the collection of homomorphisms $(\psi_i)_i$.

Commutativity of the diagram (7.13.5). Put, where $c = \sum_{i=1}^r z_i$,

$$S' = S/(a_{z_1} \otimes 1, a_{z_2} \otimes 1, \ldots, a_{z_r} \otimes 1).$$

Then the S-algebra S' is an infinitesimal trait and there is an isomorphism of S-modules

$$\bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1) \cong S'.$$

Furthermore, the Heegner module $\mathcal{H}_{c,S} \otimes S'$ is $\Delta_{c,S}$-isomorphic to $\mathcal{H}_{c,S'}$ (see corollary 5.9.5). We have an isomorphism of S-modules

$$M(c) \cong \bigotimes_i \mathrm{Hom}(G(c/c-z_i), S').$$

As the image of every element $a_{z_i} \otimes 1$ is zero in S', we have for all $\delta \in \Delta_{c',S'}$ where $c' \leq c$ and all $z_i \in \mathrm{Supp}(c')$ (see (5.3.6))

$$K_{c',c'-z_i}(\delta) = (a_{z_i} \otimes 1) t^{\Delta}_{c',c'-z_i}(\delta) - \frac{|O^*_{c'-z_i}|}{|A^*|} e_{c',c'-z_i}\delta$$

$$= -\frac{|O^*_{c'-z_i}|}{|A^*|} e_{c',c'-z_i}\delta$$

where $\frac{|O^*_{c'-z_i}|}{|A^*|}$ is a unit of S'. Hence the Heegner module $\mathcal{H}_{c,S'}$ decomposes as a direct sum of $\Delta_{c,S}$-modules

$$\mathcal{H}_{c,S'} \cong \bigoplus_{c' \leq c} \frac{\Delta_{c',S'}}{\sum_{z_i \in \mathrm{Supp}(c')} e_{c',c'-z_i}\Delta_{c',S'}}. \tag{7.13.7}$$

Write G for $G(c/c-z_1)$. By proposition 5.8.4(iii), $\{\ker(t_{c,c-z_i})\}_{i=1,\ldots,r}$ is an S-admissible family of subgroups of $\mathrm{Pic}(O_c)$. Taking the submodules

$$P = e_{c,c-z_1}\Delta_{c,S'} \quad \text{and} \quad N = \sum_{i=2}^{r} e_{c,c-z_i}\Delta_{c,S'}$$

of $\Delta_{c,S'}$, we have that N is a cohomologically trivial G-module (by lemma 5.6.19(i)) and that $P^G = P$; furthermore $P, N \cap P$ and $P/(N \cap P)$ are flat S'-modules (by lemma 5.6.27). By lemma 5.6.24, the inclusion of submodules $P \subseteq P + N$ gives rise to short exact sequences of $\Delta_{c,S}$-modules

$$0 \to \big(N \cap P\big) \otimes_S H^m(G, S') \to H^m(G, P) \to H^m(G, P+N) \to 0 \quad \text{for all } m \geq 1.$$

For the case where $m = 1$ this exact sequence gives the short exact sequence (7.13.8)

$$0 \to (N \cap P) \otimes_S \mathrm{Hom}(G, S') \to P \otimes_S \mathrm{Hom}(G, S') \to H^1(G, P + N) \to 0.$$

Hence by examples 5.6.3(5), the submodule of $\Delta_{c,S'}$

$$N \cap P = (\sum_{i=2}^{r} e_{c,c-z_i}\Delta_{c,S'}) \cap e_{c,c-z_1}\Delta_{c,S'}$$

is equal to the submodule

$$\sum_{i=2}^{r} e_{c,c-z_i-z_1}\Delta_{c,S'}.$$

Put

$$Q = \frac{P}{N \cap P} = \frac{e_{c,c-z_1}\Delta_{c,S'}}{\sum_{i=2}^{r} e_{c,c-z_i-z_1}\Delta_{c,S'}}.$$

Then the modules $N \cap P, P, Q$ are flat S'-modules by lemma 5.6.27 as already

noted. We then have the short exact sequence

$$0 \ \to \ N \cap P \ \to \ P \ \to \ Q \ \to \ 0.$$

and tensoring this sequence with the S-module $H^m(G, S')$ it remains exact

$$0 \ \to \ (N \cap P) \otimes_S H^m(G, S') \ \to \ P \otimes_S H^m(G, S') \ \to \ Q \otimes_S H^m(G, S') \ \to \ 0.$$

Hence this short exact sequence (7.13.8) provides an isomorphism of $\Delta_{c,S}$-modules

$$Q \otimes_S \mathrm{Hom}(G, S') \cong H^1(G, P + N). \tag{7.13.9}$$

As $\Delta_{c,S'}$ is a cohomologically trivial G-module, the short exact sequence of $\Delta_{c,S'}$-modules

$$0 \quad \to \quad P + N \quad \to \quad \Delta_{c,S'} \quad \to \quad \frac{\Delta_{c,S'}}{P + N} \quad \to \quad 0$$

gives rise to a long exact sequence of cohomology from which we obtain isomorphisms

$$H^{i-1}(G, \frac{\Delta_{c,S'}}{P + N}) \cong H^i(G, P + N) \ \text{ for all } i \geq 2$$

and also a short exact sequence

$$0 \to H^0(G, P + N) \to H^0(G, \Delta_{c,S'}) \to H^0(G, \frac{\Delta_{c,S'}}{P + N}) \to H^1(G, P + N) \to 0.$$

Hence we obtain the short exact sequence from the isomorphism (7.13.9)

$$0 \to (P + N)^G \to (\Delta_{c,S'})^G \to \big(\frac{\Delta_{c,S'}}{P + N}\big)^G \to Q \otimes_S \mathrm{Hom}(G, S') \to 0. \tag{7.13.10}$$

The module $\Delta_{c,S'}/(P + N)$ is $\Delta_{c,S'}$-isomorphic to the component over c of the Heegner module $\mathcal{H}_{c,S'}$ (see (7.13.7)). Let

$$\pi : \mathcal{H}_{c,S'} \to \frac{\Delta_{c,S'}}{P + N} = \mathcal{H}'_{c,S'}$$

denote the projection homomorphism onto the component over c. Furthermore, by (7.13.7) again the module Q is $\Delta_{c,S'}$-isomorphic to the component over $c - z_1$ of $\mathcal{H}_{c-z_1,S'}$ that is to say $\mathcal{H}'_{c-z_1,S'}$. Hence from (7.13.10) we obtain a homomorphism

$$(\mathcal{H}_{c,S'})^G \to \mathcal{H}_{c-z_1,S'} \otimes_S \mathrm{Hom}(G, S')$$

which is a composite homomorphism

$$\mathcal{H}^G_{c,S'} \xrightarrow{\pi} \Big(\frac{\Delta_{c,S'}}{P+N}\Big)^G = (\mathcal{H}'_{c,S'})^G \to Q \otimes_S \mathrm{Hom}(G, S') \to \mathcal{H}_{c-z_1,S'} \otimes_S \mathrm{Hom}(G, S').$$

The map $\eta : \mathcal{H}_{c,S} \otimes_S M(c) \to (\mathcal{H}_{c,S})^{G(c/0)}$ of diagram (7.13.5) is given by

$$\delta \otimes (\psi_i)_i \otimes a \mapsto E_\psi(\delta \otimes_S a).$$

We obtain maps

$$\mathcal{H}_{c,S} \otimes_S M(c) \xrightarrow{\eta} (\mathcal{H}_{c,S'})^{G(c/0)} \to (\mathcal{H}_{c,S'})^G \to \mathcal{H}_{c-z_1,S'} \otimes_S \mathrm{Hom}(G, S').$$

Let ψ_i be group homomorphisms with values in the additive group of S where

$$\psi_i \in \mathrm{Hom}(G(c/c - z_i), S) \quad \text{for all } i.$$

Let ψ_0 be the multilinear map

$$\psi_0 : \prod_i G(c/c - z_i) \to S$$
$$(g_1, \ldots, g_m) \mapsto \prod_i \psi_i(g_i).$$

As we have already shown above, the map ψ_0 factors though a map $\psi : G(c/0) \to S$ where the restriction of ψ to each subgroup $G(c/c - z_i)$ is equal to ψ_i for all i.

Similarly each homomorphism ψ_i for $i \geq 2$ induces a homomorphism

$$\psi_i^{(2)} : G(c - z_1/c - z_1 - z_i) \to S, \quad \text{for all } i \geq 2$$

and in general we obtain that ψ_i induces a homomorphism

$$\psi_i^{(j)} : G(c - d_j/c - z_i - d_j) \ \to \ S, \quad \text{for all } j \leq i.$$

where

$$d_j = \sum_{k=1}^{j-1} z_k.$$

Hence the collection $(\psi_i^{(j)})_{i \geq j}$ of homomorphisms induces a multilinear map

$$\psi^{(j)} : G(c - d_j, 0) \ \to \ S.$$

The map $\psi^{(j)}$ is a 1-cochain in $\mathrm{Coch}^1(G(c - d_j/0), S)$. Let

$$E_{\psi^{(j)}} = \sum_{g \in G(c-d_j/0)} \psi^{(j)}(g) g^{-1} \ \in \Delta_{c-d_j,S}$$

be the Kolyvagin element of $\psi^{(j)}$ (see §5.6, definition 5.6.11), where

$$E_{\psi^{(j)}} \in S[G(c-d_j/0)].$$

As the restriction of $\psi^{(j)}$ to the subgroup $G(c-d_j/c-z_i-d_j)$ of $G(c/0)$ is the homomorphism $\psi_i^{(j)}$, it follows from proposition 5.6.12 that for some $x_i \in S[G(c-d_j/0)]$ and for all $g \in G(c-d_j/c-z_i-d_j)$ we have

$$(g-1)E_{\psi^{(j)}} = \psi_i^{(j)}(g)e_{c-d_j,c-z_i-d_j}x_i$$

where

$$e_{c-d_j,c-z_i-d_j} = \sum_{h \in G(c-d_j/c-z_i-d_j)} h.$$

This composite homomorphism

$$\mathcal{H}_{c,S} \otimes_S M(c) \to \mathcal{H}_{c-z_1,S'} \otimes_S \mathrm{Hom}_{\mathbb{Z}}(G, S')$$

is given by

$$\delta \otimes (\psi_i)_i \otimes a \mapsto E_\psi(\pi(\delta \otimes a)) \mapsto \{g \mapsto (g-1)E_\psi(\pi(\delta \otimes a)), \quad \text{for } g \in G\}.$$

But we have for all $g \in G$

$$(g-1)E_\psi = \psi_1(g)e_{c,c-z_1}E$$

where

$$E = \sum_{g \in G(c/0)/G_1} \psi^{(2)}(g)g^{-1}$$

where $G_i = G(c/c-z_i)$ and the sum runs over a set of coset representatives of G_1 in $G(c/0)$. As there is an isomorphism of $\Delta_{c,S}$-modules

$$e_{c,c-z_1}\Delta_{c,S} \cong \Delta_{c-z_1,S}$$

we obtain that

$$E_{\psi^{(2)}} = \sum_{h \in G(c-z_1/0)} \psi^{(2)}(h)h^{-1}$$

acts in the same way as E on $e_{c,c-z_1}\Delta_{c,S}$ and that

$$\mathcal{H}_{c,S} \otimes_S M(c) \to \mathcal{H}_{c-z_1,S'} \otimes_S \mathrm{Hom}_{\mathbb{Z}}(G, S')$$

is given by

$$\delta \otimes (\psi_i)_i \otimes a \mapsto E_\psi(\pi(\delta \otimes a)) \mapsto \{g \mapsto (g-1)E_\psi(\pi(\delta \otimes a)) \quad \text{for } g \in G\}$$

$$= \{g \mapsto \psi_1(g)E_{\psi^{(2)}}(t^{\Delta}_{c,c-z_1}(\pi(\delta \otimes a))), \quad \text{for } g \in G\}$$

where $\psi_1(g)E_{\psi^{(2)}}(t^{\Delta}_{c,c-z_1}(\pi(\delta \otimes a))) \in \Delta_{c-z_1,S}$. Hence we obtain that the

composite map

$$\mathcal{H}_{c,S} \otimes_S M(c) \to \mathcal{H}_{c-z_1,S'} \otimes_S \mathrm{Hom}_{\mathbb{Z}}(G, S')$$

is given by

$$\delta\otimes(\psi_i)_i\otimes a \mapsto E_\psi(\delta\otimes a) \mapsto \{g \mapsto E_{\psi^{(2)}}(t^{\Delta}_{c,c-z_1}(\pi(\delta\otimes a)))\otimes_S \psi_1(g), \text{ for } g \in G\}.$$

It follows by induction from this last homomorphism that if h is the homomorphism of (7.13.5) and $a \in \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1)$ then we have

$$h \circ \eta\big(\delta \otimes \psi \otimes a\big) = h(E_\psi(\pi(\delta \otimes_S a))) =$$

$$\{(g_1, \ldots, g_r) \mapsto e_{c,c-z_1} e_{c-z_1,c-z_2} \ldots e_{z_r,0} \psi_1(g_1)\psi_2(g_2)\ldots\psi_r(g_r)\pi(\delta \otimes a)\}$$

for all $g_i \in G(c - d_i/c - d_{i+1})$ for all i and for all $\delta \in \mathcal{H}_{c,S}$. For all i there are surjective group homomorphisms

$$G(c - d_i/c - d_{i+1}) \to G(z_i/0)$$

induced from the inclusions of orders $O_c \subseteq O_{z_i}$ whose kernels have order dividing $|B^*|/|A^*|$. Hence we have that if h is the homomorphism of (7.13.5) and $a \in \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1)$ then

$$h(E_\psi(\pi(\delta \otimes_S a)))(g_1, \ldots, g_r) = e_{G(c/0)}\pi(\delta \otimes a) \otimes (\psi_1(g_1)\psi_2(g_2)\ldots\psi_r(g_r))$$

for all $\delta \in \mathcal{H}_{c,S}$ and for all $g_i \in G(c/c - z_i)$ for all i. Hence the diagram (7.13.5) is commutative. □

7.14 The cohomology classes $\gamma(c), \delta(c)$

In the first part of this section, we define a homomorphism

$$(\mathcal{H}^{(0)}_{c,S})^{\mathcal{G}_c} \to H^1(K, E),$$

where $S = \mathbb{Z}/l^n\mathbb{Z}$ and for all but finitely many prime numbers l. This map is obtained by sending a generator $< b, c >$ of the Heegner module $\mathcal{H}^{(0)}_{c,S}$ to the corresponding point on the elliptic curve E. Composing this homomorphism with the part of $(\mathcal{H}^{(0)}_{c,S})^{G(c/0)}$ identified by proposition 7.13.4 we obtain the cohomology class $\delta(c)$ in $H^1(K, E)$ for suitable divisors c (lemma 7.14.9 and Notation 7.14.10).

In the final part of this section, we derive properties of the cohomology classes $\delta(c)$ under the action of the Galois group $\mathrm{Gal}(K/F)$ and also under restriction to the completions of the field K (lemmas 7.14.11 and 7.14.14).

(7.14.1) As in (7.13.1), let

$m \geq 1$ be a positive integer prime to the characteristic of F and prime to the order of the group B^*/A^*;
S be the ring $\frac{\mathbb{Z}}{m\mathbb{Z}}$;
$\mathcal{H}(\rho_S, S) = \varinjlim \mathcal{H}_{c,S} \cong \mathcal{H}(\rho)_{\mathbb{Z}} \otimes_{\mathbb{Z}} S$ be the Heegner module of $\rho, K/F$ and with coefficients in S.

For any divisor c of $\mathrm{Div}_+(A)$, we have the exact sequence of finite abelian groups

$$0 \to G(c/0) \to \mathcal{G}_c \to \mathrm{Gal}(K[0]/K) \to 0$$

where

$$G(c/0) = \mathrm{Gal}(K[c]/K[0]),\ \mathcal{G}_c = \mathrm{Gal}(K[c]/K).$$

7.14.2. Proposition. *For any divisor c of $\mathrm{Div}_+(A)$, the restriction homomorphism*

$$\{H^1(K, E_n)\}_{n \in \mathbb{N}^{(p)}} \to \{H^1(K[c], E_n)^{\mathcal{G}_c}\}_{n \in \mathbb{N}^{(p)}}$$

is a quasi-isomorphism of quasi-groups. Furthermore, there is a finite set of exceptional prime numbers $\mathcal{E}$ such that if $\mathbb{N}^{\mathcal{E}}$ is the set of positive integers prime to $\mathcal{E}$ then for all $c \in \mathrm{Div}_+(A)$

$$\{H^1(K, E_n)\}_{n \in \mathbb{N}^{\mathcal{E}}} \to \{H^1(K[c], E_n)^{\mathcal{G}_c}\}_{n \in \mathbb{N}^{\mathcal{E}}}$$

is an isomorphism of quasi-groups.

Proof. Attached to the Hochschild-Serre spectral sequence

$$H^i(\mathcal{G}_c, H^j(K[c], E_n(K^{\mathrm{sep}}))) \Rightarrow H^{i+j}(K, E_n(K^{\mathrm{sep}}))$$

is the short exact sequence of low degree terms

$$0 \to H^1(\mathcal{G}_c, E_n(K[c])) \to H^1(K, E_n) \to H^1(K[c], E_n)^{\mathcal{G}_c} \to H^2(\mathcal{G}_c, E_n(K[c])).$$

Here $n \geq 1$ is any integer prime to p. The quasi-groups $\{H^1(\mathcal{G}_c, E_n(K[c]))\}_{n \in \mathbb{N}^{(p)}}$ and $\{H^2(\mathcal{G}_c, E_n(K[c]))\}_{n \in \mathbb{N}^{(p)}}$ are both trivial because $\{E_n(K[c])\}_{n \in \mathbb{N}^{(p)}}$ is trivial by the Mordell-Weil theorem; furthermore, by proposition 7.3.8 there is a finite set of prime numbers $\mathcal{E}$ such that for all divisors c on Spec A and all integers n prime to $\mathcal{E}$ the group $E_n(K[c])$ is trivial. Hence the restriction homomorphism

$$\phi(n, c) : H^1(K, E_n) \to H^1(K[c], E_n)^{\mathcal{G}_c}$$

is a quasi-isomorphism of quasi-groups in $[\mathbb{N}^{(p)}]_{\mathbb{Z}}$; furthermore, for all divisors c on Spec A and all integers n prime to $\mathcal{E}$ the homomorphism $\phi(n, c)$ is an isomorphism, which proves the final statement of the proposition. □

(7.14.3) The homomorphism $\mathcal{H}(\pi)_c : \mathcal{H}^{(0)}_{c,\mathbb{Z}} \to E(K[c])$ then provides a homomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$\mathcal{H}(\pi)_{c,S} : \mathcal{H}^{(0)}_{c,S} \to E(K[c]) \otimes_{\mathbb{Z}} S.$$

Hence we obtain a homomorphism of $\mathcal{G}_c$-invariants

$$f : (\mathcal{H}^{(0)}_{c,S})^{\mathcal{G}_c} \to (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}.$$

(7.14.4) A standard generator of the Heegner module $\mathcal{H}(\rho)_{\mathbb{Z}} = \varinjlim \mathcal{H}_{c,\mathbb{Z}}$ is denoted as usual by $< a, c >$ where $a \in \mathrm{Pic}(O_c)$ (see (5.3.8)). Whenever c is prime to I, we write the Drinfeld-Heegner point (a, I_1, c, π) as

$$y_{a,c} = (a, I_1, c, \pi) = \mathcal{H}(\pi)_c(< a, c >) \in E(K[c]).$$

(7.14.5) For any field extension L of F we have the exact sequence

$$0 \to {}_mE(L) \to H^1(L^{\mathrm{sep}}/L, E_m(L^{\mathrm{sep}})) \to H^1(L^{\mathrm{sep}}/L, E(L^{\mathrm{sep}}))_m \to 0.$$

From this and the homomorphism f (of (7.14.3)) we obtain for any divisor c of $\mathrm{Div}_+(A)$ prime to I the following commutative diagram with exact rows and an exact right-hand column:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(K[c]/K, E(K[c]))_m & & \\
 & & & & & \overset{j}{\to} & \inf \downarrow & & \\
0 \to & {}_mE(K) & \to & H^1(K, E_m) & & \to & H^1(K, E)_m & \to & 0 \\
 & \downarrow & & \mathrm{res} \downarrow \ \mathrm{quasi-isom.} & & & \mathrm{res} \downarrow & & \\
0 \to & ({}_mE(K[c]))^{\mathcal{G}_c} & \overset{\partial}{\to} & H^1(K[c], E_m)^{\mathcal{G}_c} & & \to & H^1(K[c], E)^{\mathcal{G}_c}_m & & \\
 & f \uparrow & & & & & & & \\
 & (\mathcal{H}^{(0)}_{c,S})^{\mathcal{G}_c} & & & & & & &
\end{array}$$

The middle restriction homomorphism here is a quasi-isomorphism of quasi-groups in $[\mathbb{N}^{(p)}]_{\mathbb{Z}}$ where the finite exceptional set of prime numbers may be taken independent of c, by the preceding proposition 7.14.2.

This diagram then provides the fundamental *Heegner homomorphism*, for all m prime to the finite exceptional set of prime numbers,

$$(\mathcal{H}^{(0)}_{c,S})^{\mathcal{G}_c} \to H^1(K, E)$$

whose image lies in $H^1(K[c]/K, E(K[c]))_m$.

(7.14.6) Assume $c \in \mathrm{Div}_+(A)$ is a sum $\sum_{i=1}^r z_i$ of distinct prime divisors z_i which are unramified and inert in K/F. As in proposition 7.13.4, put

$$M(c) = \bigotimes_{i=1}^{r} \mathrm{Hom}(G(c/c - z_i), S) \otimes_S \bigotimes_{i=1}^{r} \mathrm{Ann}_S(a_{z_i} \otimes 1).$$

(7.14.7) Assume $c \in \mathrm{Div}_+(A)$ is a sum $\sum_i z_i$ of distinct prime divisors z_i which are unramified and inert in K/F, in particular c is prime to I. By proposition 7.13.4 we have a homomorphism of S-modules

$$\eta : \mathcal{H}_{c,S} \otimes_S M(c) \to (\mathcal{H}_{c,S})^{G(c/0)}$$

given by

$$\delta \otimes_S (\psi_i)_i \otimes_S a \mapsto E_\psi(\delta \otimes_S a)$$

where E_ψ is a Kolyvagin element (definition 5.6.11). Composing this with the trace

$$\mathrm{Tr}_{K[0]/K} : (\mathcal{H}_{c,S})^{G(c/0)} \to (\mathcal{H}_{c,S})^{\mathcal{G}_c}, \quad \delta \mapsto \sum_{\sigma \in \mathcal{G}_c/G(c/0)} \sigma\delta,$$

we obtain the homomorphism of S-modules

$$\mathrm{Tr}_{K[0]/K} \circ \eta : \mathcal{H}_{c,S} \otimes_S M(c) \to (\mathcal{H}_{c,S})^{\mathcal{G}_c}.$$

(7.14.8) Assume $c \in \mathrm{Div}_+(A)$ is a sum $\sum_i z_i$ of distinct prime divisors z_i which are unramified and inert in K/F. We may compose the homomorphism $\mathrm{Tr}_{K[0]/K} \circ \eta$ with the homomorphism f (see the diagram (7.14.5))

$$\mathcal{H}_{c,S} \otimes_S M(c) \overset{\mathrm{Tr}_{K[0]/K} \circ \eta}{\longrightarrow} (\mathcal{H}_{c,S})^{\mathcal{G}_c} \overset{f}{\to} (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$$

and obtain the homomorphism of S-modules $\tilde{\eta}_c$

$$\tilde{\eta}_c : \mathcal{H}_{c,S} \otimes_S M(c) \to (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}.$$

By the diagram of (7.14.5), there is a finite set $\mathcal{E}$ of exceptional prime numbers such that for all integers m prime to $\mathcal{E}$ we have a homomorphism of quasi-groups where $\mathbb{N}^{\mathcal{E}}$ denotes the set of positive integers prime to $\mathcal{E}$

$$\{(E(K[c]) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z})^{\mathcal{G}_c}\}_{m \in \mathbb{N}^{\mathcal{E}}} \to \{H^1(K, E_m)\}_{m \in \mathbb{N}^{\mathcal{E}}}.$$

The exceptional set $\mathcal{E}$ is independent of the divisor c. We may then compose this homomorphism with the homomorphism of S-modules $\tilde{\eta}_c$ and obtain the homomorphism γ_c of S-modules

$$\gamma_c : \mathcal{H}_{c,S} \otimes_S M(c) \to H^1(K, E_m)$$

for all integers m prime to $\mathcal{E}$, where $S = \mathbb{Z}/m\mathbb{Z}$. We may then compose γ_c with the homomorphism $j : H^1(K, E_m) \to H^1(K, E)_m$ (see the diagram of (7.14.5)) and obtain a homomorphism of S-modules for all m prime to $\mathcal{E}$

$$\delta_c : \mathcal{H}_{c,S} \otimes_S M(c) \to H^1(K[c]/K, E(K[c]))_m.$$

7.14.9. Lemma. *Suppose that l is a prime number where $l \in \mathcal{P} \setminus \mathcal{E}$ and $\mathcal{E}$ is the finite exceptional set of proposition 7.14.2. Let $c \in \mathcal{D}_{l^n}$ and put $S = \mathbb{Z}/l^n\mathbb{Z}$. Then we have:*
(i) *The divisor $c \in \mathrm{Div}_+(A)$ is a sum of distinct prime divisors $\sum_i z_i$ which are unramfied and inert in K/F.*
(ii) *We have an isomorphism of S-modules $M(c) \cong S$ and the maps $\tilde{\eta}_c, \gamma_c, \delta_c$ form a commutative diagram*

$$\begin{array}{ccc} & & (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c} \\ & \tilde{\eta}_c \nearrow & \downarrow \\ \mathcal{H}_{c,S} & \xrightarrow{\gamma_c} & H^1(K, E_{l^n}) \\ & \delta_c \searrow & \downarrow \\ & & H^1(K[c]/K, E(K[c]))_{l^n} \end{array}$$

Proof. The lemma holds as c is a sum of prime divisors $c = \sum_i z_i$ where z_i is inert and unramified in K/F (definition 7.11.3(ii)) and where $|G(c/c - z_i)|$ is divisible by l^n for all i and the integer a_{z_i} is divisible by l^n for all i (lemma 7.11.5). Hence we have an isomorphism of S-modules

$$M(c) = \bigotimes_i {}_S\mathrm{Hom}(G(c/c - z_i), S) \otimes_S \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1) \cong S. \quad \square$$

7.14.10. Notation. Suppose that l is a prime number where $l \in \mathcal{P} \setminus \mathcal{E}$. Let $c \in \mathcal{D}_{l^n}$ where $c = \sum_{i=1}^r z_i$ is a sum of prime divisors; the divisor c is a sum of distinct prime divisors z_i which are unramfied and inert in K/F by the previous lemma 7.14.9. Put $S = \mathbb{Z}/l^n\mathbb{Z}$.

(i) Each group $G(c/c - z_i)$ for all i is cyclic of order $(|\kappa(z_i)| + 1)$ or $(|\kappa(z_i)| + 1)/(|B^*|/|A^*|)$ (see (2.3.11)); in particular the order is an integer divisible by l^n (lemma 7.11.5). Fix a generator σ_{z_i} of $G(c/c - z_i)$ for all i and fix the homomorphism $h_{z_i} \in \mathrm{Hom}(G(c/c - z_i), S)$ such that $h_{z_i} : \sigma_{z_i} \mapsto 1$. The homomorphisms h_{z_i} determine a unique isomorphism of S-modules $M(c) \cong S$.

(ii) The images $\tilde{\eta}_c(\mathcal{H}_{c,S}), \gamma_c(\mathcal{H}_{c,S}), \delta_c(\mathcal{H}_{c,S})$ are principal S-modules.

[To prove this, it suffices by lemma 7.14.9 to show that $\tilde{\eta}_c(\mathcal{H}_{c,S})$ is a principal S-module. By definition, all primes of $\mathcal{P}$ are odd hence l^n is an odd integer. For any homomorphism of finite abelian groups

$\chi : D \to S = \mathbb{Z}/l^n\mathbb{Z}$ we then have $\sum_{x\in D} \chi(x) = 0$. From the definition of the map $\eta : \mathcal{H}_{c,S} \otimes_S M(c) \to (\mathcal{H}_{c,S})^{G(c/0)}$, given by

$$\delta \otimes_S (\psi_i)_i \otimes_S a \mapsto E_\psi(\delta \otimes_s A)$$

we have that $E_\psi = E_{\psi_i} x_i$ for all i and for some $x_i \in \Delta_{c,S}$; hence we have

$$t^{\Delta}_{c,c-z_i}(E_\psi) = x_i t^{\Delta}_{c,c-z_i}(\sum_{g\in G(c/c-z_i)} \psi_i(g)g^{-1}) = 0 \quad \text{for all } i$$

by the previous remark. Hence η factors through the natural surjection

$$\mathcal{H}_{c,S} \otimes_S M(c) \to \mathcal{H}'_{c,S} \otimes_S M(c).$$

As the image of η lies in $(\mathcal{H}_{c,S})^{G(c/0)}$ by proposition 7.13.4, we obtain that the image of η lies in $(\mathcal{H}'_{c,S})^{G(c/0)}$. Hence the image of η coincides with the image of $\Delta_{c,S}$ in $(\mathcal{H}'_{c,S})^{G(c/0)}$ under the map $\Delta_{c,S} \otimes_S M(c) \to (\mathcal{H}'_{c,S})^{G(c/0)}$. The module $M(c)$ is itself a principal S-module as the groups $G(c/c-z_i)$ are cyclic for all $i = 1, \ldots, r$. Hence the image of $\tilde{\eta}_c : \mathcal{H}_{c,S} \otimes_S M(c) \to (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$ coincides with the image of $\Delta^{\mathcal{G}_c}_{c,S} \otimes_S M(c)$; but this last module is a principal S-module. Hence the image of $\tilde{\eta}_c$ is a principal S-module.]

(iii) Select generators $P_c, \gamma(c), \delta(c)$ of the principal S-modules $\tilde{\eta}_c(\mathcal{H}_{c,S})$, $\gamma_c(\mathcal{H}_{c,S})$, $\delta_c(\mathcal{H}_{c,S})$, respectively, as follows. Let $< a, c >$ be a standard generator of the Heegner module $\mathcal{H}_{c,S}$ where $a \in \mathrm{Pic}(O_c)$ (see (5.3.8)). We put

$$P_c = \tilde{\eta}_c(< a, c > \otimes h_{z_1} \otimes \ldots \otimes h_{z_r}) \in (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$$

where $\tilde{\eta}_c$ is the homomorphism defined in (7.14.8). As the image of $\tilde{\eta}_c$ lies in the $\mathcal{G}_c$-invariant submodule of $E(K[c]) \otimes_{\mathbb{Z}} S$, the element P_c is independent of the class $a \in \mathrm{Pic}(O_c)$.

Put

$$\gamma(c) = \gamma_c(< a, c > \otimes h_{z_1} \otimes \ldots \otimes h_{z_r}) \in H^1(K, E_{l^n})$$

$$\delta(c) = \delta_c(< a, c > \otimes h_{z_1} \otimes \ldots \otimes h_{z_r}) \in H^1(K[c]/K, E(K[c]))_{l^n}$$

The elements $\gamma(c), \delta(c)$ are independent of the class $a \in \mathrm{Pic}(O_c)$ and are induced by the element $P_c \in (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$ under the homomorphisms of lemma 7.14.9.

7.14.11. Lemma. *There is a finite set of exceptional prime numbers $\mathcal{F}$ such that for all integers $n \geq 1$, for all prime numbers $l \in \mathcal{P} \setminus \mathcal{F}$ we have the following, where $S = \mathbb{Z}/l^n\mathbb{Z}$.*
(i) *$E(K[d])_{l^\infty} = 0$ for all $d \in \mathrm{Div}_+(A)$;*
(ii) *Let τ be the non-trivial element of* $\mathrm{Gal}(K/F)$. *For all $c \in \mathcal{D}_{l^n}$ we have*

$$P_c \in \left((E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}\right)^{\tau=-\epsilon_c}$$

$$\gamma(c) \in H^1(K, E_{l^n})^{\tau=-\epsilon_c}$$

$$\delta(c) \in H^1(K[c]/K, E)_{l^n}^{\tau=-\epsilon_c}$$

where $\epsilon_c = \epsilon(-1)^{g(c)}$, $g(c)$ is the number of prime divisors in $\mathrm{Supp}(c)$, *and $\epsilon = \pm 1$ is the sign in the functional equation of the L-function $L(s, E)$ of E.*

Proof. We take $\mathcal{F}$ to be the smallest finite set of prime numbers l containing the set $\mathcal{E}$ (of proposition 7.14.2) such that for all $l \in \mathcal{P} \setminus \mathcal{F}$ and for all $d \in \mathrm{Div}_+(A)$ we have $E(K[d])_{l^\infty} = 0$. The finite set $\mathcal{F}$ exists by proposition 7.3.8. The property (i) then holds by the definition of $\mathcal{F}$.

For (ii), let

$$c = \sum_{i=1}^{m} z_i$$

where z_i are prime divisors. The group $\mathrm{Gal}(K[c]/F)$ is generalised dihedral (proposition 2.5.7) and hence contains an element $\tau^\sharp$ of order 2 which lifts τ, the non-trivial element of $\mathrm{Gal}(K/F)$; namely, we may take $\tau^\sharp$ to be the restriction to $K[c]$ of the non-trivial element of $\mathrm{Gal}(K_\infty/F_\infty)$.

For $a \in \mathrm{Pic}(O_c)$ we have that

$$(a, I_1, c, \pi) = \mathcal{H}(\pi)_{c,\mathbb{Z}}(< a, c >) \in E(K[c])$$

is the Drinfeld-Heegner point corresponding to $< a, c > \in \mathcal{H}_{c,\mathbb{Z}}$, as in (7.14.4). By theorem 4.8.6 we have

$$\tau^\sharp(a, I_1, c, \pi) \equiv -\epsilon\sigma(a, I_1, c, \pi) \quad \text{modulo} \quad E(K^{\mathrm{sep}})_{\mathrm{tors}}$$

for some $\sigma \in \mathrm{Gal}(K[c]/K) = \mathcal{G}_c$. Denote by $[x]$ the image of $x \in E(K[c])$ in $E(K[c]) \otimes_{\mathbb{Z}} S$. As $E(K[c])_{l^\infty} = 0$ for all except finitely many prime numbers l by part (i), we then have that for some $\sigma \in \mathcal{G}_c$ there is an equality of elements of $E(K[c]) \otimes_{\mathbb{Z}} S$

$$\tau^\sharp[(a, I_1, c, \pi)] = -\epsilon[\sigma(a, I_1, c, \pi)].$$

As $\mathrm{Gal}(K[c]/F)$ is a generalised dihedral group, for any

$$\psi \in \bigotimes_{i=1}^{m} \mathrm{Hom}(G(c/c - z_i), S)$$

the action of $\tau^\sharp$ on the Kolyvagin element E_ψ is given by (see definition 5.6.11)

$$\tau^\sharp E_\psi = \tau^\sharp \sum_{g \in G(c/0)} g^{-1}\psi(g)$$

$$= \sum_{g \in G(c/0)} g\psi(g)\tau^\sharp = (-1)^m E_\psi \tau^\sharp.$$

Hence we have for any elements $\psi_i \in \mathrm{Hom}(G(c/c - z_i), S)$ for all i where $\psi = \otimes_i \psi_i$

$$\tau^\sharp \tilde{\eta}_c(< a, c > \otimes \psi_1 \otimes \ldots \otimes \psi_m) = (-1)^m(-\epsilon)\tilde{\eta}_c(\sigma < a, c > \otimes \psi_1 \otimes \ldots \psi_m)$$

$$= -\epsilon_c \tilde{\eta}_c(< a, c > \otimes \psi_1 \otimes \ldots \otimes \psi_m).$$

Hence the image $\tilde{\eta}_c(\mathcal{H}_{c,S} \otimes_S M(c))$ lies in the $-\epsilon_c$-eigenspace of $(E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$. Similar conclusions for the images $\gamma_c(\mathcal{H}_{c,S} \otimes_S M(c))$ and $\delta_c(\mathcal{H}_{c,S} \otimes_S M(c))$ now follow from this and the commutative diagram of lemma 7.14.9(ii). □

7.14.12. Remarks. Let $l \in \mathcal{P} \setminus \mathcal{E}$, where $\mathcal{E}$ is the finite exceptional set proposition 7.14.2, and let $c \in \mathcal{D}_{l^n}$ where $n \geq 1$ is an integer.

(i) The homomorphism

$$\delta_0 : \mathcal{H}_{0,\mathbb{Z}/l^n\mathbb{Z}} \to H^1(K[0]/K, E)_{l^n}$$

is zero.

[For the proof, let $< a, 0 >$ where $a \in \mathrm{Pic}(B)$ be one of the standard generators of the Heegner module $\mathcal{H}_{0,\mathbb{Z}}$ with coefficients in $\mathbb{Z}$. We have that (see (7.14.4))

$$(a, I_1, 0, \pi) = \mathcal{H}(\pi)_{0,\mathbb{Z}}(< a, 0 >) \in E(K[0]).$$

Put

$$x = \mathrm{Tr}_{K[0]/K}(a, I_1, 0, \pi)$$

where $x \in E(K)$ lies in the group $E(K)$ of K-rational points of E. Then $P_0 = \tilde{\eta}_0(< a, 0 >)$ is the image in ${}_{l^n}E(K)$ of x for all l and n (see notation 7.14.10). It follows from the diagram (7.14.5) that $\gamma_0(< a, 0 >)$ is zero if and only if x is divisible by l^n in $E(K)$ and that $\delta_0(< a, 0 >)$ is always equal to 0.]

(ii) The order l^t of $\gamma(c)$ is equal to the order of P_c in ${}_{l^n}E(K[c])$.

[This follows from the diagram (7.14.5).]

(iii) The exponent t of the order l^t of $\delta(c)$ is the least integer t such that

$$l^t P_c \in \frac{l^n E(K[c]) + E(K)}{l^n E(K[c])}.$$

[This also follows from the diagram (7.14.5).]

7.14.13. Notation. For any place v of K, we define the restrictions $\mathrm{res}_v\gamma(c)$ and $\mathrm{res}_v\delta(c)$ for all suitable divisors $c \in \mathrm{Div}_+(A)$ as follows.

(i) Let

$$\mathrm{res}_v : H^1(K^{\mathrm{sep}}/K, E_n) \to H^1(K_v^{\mathrm{sep}}/K_v, E_n)$$

be the evident restriction homomorphism for all integers $n \geq 1$. This defines the restriction $\mathrm{res}_v\gamma(c)$ for all v and all suitable divisors c.

(ii) For any divisor $c \in \mathrm{Div}_+(A)$, for v a place of K, let res_v denote the restriction homomorphism

$$\mathrm{res}_v : H^1(K[c]/K, E) \to H^1(K_v^{\mathrm{sep}}/K_v, E)$$

obtained as a composite

$$H^1(K[c]/K, E) \overset{\mathrm{inf}}{\to} H^1(K^{\mathrm{sep}}/K, E) \overset{\mathrm{res}}{\to} H^1(K_v^{\mathrm{sep}}/K_v, E)$$

where the first homomorphism is inflation and the second homomorphism is the restriction induced from the inclusion of fields $K \to K_v$. This defines $\mathrm{res}_v\delta(c)$ for all v and all suitable divisors c.

7.14.14. Lemma. *Assume that $c \in \mathcal{D}_{l^n}$ where $l \in \mathcal{P} \setminus \mathcal{F}$, where $\mathcal{F}$ is the finite exceptional set of prime numbers of proposition 7.14.11, and where $n \geq 1$ is an integer.*
(i) *We have $\mathrm{res}_v\delta(c) = 0$ for all places v of K where $v \notin \mathrm{Supp}(c)$.*
(ii) *Suppose that $c = z + c'$, $z, c' \in \mathcal{D}_{l^n}$ where z is a prime divisor prime to c'. Let $z^\sharp$ be the unique prime of K lying over z and let z' be a prime divisor of $K[c']$ over $z^\sharp$. Let $K[c']_{z'}$ be the completion of $K[c']$ at z'. Suppose that the order of the class of $z^\sharp$ in $\mathrm{Pic}\ (O_{c'})$ is prime to l. Then the order of $\mathrm{res}_{z^\sharp}\delta(c)$ in $H^1(K_{z^\sharp}, E(K_{z^\sharp}^{\mathrm{sep}}))_{l^n}$ is equal to the order of $\mathrm{res}_{z'}P_{c'}$ in ${}_{l^n}E(K[c']_{z'})$.*

Proof. (i) The field $K[c]$ is a subfield of K_∞ as ∞ is split completely in $K[c]/K$ (see (2.3.13)). We have $\mathrm{res}_\infty\delta(c) \in H^1(K_\infty, E)_{l^n}$ and $\mathrm{res}_\infty P_c \in {}_{l^n}E(K_\infty)$. From the diagram (7.14.5), it follows that $\mathrm{res}_\infty\delta(c) = 0$.

Suppose now that v is a place of K such that $v \neq \infty$ and $v \notin \mathrm{Supp}(c)$. We have that

$$\delta(c) \in H^1(K[c]/K, E(K[c]))_{l^n}.$$

But $K[c]/K$ is unramified at v (see (2.3.13)) and hence

$$\mathrm{res}_v \delta(c) \in H^1(K_v^{\mathrm{nr}}/K_v, E(K_v^{\mathrm{nr}}))_{l^n} \subset H^1(K_v, E(K_v^{\mathrm{sep}}))_{l^n}.$$

Therefore $\mathrm{res}_v \delta(c) = 0$ by (7.10.3)(d).
(ii) We prove the result in several steps. We write Δ for the cohomology class $\mathrm{res}_{z^\sharp} \delta(c) \in H^1(K_{z^\sharp}, E(K_{z^\sharp}^{\mathrm{sep}}))$.

Step 1. The prime divisor z' is totally ramified in the field extension $K[c]/K[c']$

That z' is totally ramified in this field extension is shown in (2.3.13). Let $z^\times$ be the unique prime divisor of $K[c]$ lying over z'. The class $\delta(c)$ lies in $H^1(K[c]/K, E(K[c]))_{l^n}$ which is contained via the inflation map in $H^1(K, E(K^{\mathrm{sep}}))_{l^n}$ (diagram (7.14.5)).

Step 2. Let $\bar{P}_c \in E(K[c])$ be a lifting of $P_c \in {}_{l^n}E(K[c])$. The class $\Delta \in H^1(K_{z^\sharp}, E(K_{z^\sharp}^{\mathrm{sep}}))$ is represented by the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n}, \qquad \mathrm{Gal}(K[c]_{z^\times}/K_{z^\sharp}) \to E(K_{z^\sharp}^{\mathrm{sep}}).$$

To prove this, from the diagram (7.14.5) the restriction homomorphism

$$H^1(K, E_{l^n}(K^{\mathrm{sep}})) \to H^1(K[c], E_{l^n}(K^{\mathrm{sep}}))^{\mathcal{G}_c}$$

is an isomorphism.

Let $\frac{\bar{P}_c}{l^n} \in E(K^{\mathrm{sep}})$ be a fixed l^nth division point of $\bar{P}_c$, that is to say $\frac{\bar{P}_c}{l^n}$ is any point which satisfies $l^n(\frac{\bar{P}_c}{l^n}) = \bar{P}_c$. Then the cocycle

$$\phi : g \mapsto g\big(\frac{\bar{P}_c}{l^n}\big) - \frac{\bar{P}_c}{l^n}, \ \mathrm{Gal}(K^{\mathrm{sep}}/K[c]) \to E_{l^n}(K^{\mathrm{sep}}),$$

represents a cohomology class in $H^1(K[c], E_{l^n}(K^{\mathrm{sep}}))^{\mathcal{G}_c}$ which is the image of $P_c \in {}_{l^n}E(K[c])$ under

$$\partial : {}_{l^n}E(K[c]) \to H^1(K[c], E_{l^n}(K^{\mathrm{sep}}))^{\mathcal{G}_c}$$

(see the diagram (7.14.5)). The inflation of ϕ to $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is given by the cocycle

$$\phi^\sharp : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to E(K^{\mathrm{sep}}), \quad g \mapsto g\big(\frac{\bar{P}_c}{l^n}\big) - \frac{\bar{P}_c}{l^n}$$

which need not necessarily be annihilated by l^n.

For any element $g \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, denote by

$$\frac{(g-1)\bar{P}_c}{l^n}$$

the unique l^nth root of $(g-1)\bar{P}_c$ in $E(K[c])$. This root exists because P_c lies in $({}_{l^n}E(K[c]))^{\mathcal{G}_c}$; furthermore, it is unique because $E(K[c])_{l^\infty} = 0$ (see lemma 7.14.11(i)).

The cochain

$$\psi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to E(K[c]), \quad g \mapsto -\frac{(g-1)\bar{P}_c}{l^n},$$

is a cocycle whose restriction to the subgroup $\mathrm{Gal}(K^{\mathrm{sep}}/K[c])$ is the zero cochain. But ψ need not be annihilated by l^n. The cochain

$$\phi^\sharp + \psi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to E(K[c]), g \mapsto g\big(\frac{\bar{P}_c}{l^n}\big) - \frac{\bar{P}_c}{l^n} - \frac{(g-1)\bar{P}_c}{l^n},$$

is a cocycle which is annihilated by l^n and whose restriction to $\mathrm{Gal}(K^{\mathrm{sep}}/K[c])$ is the cocycle

$$\phi : \mathrm{Gal}(K^{\mathrm{sep}}/K[c]) \to E_{l^n}(K^{\mathrm{sep}}).$$

Hence the cochain $\phi^\sharp + \psi$ is a cocycle

$$\phi^\sharp + \psi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to E_{l^n}(K^{\mathrm{sep}})$$

and this cochain represents the cohomology class $\gamma(c)$ in $H^1(K, E_{l^n})$. Therefore the cohomology class $\delta(c)$ of $H^1(K[c]/K, E)_{l^n}$ is represented by the cocycle

$$\psi : \mathrm{Gal}(K[c]/K) \to E(K^{\mathrm{sep}}), \quad g \mapsto -\frac{(g-1)\bar{P}_c}{l^n}.$$

It follows that Δ is represented by the cocycle obtained by restriction (as in (7.14.13)(iii)) of the cocycle ψ to the galois group $\mathrm{Gal}(K[c]_{z^\times}/K_{z^\sharp})$, as required.

Step 3. Let $\mathcal{E}_0$ be the closed fibre above z of the Néron model of E/F. There is an isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, E(K[c]_{z^\times}))_{l^n} \ \stackrel{\cong}{\to}\ H^1(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z^\times)))_{l^n}.$$

The image of Δ under this isomorphism is represented by the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}.$$

For $z \neq \infty$ is coprime to the conductor I, hence the elliptic curve E has good reduction at z. Let $\mathcal{E}_0$ be the closed fibre above z of the Néron model of E/F. The kernel J of the surjective reduction map modulo z

$$E(K[c]_{z^\times}) \to \mathcal{E}_0(\kappa(z^\times))$$

is a pro-p-group (see for example [L, Chapter 3, §3]). Hence we have

$$H^i(K[c]_{z^\times}/K_{z^\sharp}, J)_{l^n} = 0 \ \text{ for all } i \geq 1.$$

We obtain from the long exact sequence of cohomology an isomomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, E(K[c]_{z^\times}))_{l^n} \to H^1(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z^\times)))_{l^n}.$$

Therefore the order of Δ is the same as that of its image in $H^1(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z')))_{l^n}$, where we note that $\kappa(z^\times) = \kappa(z')$, as required.

Step 4. There is an isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, E(K[c]_{z^\times}))_{l^n} \overset{\cong}{\to} \mathrm{Hom}(\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}.$$

The image of Δ under this isomorphism is represented by the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}, \quad \mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}) \to \mathcal{E}_0(\kappa(z^\sharp)).$$

For the proof, we have the Hochschild-Serre spectral sequence

$$E_2^{i,j} \Rightarrow H^{i+j}(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z'))).$$

where we have $\kappa(z') = \kappa(z^\times)$ (by Step 1) and where we write

$$E_2^{i,j} = H^i(K[c']_{z'}/K_{z^\sharp}, H^j(K[c]_{z^\times}/K[c']_{z'}, \mathcal{E}_0(\kappa(z')))).$$

The short exact sequence of low degree terms attached to this spectral sequence is then in part

$$0 \to E_2^{1,0} \to H^1(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z'))) \to E_2^{0,1} \to E_2^{2,0}.$$

But we have, as z' is totally ramified in the field extension $K[c]/K[c']$ (Step 1),

$$\begin{aligned} E_2^{i,0} &= H^i(K[c']_{z'}/K_{z^\sharp}, H^0(K[c]_{z^\times}/K[c']_{z'}, \mathcal{E}_0(\kappa(z')))) \\ &\cong H^i(K[c']_{z'}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z'))). \end{aligned}$$

The extension of local fields $K[c']_{z'}/K_{z^\sharp}$ is unramified. Hence by passage to the residue fields, we obtain an isomorphism of galois groups compatible with the action on $\mathcal{E}_0(\kappa(z'))$

$$\mathrm{Gal}(K[c']_{z'}/K_{z^\sharp}) \cong \mathrm{Gal}(\kappa(z')/\kappa(z^\sharp)).$$

Hence we have isomorphisms

$$E_2^{i,0} \cong H^i(\kappa(z')/\kappa(z^\sharp), \mathcal{E}_0(\kappa(z'))).$$

But the order of the class of $z^\sharp$ in Pic $(O_{c'})$ is prime to l. Hence the degree of the extension $\kappa(z')/\kappa(z^\sharp)$ is prime to l. But then

$$(E_2^{i,0})_{l^n} = 0 \quad \text{for all } i \geq 1.$$

The galois group $\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'})$ acts trivially on $\mathcal{E}_0(\kappa(z'))$ again because z' is totally ramified in $K[c]_{z^\times}/K[c']_{z'}$ (see Step 1). Hence we have

$$\begin{aligned} E_2^{0,1} &= H^0(K[c']_{z'}/K_{z^\sharp}, H^1(K[c]_{z^\times}/K[c']_{z'}, \mathcal{E}_0(\kappa(z')))) \\ &\cong H^0(K[c']_{z'}/K_{z^\sharp}, \mathrm{Hom}(\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}), \mathcal{E}_0(\kappa(z')))) \\ &\cong \mathrm{Hom}(\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}), \mathcal{E}_0(\kappa(z^\sharp)). \end{aligned}$$

Hence the short exact sequence of low degree terms above provides the isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z')))_{l^n} \cong (E_2^{0,1})_{l^n} = \mathrm{Hom}(\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}.$$

Combining this isomorphism with the isomorphism of Step 3, we obtain an isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, E(K[c]_{z^\times}))_{l^n} \cong \mathrm{Hom}(\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}.$$

The image of Δ under this isomorphism is given by the restriction of the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}$$

to the subgroup $\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'})$ where this restricted cocycle takes its values in the subgroup $\mathcal{E}_0(\kappa(z^\sharp))$ of $\mathcal{E}_0(\kappa(z'))$, as required.

Step 5. We have an isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, E(K[c]_{z^\times}))_{l^n} \cong \mathrm{Hom}(G(c/c'), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}.$$

The image of Δ under this isomorphism is given by the restriction of the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}$$

to the subgroup $\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}) \cong G(c/c')$.

The group $\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'})$ has order (see (2.3.8), (2.3.12))

$$\begin{aligned} |\kappa(z)| + 1 \quad & \text{if } c' \neq 0; \\ (|\kappa(z)| + 1)/|B^*/A^*| \quad & \text{if } c' = 0. \end{aligned}$$

As $K \neq F \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$ (by the hypothesis (7.6.1)(c)) we have that B^*/A^* is the trivial group. Hence passage to the completions provides an isomorphism of groups

$$\mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}) \cong G(c/c')$$

where $G(c/c')$ is a cyclic group of order $|\kappa(z)|+1$ and where this isomorphism is compatible with the action of the galois groups on $\bar{P}_c \in E(K[c])$. We obtain the isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, \mathcal{E}_0(\kappa(z^\sharp))) \cong \mathrm{Hom}(G(c/c'), \mathcal{E}_0(\kappa(z^\sharp))).$$

From Step 4, we then obtain an isomorphism

$$H^1(K[c]_{z^\times}/K_{z^\sharp}, E(K[c]_{z^\times}))_{l^n} \to \mathrm{Hom}(G(c/c'), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}$$

as required. The image of Δ under this isomorphism is given by the restriction of the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}$$

to the subgroup $G(c/c') \cong \mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'})$ where the restricted cocycle takes its values in the subgroup $\mathcal{E}_0(\kappa(z^\sharp))$ of $\mathcal{E}_0(\kappa(z'))$.

Step 6. End of proof.

By Step 5, the image of Δ in $\mathrm{Hom}(G(c/c'), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}$ is given by the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}, \quad \mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}) \cong G(c/c') \to \mathcal{E}_0(\kappa(z^\sharp)).$$

This cocycle is the reduction modulo $z^\times$ of a cocycle in $H^1(K[c]/K[c'], E(K[c]))^{\mathrm{Gal}(K[c']/K)}$ given by $g \mapsto -\frac{(g-1)\bar{P}_c}{l^n}$.

Since $G(c/c-z) = G(c/c')$ is cyclic and generated by σ_z (notation 7.14.10(i)), the cohomology class Δ has the same order as Q (mod $z^\times$) where

$$Q = -\frac{(\sigma_z - 1)\bar{P}_c}{l^n}.$$

We write $\mathcal{Q}$ for the image of Q modulo $z^\sharp$ in $\mathcal{E}_0(\kappa(z^\times))$ where $\mathcal{Q}$ lies in the subgroup $\mathcal{E}_0(\kappa(z^\sharp))$.

The definition of P_c (see notation 7.14.10) is the following. Let $c = \sum_{i=1}^r z_i$ be the decomposition of c as a sum of distinct prime divisors, where we write $z = z_1$. Put $S = \mathbb{Z}/l^n\mathbb{Z}$. Let $< a, c >$ be a standard generator of the Heegner module $\mathcal{H}_{c,S}$ where $a \in \mathrm{Pic}(O_c)$ (see (5.3.8)). Then we have

$$P_c = \tilde{\eta}_c(< a, c > \otimes h_{z_1} \otimes \ldots \otimes h_{z_r}) \in (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$$

where h_{z_i} are standard generators of $\mathrm{Hom}(G(c/c-z_i), S)$; the element $\bar{P}_c$ is an inverse image of P_c under the map $E(K[c]) \to E(K[c]) \otimes_{\mathbb{Z}} S$. The map $\tilde{\eta}_c$ is the composite

$$\mathcal{H}_{c,S} \otimes_S M(c) \overset{\mathrm{Tr}_{K[0]/K} \circ \eta}{\longrightarrow} (\mathcal{H}_{c,S})^{\mathcal{G}_c} \overset{f}{\to} (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}$$

where f is defined in the diagram (7.14.5).

The elements h_{z_i} are group homomorphisms with values in the additive group of S where

$$h_{z_i} \in \mathrm{Hom}(G(c/c-z_i), S) \text{ for all } i.$$

Let ψ_0 be the multilinear map

$$\psi_0 : \prod_i G(c/c-z_i) \to S$$

$$(g_1, \ldots, g_r) \mapsto \prod_i h_{z_i}(g_i).$$

As the kernel of the natural homomorphism $\prod_i G(c/c - z_i) \to G(c/0)$ has order which is a unit of S, it follows that the map ψ_0 factors though a map $\psi : G(c/0) \to S$ where the restriction of ψ to each subgroup $G(c/c - z_i)$ is equal to h_{z_i} for all i (as in the definition of η in the proof of proposition 7.13.4).

The map ψ is a 1-cochain in $\mathrm{Coch}^1(G(c/0), S)$. Let

$$E_\psi = \sum_{g \in G(c/0)} \psi(g) g^{-1}$$

be the Kolyvagin element of ψ (see §5.6, definition 5.6.11), where

$$E_\psi \in S[G(c/0)].$$

The map η is then given by

$$\delta \otimes a \mapsto E_\psi(a\delta)$$

where $\delta \in \mathcal{H}_{c,S}$ and $a \in \bigotimes_i \mathrm{Ann}_S(a_{z_i} \otimes 1)$.

We have an exact sequence of abelian groups

$$0 \to G(c/c') \to G(c/0) \to G(c'/0) \to 0.$$

We obtain a corresponding decomposition of the Kolyvagin element E_ψ

$$E_\psi = \sum_{g \in G(c/c')} \psi(g) g^{-1} \sum_{h \in G(c/0)/G(c/c')} \psi(h) h^{-1}$$

where the inner sum here runs over a set of coset representatives of $G(c/c')$ in $G(c/0)$. Put, where the sum runs over a fixed set of coset representatives,

$$E_1 = \sum_{h \in G(c/0)/G(c/c')} \psi(h) h^{-1}.$$

Then E_1 is an element of $S[G(c/0)]$; select a lifting $E_1^\sharp$ of E_1 where $E_1^\sharp \in \mathbb{Z}[G(c/0)]$ and

$$E_1^\sharp \equiv E_1 \pmod{l^n}.$$

Let $\psi_1^\sharp$ be a lifting of $\psi_1 : G(c/c') \to S$ to $\mathbb{Z}$; that is to say

$$\psi_1^\sharp : G(c/c') \to \mathbb{Z}$$

is a map such that

$$\psi_1^\sharp \equiv \psi_1 \pmod{l^n}.$$

Let $E_{\psi_1^\sharp} \in \mathbb{Z}[G(c/0)]$ be the Kolyvagin element of $\psi_1^\sharp$. Then $E_{\psi_1^\sharp}$ is a lifting of

$$E_{\psi_1} = \sum_{g \in G(c/c')} \psi_1(g) g^{-1}.$$

Then we have

$$E_{\psi_1^\sharp} E_1^\sharp \equiv E_\psi \pmod{l^n}.$$

As in 7.14.10, the element σ_{z_1} is a standard generator of the cyclic group $G(c/c')$ and $h_{z_1} : G(c/c') \to S$ is the homomorphism $\sigma_{z_1} \mapsto 1$. We may then select a lifting $\Psi : G(c/c') \to \mathbb{Z}$ where

$$\sigma_{z_1}^{-s} \mapsto -s, \quad \text{for } s = 0, 1, \ldots, |G(c/c')| - 1.$$

The Kolyvagin element of Ψ is then

$$E_\Psi = -\sum_{r=1}^{|G(c/c')|-1} r\sigma_{z_1}^r.$$

We have

$$(\sigma_{z_1} - 1)E_\Psi = e_{G(c/c')} - |G(c/c')|. \tag{7.14.15}$$

Furthermore, we have

$$E_{\psi_1^\sharp} \equiv E_\Psi \pmod{l^n}.$$

As $E_{\psi_1^\sharp}$ is a Kolyvagin element, we have by proposition 5.6.12,

$$(g-1)E_{\psi_1^\sharp} = \psi_1^\sharp(g) e_{G(c/c')} - \sum_{h \in G(c/c')} h^{-1}(\partial^1 \psi_1^\sharp)(h, g), \quad \text{for all } g \in G(c/c').$$

As ψ_1 is a homomorphism $G(c/c') \to S$ we have that

$$(\partial^1 \psi_1^\sharp)(h, g) \in l^n \mathbb{Z} \text{ for all } g, h \in G(c/c').$$

By definition we have

$$P_c = f \circ \mathrm{Tr}_{K[0]/K} \circ \eta(< a, c > \otimes h_{z_1} \otimes \ldots \otimes h_{z_r}) \in (E(K[c]) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_c}.$$

Let $\mathcal{S}$ be a set of coset representatives of $G(c/0)$ in $\mathcal{G}_c = \mathrm{Gal}(K[c]/K)$. The element $\bar{P}_c \in E(K[c])$, which is any lifting of P_c, may then be taken to be

$$\bar{P}_c = \sum_{\sigma \in S} \sigma E_1^\sharp E_\Psi y_{a,c}.$$

If here E_Ψ is replaced by $E_{\psi_1}^\sharp$ then $\bar{P}_c$ is changed by an element of $l^n E(K[c])$.

Put

$$a' = t_{c,c'}^\Delta(a) \in \mathrm{Pic}(O_{c'}).$$

We have (see (4.8.3) and the table 4.8.5), where $y_{a,c} = (a, I_1, c, \pi)$,

$$\frac{|O_{c'}^*|}{|A^*|} \mathrm{Tr}_{K[c]/K[c']} y_{a,c} = a_z y_{a',c'}.$$

By definition $Q = -((\sigma_z - 1)\bar{P}_c)/l^n$ hence we have from (7.14.15)

$$Q = -\sum_{\sigma\in\mathcal{S}} \sigma E_1^\sharp\big(\frac{(\sigma_z - 1)E_\Psi}{l^n}\big)y_{a,c}$$

$$= \sum_{\sigma\in\mathcal{S}} \sigma E_1^\sharp\big(\frac{|G(c/c')|}{l^n}y_{a,c} - \frac{|A^*|}{|O^*_{c'}|}\frac{a_z}{l^n}y_{a',c'}\big).$$

As K is not obtained from F by ground field extension (hypothesis 7.6.1(c)), we have $A^* = O^*_{c'}$; hence we obtain

$$Q = \sum_{\sigma\in\mathcal{S}} \sigma E_1^\sharp\big(\frac{|G(c/c')|}{l^n}y_{a,c} - \frac{a_z}{l^n}y_{a',c'}\big).$$

As the image of Δ in $\mathrm{Hom}(G(c/c'), \mathcal{E}_0(\kappa(z^\sharp)))_{l^n}$ is given by the cocycle

$$g \mapsto -\frac{(g-1)\bar{P}_c}{l^n} \pmod{z^\times}, \quad \mathrm{Gal}(K[c]_{z^\times}/K[c']_{z'}) \cong G(c/c') \to \mathcal{E}_0(\kappa(z^\sharp))$$

we have that $-\frac{(g-1)\bar{P}_c}{l^n}$ modulo $z^\times$ lies in $\mathcal{E}_0(\kappa(z^\sharp))$. Hence the point $\mathcal{Q}$ lies in $\mathcal{E}_0(\kappa(z^\sharp))$. It follows that $-(g_z - 1)\bar{P}_c$ modulo $z^\times$ lies in $\mathcal{E}_0(\kappa(z^\sharp))$.

Denote by Frob_z the Frobenius automorphism $x \mapsto x^{|\kappa(z)|}$ of the closed fibre $\mathcal{E}_0/\kappa(z)$ of the Néron model of E/F. Theorem 4.8.9 gives that for any prime z'' of $K[c']$ above z we have, where $y_{a,c} = (a, I_1, c, \pi)$,

$$\mathrm{Frob}_z y_{a,c} \equiv y_{a',c'} \pmod{z''}. \tag{7.14.16}$$

As z is inert and unramified in K/F, theorem 4.6.19(ii) shows that the point $< a, c >$ of the modular curve $X_0^{\mathrm{Drin}}(I) \otimes \kappa(z)$ is defined over the quadratic extension field $\kappa(z^\sharp)$ of $\kappa(z)$. As the map

$$\pi : X_0^{\mathrm{Drin}}(I) \to E$$

is a morphism of F-schemes, we obtain that $y_{a,c}$ mod $z^\times$ is defined over the subfield $\kappa(z^\sharp)$ of $\kappa(z^\times)$. Hence we have from (7.14.16)

$$\frac{|G(c/c')|}{l^n}y_{a,c} - \frac{a_z}{l^n}y_{a',c'} \equiv \frac{|G(c/c')|\mathrm{Frob}_z - a_z}{l^n}y_{a',c'} \pmod{z''}.$$

By definition the point $P_{c'} \in (E(K[c']) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_{c'}}$ is given by

$$P_{c'} = f \circ \mathrm{Tr}_{K[0]/K} \circ \eta(< a', c' > \otimes h_{z_2} \otimes \ldots \otimes h_{z_r})$$

where f is here the map

$$f : (\mathcal{H}_{c',S})^{\mathcal{G}_{c'}} \to (E(K[c']) \otimes_{\mathbb{Z}} S)^{\mathcal{G}_{c'}}.$$

Let $\bar{P}_{c'} \in E(K[c'])$ be an inverse image of $P_{c'}$ under the map $E(K[c']) \to E(K[c']) \otimes_{\mathbb{Z}} S$. In view of the action of E_1 on $E(K[c']) \otimes_{\mathbb{Z}} S$, the element $\bar{P}_{c'}$ may be taken to be

$$\bar{P}_{c'} = \sum_{\sigma \in \mathcal{S}} \sigma E_1^\sharp y_{a',c'}$$

where $E_1^\sharp \in \mathbb{Z}[G(c/0)]$ is a lifting of E_1. We then have

$$Q = \sum_{\sigma \in \mathcal{S}} \sigma E_1^\sharp \Big(\frac{|G(c/c')|}{l^n} y_{a,c} - \frac{a_z}{l^n} y_{a',c'} \Big)$$

$$\equiv \mathcal{Q} \equiv \frac{|G(c/c')|\mathrm{Frob}_z - a_z}{l^n} \bar{P}_{c'} \pmod{z''}. \tag{7.14.17}$$

The homomorphism $|G(c/c')|\mathrm{Frob}_z - a_z$ annihilates $\mathcal{E}_0(\kappa(z^\sharp))$. For we have that the frobenius Frob_z acts on $\mathcal{E}_0/\kappa(z)$ with characteristic polynomial

$$x^2 - xa_z + |\kappa(z)|.$$

Writing F for Frob_z it follows that $F^2 - Fa_z + |\kappa(z)|$ annihilates $\mathcal{E}_0(\kappa(z^\sharp))$. But F^2 is the identity automorphism on $\mathcal{E}_0(\kappa(z^\sharp))$ as $\kappa(z^\sharp)/\kappa(z)$ is a quadratic extension of finite fields. Hence $F^2 - Fa_z + F^2|\kappa(z)|$ annihilates $\mathcal{E}_0(\kappa(z^\sharp))$. That is to say $F(F(1+|\kappa(z)|) - a_z)$ annihilates $\mathcal{E}_0(\kappa(z^\sharp))$. As F is an automorphism we obtain that $F(1 + |\kappa(z)|) - a_z$ annihilates $\mathcal{E}_0(\kappa(z^\sharp))$, as required.

Let $\alpha, \beta \in \mathbb{C}$ be the complex roots of the characteristic polynomial of frobenius Frob_z acting on $\mathcal{E}_0/\kappa(z)$

$$x^2 - xa_z + |\kappa(z)|.$$

Then we have, where $G(c/c')$ is cyclic of order $|\kappa(z)| + 1$,

$$|\mathcal{E}_0(\kappa(z))| = |G(c/c')| - \alpha - \beta = |G(c/c')| - a_z$$

and

$$|\mathcal{E}_0(\kappa(z^\sharp))| = |\kappa(z)|^2 + 1 - \alpha^2 - \beta^2 = |\kappa(z)|^2 + 1 - a_z^2 + 2|\kappa(z)|$$

$$= (|G(c/c')| - a_z)(|G(c/c')| + a_z).$$

We then obtain the decomposition under the action of τ, the non-trivial element of $\mathrm{Gal}(K/F)$,

$$\mathcal{E}_0(\kappa(z^\sharp)) \cong \mathcal{E}_0(\kappa(z)) \oplus \mathcal{E}_0(\kappa(z^\sharp))^-$$

where

$$|\mathcal{E}_0(\kappa(z^\sharp))^\epsilon| = |G(c/c')| - \epsilon a_z \quad \text{for } \epsilon = \pm 1.$$

By lemma 7.11.5, we have group isomorphisms

$$\mathcal{E}_0(\kappa(z^\sharp))^\epsilon_{l^n} \cong \frac{\mathbb{Z}}{l^n\mathbb{Z}} \text{ for } \epsilon = \pm 1.$$

In particular, as $n \geq 1$ the l-torsion subgroups of $\mathcal{E}_0(\kappa(z^\sharp))^-$ and $\mathcal{E}_0(\kappa(z^\sharp))^+$ are both non-trivial. As

$$\mathcal{E}_0(\overline{\kappa(z)})_{l^t} \cong \frac{\mathbb{Z}}{l^t\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l^t\mathbb{Z}} \text{ for all } t \geq 1$$

we obtain that the l-torsion subgroups of $\mathcal{E}_0(\kappa(z^\sharp))^-_{l^\infty}$ and $\mathcal{E}_0(\kappa(z^\sharp))^+_{l^\infty}$ are both cyclic and denoting by $|.|_l$ the normalised l-adic absolute value on $\mathbb{Q}$ we have

$$|\mathcal{E}_0(\kappa(z^\sharp))^\epsilon_{l^\infty}| = |\ |G(c/c')| - \epsilon a_z|_l^{-1} \text{ for } \epsilon = \pm 1.$$

Let h be the homomorphism

$$h = \frac{|G(c/c')|\mathrm{Frob}_z - a_z}{l^n}.$$

The map

$$h : \mathcal{E}_0(\kappa(z^\sharp)) \to \mathcal{E}_0(\kappa(z^\sharp))$$

is annihilated by l^n; furthermore, $l^n\mathcal{E}_0(\kappa(z^\sharp))$ lies in the kernel of h. Hence h induces a homomorphism

$$h' : \mathcal{E}_0(\kappa(z^\sharp)) \otimes_{\mathbb{Z}} S \to \mathcal{E}_0(\kappa(z^\sharp))_{l^n}.$$

On each eigencomponent $(\mathcal{E}_0(\kappa(z^\sharp)) \otimes_{\mathbb{Z}} S)^\epsilon$, where $\epsilon = \pm 1$, the map h' is multiplication by the integer

$$N_\epsilon = \frac{\epsilon|G(c/c')| - a_z}{l^n}.$$

We have

$$|N_\epsilon|_l = l^n|\ |G(c/c')| - \epsilon a_z|_l = l^n|\mathcal{E}_0(\kappa(z^\sharp))^\epsilon_{l^\infty}|^{-1}.$$

It follows that the restriction of h' to each eigencomponent $(\mathcal{E}_0(\kappa(z^\sharp)) \otimes_{\mathbb{Z}} S)^\epsilon$ is an injection. As τ commutes with h, the homomorphism h' preserves the τ-eigencomponents. As $\mathcal{E}_0(\kappa(z^\sharp)) \otimes_{\mathbb{Z}} S$ and $\mathcal{E}_0(\kappa(z^\sharp))_{l^n}$ have the same number l^{2n} of elements it follows that h' is an isomorphism.

The reduction $P^\flat_{c'}$ of $P_{c'}$ modulo z'' lies in the $-\epsilon_{c'}$-eigenspace for τ on $\mathcal{E}_0(\kappa(z'')) \otimes_{\mathbb{Z}} S$ (see lemma 7.14.11(ii)). As we have by (7.14.17)

$$\mathcal{Q} = h'(P^\flat_{c'})$$

and that h' is an isomorphism it follows that $\mathcal{Q}$ and $P^\flat_{c'}$ have the same order. Since the kernel of the reduction

$$E(K[c']_{z''}) \to \mathcal{E}_0(\kappa(z''))$$

modulo z'' is a pro-p-group we have that $P_{c'}^{\flat}$ and $P_{c'}$ have the same order. This proves the stated result. □

7.14.18. Remark. Referring to the proof of part (ii) of the previous lemma 7.14.13, the prime $z^\sharp$ need not split completely in $K[c']/K$ as $z^\sharp$ is not necessarily a principal prime ideal of B, the integral closure of A in K. This is unlike the proof of part (ii) of lemma 5.7.10 of [Br2] where $z^\sharp$ splits completely in $K[c']/K$. This is the reason for some complications in the proof given above in comparison with the proof of [Br2, lemma 5.7.10].

7.14.19. Conjecture. For all but finitely many prime numbers l there is an integer $n(l) \geq 0$ such that for all integers $n > n(l)$ there is $c \in \mathrm{Div}_+(A)$ such that the homomorphism (see (7.14.5))

$$(\mathcal{H}^{(0)}_{c,\mathbb{Z}/l^n\mathbb{Z}})^{\mathcal{G}_c} \to H^1(K, E_{l^n})$$

is non-zero.

7.14.20. Conjecture. For all but finitely many prime numbers l we have $n(l) = 0$.

7.14.21. Conjecture. Suppose that l is a prime number where $l \in \mathcal{P} \setminus \mathcal{E}$ and $\mathcal{E}$ is the finite exceptional set of prime numbers of proposition 7.14.2. Then for all sufficiently large integers $n > 0$ there is $c \in \mathcal{D}_{l^n}$ such that the homomorphism (see lemma 7.14.9)

$$\gamma_c : \mathcal{H}_{c,\mathbb{Z}/l^n\mathbb{Z}} \to H^1(K, E_{l^n})$$

is non-zero.

7.14.22. Remarks. Evidently conjecture 7.14.21 implies that conjecture 7.14.19 holds for prime numbers $l \in \mathcal{P} \setminus \mathcal{E}$ where the divisors c are sums of distinct prime divisors which are inert and unramified in the field extension K/F (by proposition 7.13.4).

If l is a prime number where $l \in \mathcal{P} \setminus \mathcal{E}$ then

$$\gamma_0 : \mathcal{H}_{0,\mathbb{Z}/l^n\mathbb{Z}} \to H^1(K, E_{l^n})$$

is non-zero for all sufficiently large n if and only if $x = \mathrm{Tr}_{K[0]/K}(a, I_1, 0, \pi)$ has infinite order in $E(K)$ (by remarks 7.14.12(i) and (ii)).

These conjectures above are the counterparts of conjectures of Kolyvagin [K3] for elliptic curves over $\mathbb{Q}$.

7.15 Tate-Poitou local duality

We shall briefly explain Tate-Poitou local duality for elliptic curves over a local field. For more details see [M, Chapter 1].

(7.15.1) Let

L be a non-archimedian complete local field with valuation $v : L^* \to \mathbb{Z}$;
A/L be an elliptic curve over L;
$n \geq 1$ be an integer prime to the characteristic of L;
G be the Galois group $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ where L^{sep} is a separable closure of L.

(7.15.2) Let μ_n be the multiplicative subgroup of L^{sep} of nth roots of unity. Then μ_n is a finite G-module. Let A_n denote the G-module of n-torsion points of $A(L^{\mathrm{sep}})$. We have an abelian group isomorphism

$$A_n \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Denote by $\{,\}$ the Weil pairing

$$\{,\} : A_n \times A_n \to \mu_n.$$

This is a perfect pairing of G-modules. In particular, we have an isomorphism of G-modules

$$A_n \cong \mathrm{Hom}_G(A_n, \mu_n).$$

(7.15.3) The Weil pairing induces a cup-product pairing in Galois cohomology

$$H^1(L, A_n) \times H^1(L, A_n) \to H^2(L, \mu_n).$$

By local class field theory, we have a canonical isomorphism of abelian groups, where $\mathrm{Br}(L)$ is the Brauer group of L,

$$\mathrm{Br}(L) \cong \frac{\mathbb{Q}}{\mathbb{Z}}.$$

This induces an isomorphism

$$H^2(L, \mu_n) = \mathrm{Br}(L)_n \cong \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

7.15.4. Theorem. (Tate-Poitou local duality). *The cup product pairing*

$$<,>_v: H^1(L, A_n) \times H^1(L, A_n) \to \frac{\mathbb{Z}}{n\mathbb{Z}} \tag{7.15.5}$$

obtained from the Weil pairing is an alternating and non-degenerate pairing of $\frac{\mathbb{Z}}{n\mathbb{Z}}$*-modules.*

[See [M, Chapter 1, Cor. 2.3].]□

7.15.6. Theorem. *Assume that* n *is prime to the residue field characteristic of* L.

(i) *The subgroup* ${}_nA(L)$ *of* $H^1(L, A_n)$ *is isotropic for the alternating pairing* $<,>_v$.

(ii) *If* A *has good reduction at* v *then the pairing* $<,>_v$ *on* $H^1(L, A_n)$ *induces a non-degenerate pairing of abelian groups*

$$<,>_v: {}_nA(L) \times H^1(L, A)_n \to \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Proof. (i) Let L^{nr} be the maximal unramified separable extension of L. We have the commutative diagram with exact rows obtained by multiplication by n

$$\begin{array}{ccccccccc} 0 & \to & A_n(L^{\mathrm{nr}}) & \to & A(L^{\mathrm{nr}}) & \xrightarrow{n} & A(L^{\mathrm{nr}}) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & A_n(L^{\mathrm{sep}}) & \to & A(L^{\mathrm{sep}}) & \xrightarrow{n} & A(L^{\mathrm{sep}}) & \to & 0 \end{array}$$

The long exact sequence of cohomology associated to these exact sequences provides the commutative diagram with exact rows

(7.15.7)

$$\begin{array}{ccccccccc} 0 & \to & {}_nA(L) & \to & H^1(L^{\mathrm{nr}}/L, A_n(L^{\mathrm{nr}})) & \to & H^1(L^{\mathrm{nr}}/L, A(L^{\mathrm{nr}}))_n & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & {}_nA(L) & \to & H^1(L, A_n) & \to & H^1(L, A)_n & \to & 0 \end{array}$$

It follows that the subgroup ${}_nA(L)$ of $H^1(L, A_n)$ is isotropic for the alternating pairing $<,>_v$ as we have

$$H^2(L^{\mathrm{nr}}/L, \mu_n(L^{\mathrm{nr}})) = 0.$$

(ii) If A has good reduction at v then $H^1(L^{\mathrm{nr}}/L, A(L^{\mathrm{nr}})) = 0$ (by theorem 7.10.2) and the diagram (7.15.7) then provides an isomorphism

$${}_nA(L) \cong H^1(L^{\mathrm{nr}}/L, A_n(L^{\mathrm{nr}})).$$

The result now follows from the diagram (7.15.7) and that the subgroup $H^1(L^{\mathrm{nr}}/L, A_n(L^{\mathrm{nr}}))$ is a *maximal* isotropic subgroup of $H^1(L, A_n)$ (see [M, Chap. 1, Theorem 2.6]). □

7.16 Application of Tate-Poitou duality

(7.16.1) We retain the notation of §§7.5, 7.6. in particular, we assume that
K is an imaginary quadratic extension field of F with respect to ∞;
E/F is an elliptic curve satisfying the conditions of (7.6.1);
$n > 2$ is an odd integer prime to the characteristic of F;
τ is the non-trivial element of $\mathrm{Gal}(K/F)$.

(7.16.2) The element τ acts on the Selmer group $S^{(n)}(E/K)$ of the elliptic curve $E\times_F K$ over K (see §7.9); as n is an odd integer, we have a decomposition into eigenspaces under the action of τ (see (7.11.2))

$$S^{(n)}(E/K) = S^{(n)}(E/K)^+ \oplus S^{(n)}(E/K)^-$$

where the sign $+$ or $-$ denotes the submodule on which τ acts as $+1$ or -1 respectively.

7.16.3. Proposition. *Let w be a place of K such that E has good reduction at w. Let $\epsilon = +$ or $-$. Let $m \geq 1$ be an integer dividing n. Suppose that d is an element of the eigenspace $H^1(K,E)^\epsilon_n$ of τ which satisfies the conditions*
(i) $\mathrm{res}_v(d) = 0$ *for all places v of K distinct from w;*
(ii) $\mathrm{res}_w(d)$ *has order divisible by n/m in the eigenspace $H^1(K_w,E)^\epsilon_n$;*
(iii) ${}_nE(K_w)^\epsilon$ *is a cyclic abelian group.*
Then the homomorphism $\mathrm{res}_w : S^{(n)}(E/K)^\epsilon \to {}_nE(K_w)$ *is annihilated by m.*

Proof. Let μ_n be the subgroup of $K^{\mathrm{sep}*}$ of nth roots of unity. Then μ_n is a finite $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module. Denote by $\{,\}$ the global Weil pairing

$$\{,\} : E_n \times E_n \to \mu_n.$$

This is a perfect pairing of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules. In particular, we have an isomorphism of G-modules

$$E_n \cong \mathrm{Hom}_{\mathrm{Gal}(K^{\mathrm{sep}}/K)}(E_n, \mu_n).$$

Denote by $<,>$ the global pairing obtained by cup product from the global Weil pairing $\{,\}$

$$<,>:\ H^1(K,E_n) \times H^1(K,E_n) \to H^2(K,\mu_n) = \mathrm{Br}(K)_n$$

where $\mathrm{Br}(K)$ is the Brauer group of K.

For any place v of K let $<,>_v$ denote the local Tate-Poitou pairing (as in theorem 7.15.4)

$$<,>_v:\ H^1(K_v,E_n) \times H^1(K_v,E_n) \to \mathbb{Z}/n\mathbb{Z}$$

where K_v denotes the completion of K at the place v. This induces a non-degenerate pairing of abelian groups (theorem 7.15.6)

$$ {}_nE(K_v)^{\pm} \times H^1(K_v, E)^{\pm}_n \to \mathbb{Z}/n\mathbb{Z}. $$

The global pairing $<,>$ is given in terms of the local Tate-Poitou pairings $<,>_v$ (see §7.15) via the exact sequence obtained from class field theory

$$ 0 \to \mathrm{Br}(K) \to \bigoplus_{v\in\Sigma_K} \mathrm{Br}(K_v) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0\,. \tag{7.16.4} $$

That is to say, the global pairing is the sum of the local pairings of the restrictions

$$ < x, y >= \bigoplus_{v\in\Sigma_K} < \mathrm{res}_v(x), \mathrm{res}_v(y) >_v, \quad \text{for all } x, y \in H^1(K, E_n). $$

Via the exact sequence, obtained by multiplication by n,

$$ 0 \to ({}_nE(K))^{\epsilon} \to H^1(K, E_n)^{\epsilon} \to H^1(K, E)^{\epsilon}_n \to 0 $$

the class d lifts to a class c in $H^1(K, E_n)^{\epsilon}$; this element c is determined uniquely up to the addition of an element of $({}_nE(K))^{\epsilon}$.

Let $s \in S^{(n)}(E/K)^{\epsilon}$. Then we have $\mathrm{res}_v(s) \in ({}_nE(K_v))^{\epsilon}$ for all places $v \in \Sigma_K$ and we have from property (i) of d and theorem 7.15.6(i)

$$ < \mathrm{res}_v(s), \mathrm{res}_v(d) >_v = < \mathrm{res}_v(s), \mathrm{res}_v(c) >_v = 0 \quad \text{for all} \quad v \in \Sigma_K \setminus \{w\}. $$

Hence we have

$$ < s, c >= \bigoplus_{v\in\Sigma_K} < \mathrm{res}_v(s), \mathrm{res}_v(c) >_v $$

where all terms except at most one in the sum are zero. But

$$ \sum_{v\in\Sigma_K} < \mathrm{res}_v(s), \mathrm{res}_v(c) >_v $$

is equal to zero by the exact sequence (7.16.4); hence we must have (theorem 7.15.6(ii))

$$ < \mathrm{res}_w(s), \mathrm{res}_w(c) >_w = < \mathrm{res}_w(s), \mathrm{res}_w(d) >_w = 0. $$

By property (ii) of d, the element $\mathrm{res}_w(d)$ has order divisible by n/m; hence we have that $m\mathrm{res}_w(s) = 0$ as ${}_nE(K_w)^{\epsilon}$ is a cyclic abelian group and by the non-degeneracy of the local pairing $<,>_w$ (theorem 7.15.6). □

7.17 Equivariant Pontrjagin duality

In this section we give an equivariant version of Pontrjagin duality. This variant of Pontrjagin duality explained below may be extended to general locally compact topological abelian groups but we here only consider a special case.

[For more details on Pontrjagin duality, see [P]].

(7.17.1) Let S be a multiplicative set of non-zero integers $S \subseteq \mathbb{Z}$; we may assume that S is saturated that is to say if $mn \in S$ where m, n are integers then $m \in S$ and $n \in S$. Let $S^{-1}\mathbb{Z}$ denote the subring of $\mathbb{Q}$ of rational numbers of the form p/q where $p \in \mathbb{Z}$ and $q \in S$. Let $S^{-1}\mathbb{Z}/\mathbb{Z}$ denote the subgroup of $\mathbb{Q}/\mathbb{Z}$ of torsion annihilated by the integers in S.

The group $S^{-1}\mathbb{Z}/\mathbb{Z}$ is equipped with its topology as a subgroup of the circle group $\mathbb{R}/\mathbb{Z}$ over $\mathbb{R}$.

(7.17.2) Let G be a locally compact topological abelian group. We assume that G is either a discrete torsion group or is a profinite group; in the main duality theorem 7.17.11 we assume that G is a discrete torsion group.

7.17.3. Definition. The saturated multiplicative subset S of $\mathbb{Z}$ is *sufficiently large* if when G is torsion then the order of every element of G lies in S and if when G is profinite then the order of G/U for every open subgroup U of G also lies in S.

(7.17.4) The group

$$G^* = \mathrm{Hom}_{\mathrm{cts}}(G, S^{-1}\mathbb{Z}/\mathbb{Z})$$

denotes the group of continuous characters of G with values in $S^{-1}\mathbb{Z}/\mathbb{Z}$. The group G^* is equipped with a topology making it a topological group in the following way.

For any subset U of G and any subset V of $S^{-1}\mathbb{Z}/\mathbb{Z}$ let $W(U, V)$ denote the set of characters $\chi \in G^*$ such that $\chi(U) \subseteq V$.

For any integer $k \geq 1$ let Λ_k be the set of elements x of $S^{-1}\mathbb{Z}/\mathbb{Z}$ such that x admits a representative y in $S^{-1}\mathbb{Z} \subset \mathbb{R}$ such that $|y| < 1/(3k)$. Then the set of sets of the form $W(U, \Lambda_k)$ for any compact subset U of G and any integer $k \geq 1$ forms a base of neighbourhoods of 0 of G^* and this defines the topology on the group G^*.

If S is the set of all non-zero natural numbers then G^* is the Pontrjagin dual of G, where the abelian group G is here assumed to be either discrete torsion or profinite.

(7.17.5) Let P be a profinite group, not necessarily commutative, and let M be a finite direct sum of n copies of $S^{-1}\mathbb{Z}/\mathbb{Z}$ equipped with its induced topology.

Then M is an abelian topological group. Assume that there is a continuous group homomorphism

$$\rho : P \to \mathrm{Aut}(M).$$

Then P acts on the topological group

$$G^\diamond = \mathrm{Hom}_{\mathrm{cts}}(G, M)$$

which is a direct sum of n copies of the Pontrjagin dual G^*. The set of sets of the form $W(U, V)$ for any compact subset U of G and any open neighbourhood V of zero of M forms a base of neighbourhoods of zero of $G^\diamond$.

We call $G^\diamond$ the *P-character group* of G.

(7.17.6) We obtain a pairing of topological groups

$$(,) : G \times G^\diamond \ \to \ M, \quad g \times \chi \mapsto (g, \chi) = \chi(g).$$

This pairing satisfies

$$p(g, \chi) = (g, \chi^{p^{-1}}) \ \text{ for all } p \in P, \ g \in G, \ \chi \in G^\diamond.$$

We obtain an injection

$$G \to \mathrm{Hom}_P(G^\diamond, M)$$

where $\mathrm{Hom}_P(-,-)$ denotes the module of continuous homomorphisms of topological $\mathbb{Z}[P]$-modules. The topology on $\mathrm{Hom}_P(G^\diamond, M)$ is that as a subspace of the topological group $(G^\diamond)^\diamond = \mathrm{Hom}_{\mathrm{cts}}(G^\diamond, M)$.

7.17.7. Proposition. *Assume that S is sufficiently large.*
(i) *Let H be a subgroup of the topological group G and let Φ be the annihilator of H that is*

$$\Phi = \{\chi \in G^\diamond | \ \ \chi(h) = 0 \ \text{ for all } h \in H\}.$$

Then the map

$$\Phi \mapsto \mathrm{Hom}_{\mathrm{cts}}(G/H, M), \quad x \mapsto \{g + H \mapsto x(g + H)\}$$

defines an isomorphism of topological groups $\Phi \cong (G/H)^\diamond$.
(ii) *Let Φ be a $\mathbb{Z}[P]$-submodule of the topological group $G^\diamond$ and let $A \subset \mathrm{Hom}_P(G^\diamond, M)$ be the annihilator of Φ that is*

$$A = \{h \in \mathrm{Hom}_P(G^\diamond, M) | \ \ h(\chi) = 0 \ \text{ for all } \chi \in \Phi\}.$$

Then the map

$$A \to \mathrm{Hom}_P(G^\diamond/\Phi, M), \quad x \mapsto \{\chi + \Phi \mapsto x(\chi + \Phi)\}$$

defines an isomorphism of topological groups

$$A \cong \mathrm{Hom}_P(G^\diamond/\Phi, M).$$

Proof. (i) As G is torsion or profinite and S is sufficiently large, G^* is topologically isomorphic to the Pontrjagin dual of G. Hence

$$G^\diamond \cong \bigoplus_{i=1}^{n} G^*$$

is a topological isomorphism where P acts continuously on $G^\diamond$. The property of the annhilator for the Pontrjagin dual [P, theorem 37, p.243] then transposes to $G^\diamond$.
(ii) Let $f : G^\diamond \to G^\diamond/\Phi$ be the natural surjective topological homomorphism. Let

$$\phi : \mathrm{Hom}_P(G^\diamond/\Phi, M) \to \mathrm{Hom}_P(G^\diamond, M)$$

be the induced map.

Let $h \in A$. Then we have $h(\Phi) = 0$ hence there is a homomorphism of $\mathbb{Z}[P]$-modules $x : G^\diamond/\Phi \to M$ such that $h = x \circ f$. To show that x is continuous, let V be a neighbourhood of zero of M. Let U be a neighbourhood of zero of $G^\diamond$ such that $h(U) \subseteq V$. Then $f(U)$ is a neighbourhood of zero of $G^\diamond/\Phi$ which satisfies $x(f(U)) = h(U) \subseteq V$. It follows that x is continuous. Furthermore, for any $h \in A$ there is an element $x \in \mathrm{Hom}_P(G^\diamond/\Phi, M)$ such that $h = x \circ f$; hence we have $\phi(\mathrm{Hom}_P(G^\diamond/\Phi, M)) = A$.

The kernel of ϕ is evidently zero so that ϕ is injective. Hence ϕ defines an isomorphism of groups which is continuous

$$\phi^* : \mathrm{Hom}_P(G^\diamond/\Phi, M) \to A.$$

Let $W(F^*, V)$ be any neighbourhood of zero of $\mathrm{Hom}_P(G^\diamond/\Phi, M)$ where F^* is a compact subset of $G^\diamond/\Phi$ and V is an open neighbourhood of zero of M. Let U be an open neighbourhood of zero of $G^\diamond$ having compact closure. The compact set F^* is contained in the union of a finite number of open sets of the form $f(x_i + U)$, $x_i \in G^\diamond$; let $F \subset G^\diamond$ be the union of the corresponding compact sets $x_i + \bar{U}$. Then we have $f(F) \supseteq F^*$.

Let $h \in A \cap W(F, V)$. Then as has already been shown there is an element $x \in \mathrm{Hom}_P(G^\diamond/\Phi, M)$ such that $h = x \circ f$; we then have $x(F^*) \subseteq x(f(F)) = h(F) \subseteq V$ and hence we have $x \in W(F^*, V)$. Hence we have $\phi(W(F^*, V)) \supseteq A \cap W(F, V)$ and we obtain that $\phi^* : \mathrm{Hom}_P(G^\diamond/\Phi, M) \to H$ is an open map. Hence ϕ^* is an isomorphism of topological groups. □

7.17.8. Proposition. *Let H be a subgroup of G and let $\Phi = \{f \in G^\diamond |\ \ f(H) = 0\}$ and $H' = \{f \in G |\ \ f(\Phi) = 0\}$. Then we have $H' = H$.*

Proof. Evidently we have $H \subseteq H'$. As $G^\diamond$ is a direct sum of a finite number of copies of the Pontrjagin dual G^* of G, the stated result follows from the same property for the Pontrjagin dual [P, theorem 40, p.252]. □

7.17.9. Proposition. *Let H be a subgroup of G and let $\Phi = \{f \in G^\diamond | \ \ f(H) = 0\}$. Then the $\mathbb{Z}[P]$-module $G^\diamond/\Phi$ is topologically isomorphic to the $\mathbb{Z}[P]$-module $H^\diamond$.*

Proof. As $G^\diamond$ is a direct sum of a finite number of copies of the Pontrjagin dual G^* of G, the stated result follows from the same property for the Pontrjagin dual [P, theorem 41, p.253]. □

(7.17.10) The group $S^{-1}\mathbb{Z}/\mathbb{Z}$ decomposes as a direct sum of primary components

$$S^{-1}\mathbb{Z}/\mathbb{Z} \cong \bigoplus_{l \in S} (l^{\mathbb{N}})^{-1}\mathbb{Z}/\mathbb{Z}$$

where $l^{\mathbb{N}}$ denotes the multiplicative subgroup of integers which are powers of l and l runs over all prime numbers contained in S. This isomorphism of groups in general is not an isomorphism of topological groups.

Similarly M decomposes as $\bigoplus_{l \in S} M_{l^\infty}$. The profinite group P acts continuously via this isomorphism on each component M_{l^∞} for all l.

7.17.11. Theorem. *Assume that:*

(1) *G is a discrete torsion group;*

(2) *S is sufficiently large;*

(3) *for each prime number $l \in S$, M_l is a simple $\mathbb{Z}[P]$-module and that*

$$\mathrm{End}_P(M_l) \cong \mathbb{Z}/l\mathbb{Z}.$$

Then the duality $(,) : G \times G^\diamond \to M$ is perfect that is to say the natural homomorphism

$$\omega : G \to \mathrm{Hom}_P(G^\diamond, M)$$

is an isomorphism of topological groups.

Proof. Let H be a finitely generated subgroup of G. Let

$$\Phi = \{\chi \in G^\diamond | \ \ \chi(H) = 0\}.$$

Let

$$G' = \mathrm{Hom}_P(G^\diamond, M).$$

Put

$$H' = \{f \in G' | \ \ f(\Phi) = 0\}.$$

Then $G^\diamond/\Phi$ is the P-character group of H by proposition 7.17.9.

It follows that we have an isomorphism

$$H' = \mathrm{Hom}_P(G^\diamond/\Phi, M) \cong \mathrm{Hom}_P(H^\diamond, M).$$

Furthermore the natural map

$$H \to H', \quad h \mapsto \{\chi \in H^\diamond \mapsto \chi(h) \in M\},$$

is an injection. For if $h \in H$ is in the kernel of this map then $\chi(h) = 0$ for all $\chi \in H^\diamond$. But $H^\diamond$ is a finite direct sum of Pontrjagin duals of H hence by Pontrjagin duality $h = 0$.

The group H is a finitely generated torsion group and therefore is finite. Hence H admits a canonical decomposition into finite cyclic groups of the form

$$H = \bigoplus_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$$

where the integers $m_i \geq 1$ satisfy

$$m_1 | m_2 | \ldots | m_r.$$

Then we have

$$H^\diamond = \mathrm{Hom}(H, M) = \bigoplus_{i=1}^{r} \mathrm{Hom}(\mathbb{Z}/m_i\mathbb{Z}, M) \cong \bigoplus_{i=1}^{r} M_{m_i}$$

where M_{m_i} is the $\mathbb{Z}[P]$-submodule of M annihilated by m_i. Hence we have an isomorphism of topological groups

$$\mathrm{Hom}_P(H^\diamond, M) \cong \bigoplus_{i=1}^{r} \mathrm{Hom}_P(M_{m_i}, M)$$

The image of any homomorphism of $\mathbb{Z}[P]$-modules $M_{m_i} \to M$ is contained in the submodule M_{m_i} of M. Hence we obtain an isomorphism

$$\mathrm{Hom}_P(H^\diamond, M) \cong \bigoplus_{i=1}^{r} \mathrm{Hom}_P(M_{m_i}, M_{m_i}). \tag{7.17.12}$$

Let

$$m_i = \prod_j l_j^{n_j}$$

be the factorisation of m_i as a product of prime powers where l_j are prime numbers of S and $n_j \in \mathbb{N}$ for all j. Then we have

$$\mathrm{Hom}_P(M_{m_i}, M_{m_i}) \cong \prod_j \mathrm{Hom}_P(M_{l_j^{n_j}}, M_{l_j^{n_j}}).$$

Let l be a prime number of S and let $n \geq 1$ be a positive integer. Put $F_r = l^{n-r} M_{l^n}$. The $\mathbb{Z}[P]$-module M_{l^n} admits a filtration of $\mathbb{Z}[P]$-submodules

$$M_{l^n} = F_n \supset F_{n-1} \supset \ldots \supset F_1 \supset \{0\}$$

where there are isomorphisms of $\mathbb{Z}[P]$-modules

$$F_r/F_{r-1} \cong M_l \quad \text{for all } r.$$

The module M_l is a simple $\mathbb{Z}[P]$-module by hypothesis. This Jordan-Hölder filtration of M_{l^n} is unique: the only $\mathbb{Z}[P]$-submodules of M_{l^n} are the modules F_r.

Let $s \in \mathrm{Hom}_P(M_{l^n}, M_{l^n})$. Then the image of s is a submodule of M_{l^n} which is annihilated by l^n and is equal to F_r for some r. As $s(M_{l^n}) = F_r$ we then have

$$s(F_t) = s(l^{n-t}M_{l^n}) = l^{n-r}s(M_{l^n}) = l^{n-r}F_t = F_{\max(r+t-n,0)}.$$

In particular, we have $s(F_{n-r+1}) = F_1$ and $s(F_{n-r}) = 0$. Hence the restriction $s|_{F_{n-r+1}}$ of s to F_{n-r+1} factors as

$$F_{n-r+1} \to F_{n-r+1}/F_{n-r} \cong F_1 \to F_1.$$

The isomorphism $F_{n-r+1}/F_{n-r} \cong F_1$ is obtained by multiplication by l^{n-r}; furthermore $\mathrm{End}_P(F_1) \cong \mathbb{Z}/l\mathbb{Z}$ by hypothesis. It follows that the homomorphism $s|_{F_{n-r+1}}$ is a homothety of the form $l^{n-r}m$ where $m \in \mathbb{Z}$ is an integer prime to l.

Similarly, we have $s|_{F_t/F_{t-1}} = n_t$ where $n_t \in \mathbb{Z}$ for all t and n_t is an integer of the form $l^{n-r}q_t$ where q_t is an integer prime to l. As $F_t = l^{n-t}M_{l^n}$ for all t it follows that there is an integer $q \in \mathbb{Z}$ such that $s|_{F_t/F_{t-1}} = q$ for all t. It follows from this and that the F_r form a filtation of M_{l^n} that the endomorphism s is the homothety of multiplication by the integer q. That is to say, there is an isomorphism

$$\mathrm{Hom}_P(M_{l^n}, M_{l^n}) \cong \mathbb{Z}/l^n\mathbb{Z}.$$

It follows that for any integer m in S there is an isomorphism of abelian groups

$$\mathrm{Hom}_P(M_m, M_m) \cong \mathbb{Z}/m\mathbb{Z}.$$

We obtain from (7.17.12) the isomorphism of discrete abelian groups

$$\mathrm{Hom}_P(H^\diamond, M) \cong \bigoplus_{i=1}^{r} \mathrm{Hom}_P(M_{m_i}, M_{m_i}) \cong \bigoplus_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z} \cong H.$$

Furthermore, we obtain that the injection

$$H \to \mathrm{Hom}_P(H^\diamond, M) = H'$$

is an isomorphism. We have proved that for any finitely generated subgroup H of G, the natural map $H \to H'$ is an isomorphism of topological groups.

Let a, b be arbitrary elements such that $a \in G$ and $b \in G'$. Let V be an open neigbourhood of zero of M. Let U be a neighbourhood of zero in $G^\diamond$

such that $b(U) \subseteq V$ and let $H_1 \subseteq G$ be a finitely generated subgroup such that $\{f \in G^\diamond |\ f(H_1) = 0\} \subseteq U$; as $G^\diamond$ is a finite direct sum of copies of the Pontrjagin dual of G that such a finitely generated subgroup exists follows from the same property holding for the Pontrjagin dual of G [P, §I of Section 36, p.250]. Let H be the subgroup of G generated by H_1 and a. Then we also have $\Phi = \{f \in G^\diamond |\ f(H) = 0\} \subseteq U$; as $b(\Phi) \subseteq V$ and Φ is a group, we must have $b(\Phi) = 0$ as M is a group divisible by integers belonging to S; hence we have $b \in H'$. That is to say, we have shown that there is a finitely generated subgroup H of G such that $a \in H$ and $b \in H'$. From the first part of the proof, the theorem holds for all finitely generated subgroups of G hence the natural map $\omega : G \to G'$ is an isomorphism of discrete abelian groups; this proves the theorem. □

7.18 Proof of theorem 7.7.5

The proof consists of proving separately the finiteness of the groups $Ш(E/K)^{\epsilon}_{l^\infty}$ and $Ш(E/K)^{-\epsilon}_{l^\infty}$ where ϵ is the sign in the functional equation of the L-function $L(s, E)$ of the elliptic curve E. For this, the cohomology classes $\delta(c)$ provide annihilators of the corresponding Selmer groups where c is a sum of at most 2 distinct prime divisors.

The field $L = K(E_{l^n})$

(7.18.1) Let

$\mathcal{P}$ be the infinite set of prime numbers given by definition 7.10.3;
$\mathcal{F}$ be the finite exceptional set of prime numbers of lemma 7.14.11;
$\epsilon = \pm 1$ be the sign in the functional equation of the L-function of E/F;
$l \in \mathcal{P} \setminus \mathcal{F}$.

Let $< a, 0 >$ where $a \in \mathrm{Pic}(B)$ be one of the standard generators of the Heegner module $\mathcal{H}_{0,\mathbb{Z}}$ with coefficients in $\mathbb{Z}$. We have that (see (7.14.4))

$$(a, I_1, 0, \pi) = \mathcal{H}(\pi)_{0,\mathbb{Z}}(< a, 0 >) \in E(K[0]).$$

Put

$$x_0 = \mathrm{Tr}_{K[0]/K}(a, I_1, 0, \pi)$$

where $x_0 \in E(K)$ lies in the group $E(K)$ of K-rational points of E. It is assumed that x_0 has infinite order in the group $E(K)$ (see theorem 7.7.5).

The element $P_0 = \tilde{\eta}_0(< a, 0 >)$ is the image in ${}_{l^n}E(K)$ of x_0 for all l and n (see notation 7.14.10).

(7.18.2) Let $t(l)$ be the largest integer such that

$$x_0 \in l^{t(l)}E(K).$$

Then $t(l) = 0$ for all but finitely many primes l, as x_0 has infinite order. Let n be a positive integer such that

$$n \geq 2t(l) + 1.$$

7.18.3 Lemma. *Put $L = K(E_{l^n})$. Then the restriction map*

$$H^1(K, E_{l^n}(L)) \to H^1(L, E_{l^n}(L))^{\mathrm{Gal}(L/K)}$$

is an isomorphism.

Proof. The Hochschild-Serre spectral sequence,

$$H^p(L/K, H^q(L, E_{l^n}(L))) \Rightarrow H^{p+q}(K, E_{l^n}(L))$$

gives rise to a short exact sequence of low degree terms

$$0 \to H^1(L/K, E_{l^n}(L)) \to H^1(K, E_{l^n}(L)) \to H^1(L, E_{l^n}(L))^{\mathrm{Gal}(L/K)} \to$$

$$\to H^2(L/K, E_{l^n}(L)) \to H^2(K, E_{l^n}(L)).$$

The two cohomology groups $H^1(L/K, E_{l^n}(L))$ and $H^2(L/K, E_{l^n}(L))$ are zero by definition 7.10.3(b); hence this exact sequence shows that restriction map of the lemma is an isomorphism.□

Application of Pontrjagin duality

(7.18.4) As $E_{l^n}(L)$ is a trivial $\mathrm{Gal}(L^{\mathrm{sep}}/L)$-module we obtain an isomorphism obtained from restriction (by lemma 7.18.3)

$$H^1(K, E_{l^n}(L)) \to \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L^{\mathrm{sep}}/L), E_{l^n}(L)), s \mapsto \hat{s},$$

where the action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ is described below.

As $E_{l^n}(L)$ is an abelian group, any homomorphism in $\mathrm{Hom}(\mathrm{Gal}(L^{\mathrm{sep}}/L), E_{l^n}(L))$ factors through $\mathrm{Gal}(L^{\mathrm{ab}}/L)$, where L^{ab} is the maximal abelian extension of L. Hence the restriction map gives an isomorphism

$$H^1(K, E_{l^n}(L)) \to \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L^{\mathrm{ab}}/L), E_{l^n}(L)), s \mapsto \hat{s}.$$

(7.18.5) The action of $\mathrm{Gal}(L/K)$ on the module of abelian group homomorphisms $\mathrm{Hom}(\mathrm{Gal}(L^{\mathrm{ab}}/L), E_{l^n}(L))$ is given explicitly as follows. We have an

exact sequence of profinite groups

$$0 \to \mathrm{Gal}(L^{\mathrm{ab}}/L) \to \mathrm{Gal}(L^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K) \to 0.$$

As $\mathrm{Gal}(L^{\mathrm{ab}}/L)$ is an abelian normal subgroup of $\mathrm{Gal}(L^{\mathrm{ab}}/K)$, we obtain an action of $\mathrm{Gal}(L/K)$ on the right by conjugation on $\mathrm{Gal}(L^{\mathrm{ab}}/L)$; that is to say

$$h^g = \bar{g}^{-1} h \bar{g},\ g \in \mathrm{Gal}(L/K),\ h \in \mathrm{Gal}(L^{\mathrm{ab}}/L)$$

where $\bar{g}$ is any element of $\mathrm{Gal}(L^{\mathrm{ab}}/K)$ lifting g. The action of $g \in \mathrm{Gal}(L/K)$ on a homomorphism s in $\mathrm{Hom}(\mathrm{Gal}(L^{\mathrm{ab}}/L), E_{l^n}(L))$ is given by

$$({}^g s)(h) = g(s(\bar{g}^{-1} h \bar{g})) \quad \text{for all } h \in \mathrm{Gal}(L^{\mathrm{ab}}/L).$$

where $\bar{g} \in \mathrm{Gal}(L^{\mathrm{ab}}/K)$ is any lifting of g (see [HS, Chap. 1, 7]).

(7.18.6) We then obtain a pairing of groups

$$\begin{array}{rccccc} <,>: H^1(K, E_{l^n}(L)) & \times & \mathrm{Gal}(L^{\mathrm{ab}}/L) & \to & E_{l^n}(L) \\ t & \times & h & \mapsto & <t, h> = \hat{t}(h). \end{array}$$

This satisfies, for $g \in \mathrm{Gal}(L/K)$

$$g < t, h > = g(\hat{t}(h)) = g\hat{t}(g^{-1} h^{g^{-1}} g) = \hat{t}(h^{g^{-1}}) = < t, h^{g^{-1}} > .$$

(7.18.7) Let K_L be the closed subgroup of elements $h \in \mathrm{Gal}(L^{\mathrm{ab}}/L)$ such that

$$< t, h > = 0 \quad \text{for all } t \in H^1(K, E_{l^n}(L)).$$

That is to say, K_L is the intersection of the kernels of all homomorphisms $< t, - >$. Then $G_L = \mathrm{Gal}(L^{\mathrm{ab}}/L)/K_L$ is the abelian galois group of an extension field $\tilde{L}/L$. Furthermore, G_L is a $\mathbb{Z}[\mathrm{Gal}(L/K)]$-module.

7.18.8. Proposition. *The pairing*

$$H^1(K, E_{l^n}(L)) \times G_L \to E_{l^n}(L)$$

is perfect, that is to say the natural homomorphism

$$\omega : H^1(K, E_{l^n}(L)) \to \mathrm{Hom}_{\mathrm{Gal}(L/K)}(G_L, E_{l^n}(L)).$$

is an isomorphism of discrete torsion groups and the natural homomorphism

$$\omega' : G_L \to \mathrm{Hom}(H^1(K, E_{l^n}(L)), E_{l^n}(L)).$$

is an isomorphism of profinite groups.

Proof. The abelian groups $H^1(K, E_{l^n}(L))$ and G_L are both annihilated by l^n. The group $H^1(K, E_{l^n}(L))$ is a discrete torsion group and G_L is a profinite group.

Recall from definition 7.10.3(a) and 7.10.3(c) that the prime number l is chosen so that $l \neq 2$ and we have a commutative diagram of finite groups with exact rows

$$\begin{array}{ccccccccc} & & & & \mathrm{Gal}(L/K) & & & & \\ & & & & \downarrow\cong & & & & \\ 0 & \to & \mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z}) & \to & \mathrm{Gal}(F(E_{l^n})/F) & \to & H_{l^n} & \to & 0 \\ & & \downarrow= & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z}) & \to & \mathrm{GL}(2,\mathbb{Z}/l^n\mathbb{Z}) & \underset{\det}{\to} & (\mathbb{Z}/l^n\mathbb{Z})^* & \to & 0 \end{array}$$

where H_{l^n} is the subgroup of $(\mathbb{Z}/l^n\mathbb{Z})^*$ generated by the powers of q modulo l^n. The isomorphism

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(F(E_{l^n})/F)$$

at the top of this diagram is obtained by restriction to the subfield $F(E_{l^n})$ of L; that this restriction is an isomorphism holds because K and $F(E_{l^n})$ are linearly disjoint over F (by definition 7.10.3(e)) and hence $K \cap F(E_{l^n}) = F$.

We now calculate the group

$$\mathrm{Hom}_{\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})}(E_l, E_l)$$

where we have the standard action of $\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})$.

The module E_l is a simple $\mathbb{Z}[\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})]$-module. Let $s \in \mathrm{Hom}_{\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})}(E_l, E_l)$. Then either $s : E_l \to E_l$ is surjective or s is equal to 0. Suppose then that s is surjective. As E_l has only finitely many elements, the map $s : E_l \to E_l$ must then be an isomorphism. Hence s is given by a matrix in $\mathrm{GL}(2,\mathbb{Z}/l\mathbb{Z})$ which commutes with $\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})$; hence s is a homothety. That is so say, there is an isomorphism of rings

$$\mathrm{Hom}_{\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})}(E_l, E_l) \cong \mathbb{Z}/l\mathbb{Z}.$$

As $\mathrm{SL}(2,\mathbb{Z}/l^n\mathbb{Z})$ is a subgroup of $\mathrm{Gal}(L/K)$, we obtain an isomorphism of rings

$$\mathrm{Hom}_{\mathrm{Gal}(L/K)}(E_l, E_l) \cong \mathbb{Z}/l\mathbb{Z}.$$

The conditions of theorem 7.17.11 are then fulfilled for the discrete torsion group $H^1(K, E_{l^n}(L))$ and the finite group $\mathrm{Gal}(L/K)$ acting on E_{l^n}. We obtain from this theorem the equality

$$H^\diamond = \mathrm{Hom}_{\mathrm{cts}}(H^1(K, E_{l^n}(L)), E_{l^n}(L)))$$

and the isomorphism

$$\mathrm{Hom}_{\mathrm{Gal}(L/K)}(H^\diamond, E_{l^n}(L)) \cong H^1(K, E_{l^n}(L)).$$

By (7.18.4), we obtain an isomorphism obtained from restriction

$$H^1(K, E_{l^n}(L)) \overset{\cong}{\to} \mathrm{Hom}_{\mathrm{Gal}(L/K)}(G_L, E_{l^n}(L)), s \mapsto \hat{s}.$$

The group G_L is a $\mathbb{Z}[\mathrm{Gal}(L/K)]$-submodule of $\mathrm{Hom}_{\mathrm{cts}}(H^1(K, E_{l^n}(L)), E_{l^n}(L))$; that is to say we have an inclusion of $\mathbb{Z}[\mathrm{Gal}(L/K)]$-modules

$$G_L \subseteq H^\diamond.$$

Let

$$A \subseteq \mathrm{Hom}_{\mathrm{Gal}(L/K)}(H^\diamond, E_{l^n}(L))$$

be the annihilator of G_L; that is to say

$$A = \{h \in \mathrm{Hom}_{\mathrm{Gal}(L/K)}(H^\diamond, E_{l^n}(L)) \mid \ h(g) = 0 \ \text{ for all } g \in G_L\}.$$

As we have

$$\mathrm{Hom}_{\mathrm{Gal}(L/K)}(H^\diamond, E_{l^n}(L)) \cong H^1(K, E_{l^n}(L))$$

we obtain $A = 0$. By proposition 7.17.7(ii), we obtain

$$\mathrm{Hom}_{\mathrm{Gal}(L/K)}(H^\diamond/G_L, E_{l^n}(L)) \cong A = 0.$$

The module E_l is a simple $\mathbb{Z}[\mathrm{Gal}(L/K)]$-module and E_{l^n} has a composition series whose composition factors are all isomorphic to E_l. We have

$$H^\diamond = \mathrm{Hom}_{\mathrm{cts}}(H^1(K, E_{l^n}(L)), E_{l^n}(L))$$

where $H^\diamond$ is a profinite group annihilated by l^n; it follows that every composition factor of every finitely generated $\mathbb{Z}[\mathrm{Gal}(L/K)]$-submodule of $H^\diamond$ is isomorphic to E_l. As $A = 0$, it follows that $H^\diamond/G_L = 0$ and hence $G_L = H^\diamond$. □

(7.18.9) Let S be a finite subgroup of $H^1(K, E_{l^n}(L))$. Let G_S be the open and closed subgroup of elements g of $\mathrm{Gal}(L^{\mathrm{ab}}/L)$ for which $< s, g >= 0$ for all $s \in S$. Let L_S be the finite galois extension field of L which is the fixed field of G_S. Then the pairing $<,>$ induces a pairing

$$S \times \mathrm{Gal}(L_S/L) \to E_{l^n}(L), \ s, g \mapsto < s, g > .$$

7.18.10. Corollary. *The pairing*

$$S \times \mathrm{Gal}(L_S/L) \to E_{l^n}(L),\ \ s, g \mapsto < s, g >$$

is non-degenerate that is to say it induces an isomorphism of $\mathbb{Z}[\mathrm{Gal}(L/K)]$*-modules*

$$\mathrm{Gal}(L_S/L) \cong \mathrm{Hom}(S, E_{l^n}(L))$$

and an isomorphism of abelian groups (if S *is a* $\mathbb{Z}[\mathrm{Gal}(K/F)]$*-module then an isomorphism of* $\mathbb{Z}[\mathrm{Gal}(K/F)]$*-modules)*

$$S \cong \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L_S/L), E_{l^n}(L)).$$

Proof. This follows from proposition 7.18.8, proposition 7.17.9, and theorem 7.17.11.□

The cocycles $\gamma_i(0)$

(7.18.11) Let $\mathbb{N}^{(p)}$ be the set of positive integers prime to p, where p is the characteristic of the global field F.

(7.18.12) For a place v of the field K, we write K_v for the completion of K at the place v. We have a commutative diagram of groups for all $n \in \mathbb{N}^{(p)}$, where the maps res_v are the restriction homomorphisms and the rows are exact sequences

$$\begin{array}{ccccccccc} 0 & \to & {}_nE(K) & \to & H^1(K, E(K^{\mathrm{sep}})_n) & \to & H^1(K, E(K^{\mathrm{sep}}))_n & \to & 0 \\ & & \downarrow & & \downarrow \mathrm{res}_v & & \downarrow \mathrm{res}_v & & \\ 0 & \to & {}_nE(K_v) & \to & H^1(K_v, E(K_v^{\mathrm{sep}})_n) & \to & H^1(K_v, E(K_v^{\mathrm{sep}}))_n & \to & 0 \end{array}$$

For any integer n prime to p, the Selmer group of $E \times_F K/K$ is defined as

$$S^{(n)}(E/K) = \bigcap_{v \in \Sigma_K} \mathrm{res}_v^{-1}({}_nE(K_v)).$$

Then $S^{(n)}(E/K)$ is a finite subgroup of $H^1(K, E_n(L))$.

(7.18.13) Let $\frac{x_0}{l^n} \in E(K^{\mathrm{sep}})$ be a fixed l^nth division point of x_0, that is to say $\frac{x_0}{l^n}$ is any point which satisfies $l^n(\frac{x_0}{l^n}) = x_0$. We have $x_0 \in E(K)$ and by

definition $\gamma(0) = \partial P_0$. The cocycle

$$\gamma(0) : g \mapsto g\big(\frac{x_0}{l^n}\big) - \frac{x_0}{l^n},\ \mathrm{Gal}(K^{\mathrm{sep}}/K) \to E_{l^n}(K^{\mathrm{sep}}),$$

represents a cohomology class in $H^1(K, E_{l^n}(K^{\mathrm{sep}}))$ which is the image of $P_0 \in {}_{l^n}E(K)$ under the homomorphism

$$\partial : {}_{l^n}E(K) \to H^1(K, E_{l^n}(K^{\mathrm{sep}}))$$

(see the diagram (7.14.5)).

We obtain that $\gamma(0)$ is an element of the Selmer group

$$\gamma(0) \in S^{(l^n)}(E/K).$$

The restriction of this cocycle $\gamma(0)$ to $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ is a group homomorphism

$$\gamma(0)|_L : \mathrm{Gal}(L^{\mathrm{sep}}/L) \to E_{l^n}(L),\ g \mapsto g\big(\frac{x_0}{l^n}\big) - \frac{x_0}{l^n}.$$

The kernel of this homomorphism $\gamma(0)|_L$ is the subgroup of elements which fix $\frac{x_0}{l^n}$, that is to say the fixed field of $\ker(\gamma(0)|_L)$ is precisely the field

$$L_n = L\big(\frac{1}{l^n}x_0\big).$$

which is an abelian galois extension of L.

(7.18.14) For any integer i such that $0 \le i \le n$ put

$$L_i = L\big(\frac{1}{l^i}x_0\big).$$

The element x_0 induces cocycles $\gamma_i(0) \in H^1(K, E_{l^i})$ represented by

$$g \mapsto g\big(\frac{x_0}{l^i}\big) - \frac{x_0}{l^i},\quad g \in \mathrm{Gal}(K^{\mathrm{sep}}/K).$$

The cocycle $\gamma_i(0)$ is equal to $l^{n-i}\gamma(0)$.

7.18.15 Proposition. (i) *The cocycle $\gamma_i(0)$ is zero in $H^1(K, E_{l^i})$ if and only if $x_0 \in l^i E(K)$.*
(ii) *We have $L_i = L$ if and only if $x_0 \in l^i E(K)$; in particular, we have $L_{t(l)+1} \neq L$.*

Proof. (i) The cocycle $\gamma_i(0)$ is zero in $H^1(K, E_{l^i})$ if and only if it is of the form $(g-1)Q$ where $Q \in E_{l^i}$ that is to say if and only if

$$g(\frac{x_0}{l^i} - Q) = \frac{x_0}{l^i} - Q \text{ for all } g \in \mathrm{Gal}(K^{\mathrm{sep}}/K).$$

This happens if and only if $\frac{x_0}{l^i} - Q$ is an element of $E(K)$; as $l^i Q = 0$, this is to say $\gamma_i(0) = 0$ if and only if $x_0 \in l^i E(K)$.
(ii) Letting S be the subgroup generated by $l^{n-i}\gamma(0)$ in the corollary 7.18.10, we obtain an isomorphism

$$\mathrm{Gal}(L_S/L) \cong \mathrm{Hom}(S, E_{l^n}(L)).$$

The field L_S is equal to L_i for the same reason that the fixed field of $\ker(\gamma(0)|_L)$ is equal to L_n; hence $L_i = L$ if and only if $S = 0$. That is to say, we have $L_i = L$ if and only if $x_0 \in l^i E(K)$; in particular by (7.18.2) we have $L_{t(l)+1} \neq L$. □

(7.18.16) By the isomorphism of lemma 7.18.3

$$H^1(K, E_{l^n}(L)) \cong \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L^{\mathrm{sep}}/L), E_{l^n}(L))$$

there is a smallest finite abelian extension field M of L, Galois over F and of order a power of l, through which all elements of the finite group $S^{(l^n)}(E/K)$ factor. By corollary 7.18.10, we have

$$S^{(l^n)}(E/K) = H^1(\mathrm{Gal}(M/L), E_{l^n}(L))^{\mathrm{Gal}(L/K)}.$$

and we have

$$\mathrm{Gal}(M/L) \cong \mathrm{Hom}(S^{(l^n)}(E/K), E_{l^n}(L)).$$

(7.18.17) We have the inclusions, where $L \neq L_{t(l)+1}$ by proposition 7.18.15,

$$L = L_0 = L_1 = \ldots = L_{t(l)} \subset L_{t(l)+1} \subset \ldots \subset L_n \subset M. \tag{7.18.18}$$

Let $I_i = \mathrm{Gal}(M/L_i)$ and $H = \mathrm{Gal}(M/L)$. Then I_i is a nested sequence of subgroups of H

$$H = I_0 = I_1 = \ldots = I_{t(l)} \supset I_{t(l)+1} \supset \ldots \supset I_n \supset \{1\}.$$

We have a diagram of fields

$$\begin{array}{ccc} & & M \\ & {\scriptstyle I_i}\nearrow & \\ L_i & & \uparrow {\scriptstyle H} \\ & \nwarrow & \\ & & L = K(E_{l^n}) \\ & & \uparrow \\ & & K \\ & & \uparrow \\ & & F \end{array} \tag{7.18.19}$$

Let $\tau_\infty \in \mathrm{Gal}(L/F)$ be as in (7.11.1). Then τ_∞ has order 2. Let $\tau' \in \mathrm{Gal}(M/F)$ be a lifting of τ_∞. As M/L is a galois extension of order

a power of l where $l \neq 2$ (by (7.18.1)) we may assume that τ' has order 2. Then we have

$$\tau'^2 = 1. \tag{7.18.20}$$

The element τ_∞ acts on H by conjugation by τ': this action is independent of the choice of lifting τ'. As $l > 2$, the group H, and its subgroups, decompose into a sum of eigenspaces under the action of the involution τ_∞: namely

$$H = H^+ \oplus H^-. \tag{7.18.21}$$

Lemma 7.18.22. *Let $h \in H$ and let z be a closed point of* Spec A *prime to the conductor I and the discriminant of K/F such that* $\mathrm{Frob}_z(M/F) = [\tau' h]$ *where $[g]$ denotes the conjugacy class of an element g. Then z remains inert in K; let $z^\sharp$ be the unique place of K lying above z. We have*
(i) *$z^\sharp$ splits completely in L/K and $z \in \mathcal{D}_{l^n}$;*
(ii) *$h^{1+\tau_\infty} \in I_i^+$ if and only if $x_0 \in l^i E(K_{z^\sharp})$;*
(iii) *$h^{1+\tau_\infty} \notin I_i^+$ if and only if $\mathrm{res}_{z^\sharp}\delta(z)$ (notation 7.14.13) has order at least l^{n-i+1}, provided that l is prime to $|\mathrm{Pic}(B)|$.*

Proof of lemma 7.18.22. (i) We have $\mathrm{Frob}_z(L/F) = \mathrm{Frob}_z(M/F)|_L = [\tau' h]|_L = \tau_\infty$. Hence we have $\mathrm{Frob}_{z^\sharp}(L/K) = [\tau_\infty^2] = [1]$. This shows that $z^\sharp$ splits competely in L/K and that $z \in \mathcal{D}_{l^n}$ by definition 7.11.3(ii).
(ii) We have $x_0 \in l^i E(K_{z^\sharp})$ if and only if $\mathrm{Frob}_{z^\times}(L_i/L) = [1]$ where $z^\times$ is any place of L over $z^\sharp$. But, by part (i), we have $\mathrm{Frob}_{z^\times}(L_i/L) = (\tau' h)^2|_{L_i}$, the restriction to L_i of $(\tau' h)^2$. Hence we have $x_0 \in l^i E(K_{z^\sharp})$ if and only if $(\tau' h)^2 \in I_i$ which is the case if and only if

$$\tau' h \tau'^{-1} h \in I_i$$

as τ' has order 2 by (7.18.20). As H is abelian, we have $\tau' h \tau'^{-1} h \in I_i$ if and only if (by (7.18.21))

$$h^{1+\tau_\infty} = h^{\tau_\infty} h = \tau' h \tau'^{-1} h \in I_i^+ = I_i \cap H^+.$$

(iii) By lemma 7.14.14(ii), the order of $\mathrm{res}_{z^\sharp} P_0$ in ${}_{l^n}E(K_{z^\sharp})$ is equal to the order of $\mathrm{res}_{z^\sharp}\delta(z)$ as the order of $z^\sharp$ in $\mathrm{Pic}(B)$ is prime to l by hypothesis. As $z^\sharp$ splits completely in L/K by (i), it follows that

$$E(K_{z^\sharp})_{l^n} \cong (\mathbb{Z}/l^n\mathbb{Z})^2.$$

Therefore the exponent u of the order l^u of $\mathrm{res}_{z^\sharp} P_0$ is the least integer u such that

$$x_0 \in l^{n-u} E(K_{z^\sharp}).$$

Now for any integer u we have $x_0 \in l^{n-u} E(K_{z^\sharp})$ if and only if $h^{1+\tau_\infty} \in I_{n-u}^+$ by part (ii) above.□

7.18.23. Lemma. *The field extension M/K is unramified at all primes of K not dividing I and ∞.*

Proof. Let S be a finite set of primes of K containing the primes at which E has bad reduction; that is to say, S is a set of primes of K containing all the primes dividing the conductor I of E/F and the prime ∞. Let K_S be the maximal subfield of K^{sep} containing K which is ramified only at the primes in S. Let G_S be the galois group $\mathrm{Gal}(K_S/K)$. Write $E(m)$ for the m-primary component of E that is $E(m) = \bigcup_{r\geq 1} E_{m^r}$. If m is prime to the characteristic p of F, by [M, Chap. 1, Prop. 6.5] we have an exact sequence

$$0 \to H^1(G_S, E(m)) \to H^1(K, E(m)) \to \prod_{v\notin S} H^1(K_v, E).$$

Furthermore, by the definition of the field M and (7.18.16) we have the inclusions for any n prime to p

$$S^{(n)}(E/K) = H^1(M/L, E_n(L))^{\mathrm{Gal}(L/K)} \subseteq H^1(L, E_n(L))^{\mathrm{Gal}(L/K)}.$$

It follows from this previous exact sequence and that

$$S^{(n)}(E/K) = \bigcap_{v\in\Sigma_K} \mathrm{res}_v^{-1}({}_nE(K_v))$$

that any prime of K not dividing I and ∞ is unramified in M/K. □

7.18.24. Lemma. *We have an isomorphism of groups, for $\delta = \pm$,*

$$H^\delta / I^\delta_{t(l)+1} \cong \mathbb{Z}/l\mathbb{Z}.$$

Proof. By definition of $t(l)$ (see (7.18.2)), we have

$$x_0 = l^{t(l)}y \quad \text{where} \quad y \in E(K) \setminus lE(K).$$

We then have isomorphisms of τ_∞-modules

$$H/I_{t(l)+1} \cong \mathrm{Gal}(L(\frac{1}{l}y)/L) \cong E_l(L).$$

As $H/I_{t(l)+1}$ is a group of order l^2 where $l > 2$ it follows that

$$H^\delta/I^\delta_{t(l)+1} \cong (H/I_{t(l)+1})^\delta \cong E_l(L)^\delta.$$

As $l \in \mathcal{P}$ we may select a prime divisor $z \in \mathcal{D}_{l^n}$. Then z remains inert in K/F (definition 7.11.3); let $z^\sharp$ denote the place of K lying over F. Let $\mathcal{E}_{0,z}$

denote the reduction modulo z of the Néron model of E/F. The reduction homomorphism

$$E(L)_l \to \mathcal{E}_{0,z}(\kappa(z^\sharp))_l$$

is then an isomorphism. By lemma 7.11.5, we obtain

$$E(L)^\delta_l \xrightarrow{\cong} \mathcal{E}_{0,z}(\kappa(z^\sharp))^\delta_l \cong \mathbb{Z}/l\mathbb{Z}$$

whence the result holds.□

Finiteness of $Ш(E/K)^\epsilon_{l^\infty}$

(7.18.25) Let $h \in H$ be such that

$$h^{1+\tau_\infty} \notin I^+_{t(l)+1}.$$

This choice is possible because $I^+_{t(l)+1} \neq H^+$ by lemma 7.18.24. By Čebotarev's density theorem, we may select a closed point z of Spec A, unramified in M/F, such that

$$\mathrm{Frob}_z(M/F) = [\tau' h].$$

7.18.26. Lemma. *If l is prime to $|\mathrm{Pic}(B)|$, we have*

$$l^{t(l)}\mathrm{res}_{z^\sharp}(S^{(l^n)}(E/K)^\epsilon) = 0.$$

Proof. We have $z \in \mathcal{D}_{l^n}$ by lemmas 7.18.22 and 7.18.23. Again by lemma 7.18.22, z remains inert in K and the place $z^\sharp$ lying over z splits completely in L/K.

Let $\delta(z) \in H^1(K,E)^\epsilon_{l^n}$ be the class given by notation 7.14.10 and lemma 7.14.11. By lemma 7.14.14(i), $\delta(z)$ is locally trivial at all places of K except possibly at $z^\sharp$. By lemma 7.18.22(iii) we then have the order of $\mathrm{res}_{z^\sharp}\delta(z)$ is at least $l^{n-t(l)}$.

Let $s \in S^{(l^n)}(E/K)^\epsilon$. By proposition 7.16.3 we have

$$l^{t(l)}\mathrm{res}_{z^\sharp} s = 0. \tag{7.18.27}$$

as required.□

7.18.28. Proposition. *If l is prime to $|\mathrm{Pic}(B)|$, we have*

$$l^{t(l)} S^{(l^n)}(E/K)^\epsilon = 0.$$

Proof. Let $s \in S^{(l^n)}(E/K)^\epsilon$. Let z be as in (7.18.25). The place $z^\sharp$ of K lying over z splits completely in L/K. Let $z^\times$ be a place of L lying over $z^\sharp$. As z is unramified in M/F any place above z in L is unramified in M/L. Hence the frobenius element $\mathrm{Frob}_{z^\times}(M/L)$ is well defined and we have

$$\mathrm{res}_{z^\sharp}(s) = \hat{s}(\mathrm{Frob}_{z^\times}(M/L)).$$

where $\hat{s}$ is the image of s under the isomorphism (see (7.18.4))

$$H^1(K, E_{l^n}(L)) \to \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L^{\mathrm{ab}}/L), E_{l^n}(L)), s \mapsto \hat{s}.$$

By definition $\mathrm{res}_{z^\sharp}(s)$ is the restriction to $\mathrm{Gal}(K_{z^\sharp}^{\mathrm{sep}}/K_{z^\sharp})$ of the cocycle s. As s is trivialised over M, an extension of L unramified at z, we have that the restriction of s lies in $H^1(K_{z^\sharp}^{\mathrm{un}}/K_{z^\sharp}, E_{l^n})$ where $K_{z^\sharp}^{\mathrm{un}}$ is the maximal unramified extension of $K_{z^\sharp}$. This holds because

$$0 \to H^1(K_{z^\sharp}^{\mathrm{un}}/K_{z^\sharp}, E_{l^n}) \to H^1(K, E_{l^n}) \to H^1(K_{z^\sharp}, E)$$

is exact (from [M, Chap. I, Prop.6.5]). But the group $\mathrm{Gal}(K_{z^\sharp}^{\mathrm{un}}/K_{z^\sharp})$ is generated topologically by the Frobenius element at $z^\sharp$. We have

$$\mathrm{Frob}_z(L/F) = [\tau_\infty]$$

and

$$\mathrm{Frob}_{z^\times}(M/L) = [(\tau' h)^2].$$

Hence by lemma 7.18.26 we have

$$l^{t(l)}\hat{s}((\tau' h)^2) = 0.$$

Hence we have (as τ' has order 2 by (7.18.20))

$$l^{t(l)}\hat{s}(\tau' h \tau'^{-1} h) = 0.$$

Whence we have, as $\hat{s}$ is a homomorphism $H = \mathrm{Gal}(M/L) \to E_{l^n}$,

$$l^{t(l)}\hat{s}(h^{\tau'}) + l^{t(l)}\hat{s}(h) = 0.$$

As s is in the ϵ eigenspace under the action of τ_∞, this equation becomes

$$l^{t(l)}(\epsilon\tau_\infty)\hat{s}(h) + l^{t(l)}\hat{s}(h) = l^{t(l)}(1 + \epsilon\tau_\infty)\hat{s}(h) = 0.$$

We have therefore shown that for every $g \in H$ such that

$$g^{1+\tau_\infty} \notin I^+_{t(l)+1}$$

then

$$l^{t(l)}(1 + \epsilon\tau_\infty)\hat{s}(g) = 0. \tag{7.18.29}$$

Let

$$\alpha = l^{t(l)}(1 + \epsilon\tau_\infty)\hat{s}.$$

Then α is a homomorphism $H \to E_{l^n}$ which is zero on $H \setminus (H^- \oplus I^+_{t(l)+1})$. As $H^- \oplus I^+_{t(l)+1}$ is a proper subgroup of H (lemma 7.18.24), the map α must be the zero homomorphism on H. It follows that we have from (7.18.29)

$$l^{t(l)}\hat{s}(H) \subset E^{-\epsilon}_{l^n}. \tag{7.18.30}$$

That is to say, the image of H under $l^{t(l)}\hat{s}$ is cyclic and defined over K and hence is contained in a Borel subgroup rational over K. But $\mathrm{Gal}(L/K)$ is not contained in a Borel subgroup of $\mathrm{GL}(2, E_{l^n})$ by definition 7.10.3(c) and 7.10.3(e). Hence we must have

$$l^{t(l)}\hat{s}(H) = 0.$$

Therefore we have

$$l^{t(l)} S^{(l^n)}(E/K)^\epsilon = 0.$$

as required.□

7.18.31. Corollary. *If l is prime to $|\mathrm{Pic}(B)|$, we have*

$$l^{t(l)}Ш(E/K)^\epsilon_{l^\infty} = 0$$

and

$$(E(K)/E(K)_{2-\mathrm{torsion}})^\epsilon \quad \textit{is finite.}$$

Proof. We have the exact sequence (see (7.9.3))

$$0 \to ({}_{l^n}E(K))^\epsilon \to S^{(l^n)}(E/K)^\epsilon \to Ш(E/F)^\epsilon_{l^n} \to 0.$$

By taking arbitrarily large values of n we obtain from proposition 7.18.28 and this exact sequence that

$$l^{t(l)}Ш(E/K)^\epsilon_{l^\infty} = 0.$$

Furthermore we have that

$$l^{t(l)}\left[({}_{l^n}E(K))^\epsilon\right] = 0.$$

Taking again n to be arbitrarly large we obtain that, as the group $E(K)$ is finitely generated by the Mordell-Weil theorem,

$$(E(K)/E(K)_{2-\mathrm{torsion}})^\epsilon \text{ is finite}$$

as required.□

Finiteness of $Ш(E/K)^{-\epsilon}_{l^\infty}$

(7.18.32) As in (7.18.2), let n be an integer satisfying $n \geq 2t(l) + 1$. As in (7.18.25), let $h \in H$ be such that

$$h^{1+\tau_\infty} \notin I^+_{t(l)+1}$$

and let z be a closed point of Spec A, unramified in M/F, such that

$$\mathrm{Frob}_z(M/F) = [\tau' h].$$

7.18.33. Lemma. *Let $m \geq 0$ be an integer. Suppose that l is prime to $|\mathrm{Pic}(B)|$. We have that these are equivalent:*

(a) $l^m \gamma(z) \in S^{(l^n)}(E/K)$;
(b) $\mathrm{res}_{z^\sharp}(l^m \delta(z)) = 0$;
(c) $l^m x_0 \in l^n E(K_{z^\sharp})$;
(d) $h^{1+\tau_\infty} \in I^+_{n-m}$;
(e) $l^m \delta(z) \in Ш(E/F)_{l^n}$.

Proof. We have the commutative diagram of torsion abelian groups with exact rows and an exact right-hand column

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \to & {}_*E(K) & \to & S^{(*)}(E/K) & \to & Ш(E/F)_* & \to & 0 \\
 & & =\downarrow & & \downarrow & & \downarrow & & \\
0 & \to & {}_*E(K) & \to & H^1(K, E_*) & \to & H^1(K, E)_* & \to & 0 \\
 & & \downarrow & & \downarrow \mathrm{res}_v & & \downarrow \mathrm{res}_v & & \\
0 & \to & \prod_v {}_*E(K_v) & \to & \prod_v H^1(K_v, E_*) & \to & \prod_v H^1(K_v, E)_* & \to & 0
\end{array}$$

(a) ⇒ (b) follows from this diagram as $l^m \gamma(z) \in S^{(l^n)}(E/K)$ implies that $l^m \delta(z) \in Ш(E/F)_{l^n}$ and hence that $\mathrm{res}_w(l^m \delta(z)) = 0$ for all places w (lemma 7.14.14(i)).
(b) ⇒ (c) follows from lemma 7.14.14(ii) (or lemma 7.18.22(ii) and (iii)).
(c) ⇔ (d). From lemma 7.11.5(ii) it follows that

$$E(K_{z^\sharp})_{l^n} \cong (\mathbb{Z}/l^n\mathbb{Z})^2.$$

Hence the implications (c) ⇔ (d) follow from lemma 7.18.22(ii).
(d) ⇒ (e) by lemma 7.18.22 and as $\delta(z)$ is locally trivial at all places different from z.

(e) $\Leftrightarrow$ (a) from the above diagram as $\delta(z)$ is the image of $\gamma(z)$ under the homomorphism

$$H^1(K, E_{l^n}) \to H^1(K, E)_{l^n}. \quad \square$$

7.18.34. Remarks. (i) We have $z \in \mathcal{D}_{l^n}$; this holds because for any z with $\mathrm{Frob}_z(M/F) = [\tau' h]$ we have $\mathrm{Frob}_z(L/F)$ is the restriction to L of the conjugacy class $[\tau' h]$ but this restriction is equal to $[\tau_\infty]$ (see (7.11.1)). Furthermore, again by lemma 7.18.22, z remains inert in K and the place $z^\sharp$ lying over z splits completely in L/K.
(ii) Suppose that l is prime to $|\mathrm{Pic}(B)|$. By lemma 7.18.22(ii) and (iii), the element

$$\delta(z) \in H^1(K, E_{l^n})^\epsilon$$

satisfies that the order of $\mathrm{res}_{z^\sharp}\delta(z)$ is precisely equal to $l^{n-t(l)}$.

It follows that, by lemma 7.18.33 above, that $l^{n-t(l)}\gamma(z) \in S^{(l^n)}(E/K)^\epsilon$ and that $l^{n-t(l)-1}\gamma(z) \notin S^{(l^n)}(E/K)$. It also implies that the order of $\mathrm{res}_{z^\sharp}\gamma(z)$ is at least $l^{n-t(l)}$.

(7.18.35) Suppose that l is prime to $|\mathrm{Pic}(B)|$. Denote by $\hat{\gamma}$ the image of $\gamma(z)$ under the isomorphism (see lemma 7.18.3)

$$H^1(K, E_{l^n}) \cong \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L^{\mathrm{sep}}/L), E_{l^n}).$$

There is smallest finite abelian extension field L' of L through which $l^{n-t(l)-1}\hat{\gamma}$ factors; that is to say we have a commutative diagram of groups

$$\begin{array}{ccccc} & & l^{n-t(l)-1}\hat{\gamma} & & \\ \mathrm{Gal}(L^{\mathrm{sep}}/L) & & \to & & E_{l^n} \\ & \searrow & & & \nearrow g \\ & & \mathrm{Gal}(L'/L) & & \end{array}$$

where the homomorphism g is injective. Let L'' be the smallest extension field of L through which $l^{n-t(l)}\hat{\gamma}$ factors. Then $l^{n-t(l)}\gamma(z) \in S^{(l^n)}(E/K)$ (remarks 7.18.34(ii)) and we have a diagram of fields

$$\begin{array}{ccccc} L' & & & & M \\ & \nwarrow & & \nearrow & \uparrow \\ & & L'' & & L_n \\ & & \uparrow & \nearrow & \\ & & L & & \end{array}$$

Furthermore we have isomorphisms of $\mathrm{Gal}(L/K)$-modules

$$\mathrm{Gal}(L'/L'') \cong E_l$$

$$\mathrm{Gal}(L''/L) \cong E_{l^r}$$

where l^r is the order of $l^{n-t(l)}\gamma(z)$.

7.18.36. Lemma. *Suppose that l is prime to $|\mathrm{Pic}(B)|$. Let $w \in \mathcal{D}_{l^n}$, where $w \neq z$, and let $w^\sharp$ be the unique place of K above w. The following statements are equivalent:*
(a) $\mathrm{Frob}_{w^\sharp}(L'/L) = 1$;
(b) *the primes over w split completely in L'/L;*
(c) $l^{n-t(l)-1}\hat{\gamma}(\mathrm{Frob}_{w^\sharp}(L'/L)) = 0$;
(d) $\mathrm{res}_{w^\sharp} l^{n-t(l)-1}\hat{\gamma} = 0$;
(e) $\mathrm{res}_{w^\sharp} l^{n-t(l)-1} P_z = 0$.

Proof. The place $w^\sharp$ is unramified and splits completely in L/K by definition 7.11.3; we denote by the same symbol $w^\sharp$ any place of L lying over the place $w^\sharp$ of K. The equivalences of (a), (b) are evident.

The implication (b)⇒(c) is evident. That (c)⇒(b) follows from the fact (see (7.18.35)) that the homomorphism

$$g : \mathrm{Gal}(L'/L) \to E_{l^n}$$

representing $l^{n-t(l)-1}\gamma$ is injective and hence

$$l^{n-t(l)-1}\hat{\gamma}(\mathrm{Frob}_{w^\sharp}(L'/L) = g(\mathrm{Frob}_{w^\sharp}(L'/L)) = 0 \Leftrightarrow \mathrm{Frob}_{w^\sharp}(L'/L) = 1.$$

To show the equivalence of (c) and (d), by the diagram 7.14.5 we have the exact sequences

$$\begin{array}{ccccccccc}
0 \to & & {}_mE(K) & \to & H^1(K, E_m) & \to & H^1(K, E)_m & \to & 0 \\
 & & \downarrow & & \mathrm{res}\downarrow \ \mathrm{quasi-isom.} & & \mathrm{res}\downarrow & & \\
0 \to & ({}_mE(K[c]))^{\mathcal{G}_c} & \xrightarrow{\partial} & H^1(K[c], E_m)^{\mathcal{G}_c} & \to & H^1(K[c], E)^{\mathcal{G}_c}_m & & &
\end{array}$$

As $w \neq z$, we have $\mathrm{res}_{w^\sharp}\delta(z) = 0$; hence we have that $\mathrm{res}_{w^\sharp}\gamma(z) \in {}_{l^n}E(K_{w^\sharp})$ (see §7.9). That is to say $\mathrm{res}_{w^\sharp}\gamma(z)$ is in the image of the homomorphism

$${}_{l^n}E(K_{w^\sharp}) \to H^1(K_{w^\sharp}, E_m)$$

and we have

$$\gamma(z)(g) = g(\frac{P}{l^n}) - \frac{P}{l^n}$$

for some $P \in E(K_{w^\sharp})$. As $\gamma(z) \in H^1(L'/L, E_{l^n})$ the restriction of $\gamma(z)$ to $K_{w^\sharp}$ is then an element of $H^1(L'_{w^\times}/L_{w^\sharp}, E_m)$ where $w^\times$ is a place of L' over $w^\sharp$. As $\mathrm{Gal}(L'_{w^\times}/L_{w^\sharp})$ is cyclic and generated by the Frobenius element $\mathrm{Frob}_{w^\sharp}(L'/L)$ we obtain that $\mathrm{res}_{w^\sharp} l^{n-t(l)-1}\gamma(z) = 0$ if and only if $l^{n-t(l)-1}\hat{\gamma}(\mathrm{Frob}_{w^\sharp}(L'/L)) = 0$. The equivalence of (c) and (d) follows from this. That (d) and (e) are equivalent follows from remark 7.14.12(ii). □

(7.18.37) Let $\tau' \in \mathrm{Gal}(M/F)$ be as in (7.18.20), that is to say it is a lifting of τ_∞. We may then select a lifting $\tau'' \in \mathrm{Gal}(L'/F)$ of τ_∞ such that τ'' has

order 2 and that $\tau'|_{L''} = \tau''|_{L''}$. That such an element τ'' of order 2 exists is a consequence of the group $\mathrm{Gal}(L'/K)$ having odd order namely a power of l.

7.18.38. Lemma. *Suppose that l is prime to $|\mathrm{Pic}(A)|$. For any element $i \in H$ such that $i^{1+\tau_\infty} \in I_n^+$ there is a prime divisor $w \in \mathcal{D}_{l^n}$, $w \neq z$, of* Spec A, *and with lifting $w^\sharp$ to K, satisfying the four conditions*

(a) $\mathrm{Frob}_w(M/F) = [\tau' i]$ *where* $i^{1+\tau_\infty} \in I_n^+$;
(b) $\mathrm{Frob}_w(L'/F) = [\tau'' j]$ *where* $j \in \mathrm{Gal}(L'/L)$ *satisfies* $j^{1+\tau_\infty} \neq 1$;
(c) $\mathrm{Frob}_{w^\sharp}(K[z]/K)$ *has order prime to* l;
(d) $\mathrm{Frob}_{z^\sharp}(K[w]/K)$ *has order prime to* l.

Proof. The two conditions (a) and (b) on w are simultaneously satisfiable provided that

$$i|_{L''} = j|_{L''}$$

as we have $L' \cap M = L''$; for then the restrictions to L'' of the Frobenius elements $\mathrm{Frob}_w(M/F)$ and $\mathrm{Frob}_w(L'/F)$ coincide.

If l^r is the order of $l^{n-t(l)}\hat{\gamma}$, we have by corollary 7.18.10

$$\mathrm{Gal}(L'/L) \cong \mathrm{Hom}(\mathbb{Z}l^{n-t(l)-1}\hat{\gamma}, E_{l^n}(L)) \cong E_{l^{r+1}}(L)$$

and

$$\mathrm{Gal}(L''/L) \cong \mathrm{Hom}(\mathbb{Z}l^{n-t(l)}\hat{\gamma}, E_{l^n}(L)) \cong E_{l^r}(L).$$

Hence we have an isomorphism of τ_∞-modules

$$\mathrm{Gal}(L'/L'') \cong E_{l^{r+1}}(L)/E_{l^r}(L).$$

The surjective homomorphism

$$E_{l^{r+1}}(L) \xrightarrow{l^r} E_l$$

shows that there is an isomorphism

$$\mathrm{Gal}(L'/L'') \cong E_l(L).$$

It follows from this and from lemma 7.11.5(ii) that we have

$$\mathrm{Gal}(L'/L'')^\pm \cong E_l(L)^\pm \cong \mathbb{Z}/l\mathbb{Z}.$$

In particular, $\mathrm{Gal}(L'/L'')^+$ is not reduced to the identity element. We have surjective homomorphism of galois groups

$$\begin{array}{ccccc} \mathrm{Gal}(L'/L) & & & & \mathrm{Gal}(M/L) \\ & \searrow & & \swarrow & \\ & & \mathrm{Gal}(L''/L) & & \end{array}$$

It follows that for any element $i \in \mathrm{Gal}(M/L)$ such that $i^{1+\tau_\infty} \in I_n^+$ there is at least one element $j \in \mathrm{Gal}(L'/L)$ such that $j^{1+\tau_\infty} \neq 1$ and $j|_{L''} = i|_{L''}$ that is to say for any element i satisfying (a) there is an element j satisfying (b) where

$$i|_{L''} = j|_{L''}.$$

Hence for any element $i \in \mathrm{Gal}(M/F)$ satisfying $i^{1+\tau_\infty} \in I_n^+$ there is a prime divisor $w \in \mathcal{D}_{l^n}$ and satisfying the conditions (a) and (b) above.

Furthermore, as $w \in \mathcal{D}_{l^n}$ the prime w remains inert in K/F (definition 7.11.3). It follows from the conditions (a) and (b) that $\mathrm{Frob}_w(K[z]/F) = [m]$, where $m \in \mathrm{Gal}(K[z]/F)$ and $m \notin \mathrm{Gal}(K[z]/K)$. Hence we have $\mathrm{Frob}_w(K[z]/F) = [\tau k]$ where τ is the nontrivial element of $\mathrm{Gal}(K/F)$ and $k \in \mathrm{Gal}(K[z]/K)$. Then we have $\mathrm{Frob}_{w^\sharp}(K[z]/K) = [(\tau k)^2]$. As $\mathrm{Gal}(K[z]/F)$ is a generalised dihedral group (proposition 2.5.7), it follows that $(\tau k)^2$ lies in the subgroup $\mathrm{Pic}(A)$ of $\mathrm{Gal}(K[z]/K)$. As l is prime to $|\mathrm{Pic}(A)|$, it follows that $\mathrm{Frob}_{w^\sharp}(K[z]/K) \in \mathrm{Pic}(A)$ has order prime to l; this gives the condition (c).

Similarly, as $z \in \mathcal{D}_{l^n}$ the prime z remains inert in K/F (definition 7.11.3). Hence we have $\mathrm{Frob}_z(K[w]/F) = [m]$, where $m \in \mathrm{Gal}(K[w]/F)$ and $m \notin \mathrm{Gal}(K[w]/K)$. Hence we have $\mathrm{Frob}_z(K[w]/F) = [\tau k]$ where τ is the nontrivial element of $\mathrm{Gal}(K/F)$ and $k \in \mathrm{Gal}(K[w]/K)$. Then we have $\mathrm{Frob}_{z^\sharp}(K[w]/K) = [(\tau k)^2]$. As $\mathrm{Gal}(K[w]/F)$ is a generalised dihedral group (proposition 2.5.7), it follows that $(\tau k)^2$ lies in the subgroup $\mathrm{Pic}(A)$ of $\mathrm{Gal}(K[w]/K)$. As l is prime to $|\mathrm{Pic}(A)|$, it follows that $\mathrm{Frob}_{z^\sharp}(K[w]/K) \in \mathrm{Pic}(A)$ has order prime to l; this gives the condition (d).□

7.18.39. Lemma. *Suppose that l is prime to $|\mathrm{Pic}(A)|$ and is prime to $|\mathrm{Pic}(B)|$. Let $i \in H$ be any element such that $i^{1+\tau_\infty} \in I_n^+$. Let $w \in \mathcal{D}_{l^n}$ be as in lemma 7.18.38 applied to i. Let $w^\sharp$ be the unique place of K above w. Then $l^{t(l)}\delta(z+w)$ is locally trivial at all places except at $w^\sharp$ and its restriction at the latter place has order at least $l^{n-2t(l)}$.*

Proof. The place $w^\sharp$ splits completely in the extension L/K. For we have $\mathrm{Frob}_w(L/F) = \mathrm{Frob}_w(L'/F)|_L = [\tau'' j]|_L = \tau_\infty$ so we have $\mathrm{Frob}_{w^\sharp}(L/K) = [\tau'']^2 = 1$.

Since $i^{1+\tau_\infty} \in I_n^+$, by lemma 7.18.22(iii) we obtain that $\mathrm{res}_{w^\sharp}(\delta(w)) = 0$. Hence by lemma 7.14.14(i), $\delta(w)$ is locally trivial everywhere. Therefore we have (by lemma 7.14.14(ii) and lemma 7.18.33)

$$\delta(w) \in Ш(E/K)^\epsilon_{l^n} \quad \text{and} \quad \gamma(w) \in S^{(l^n)}(K/F)^\epsilon.$$

But by proposition 7.18.28 and corollary 7.18.31, we then have

$$l^{t(l)}\gamma(w) = l^{t(l)}\delta(w) = 0.$$

By remark 7.14.12(ii) we then have

$$l^{t(l)}P_w = 0 \text{ in } {}_{l^n}E(K[w]). \tag{7.18.40}$$

By lemma 7.14.11(ii) we have

$$\delta(z+w) \in H^1(K[z+w]/K, E)^{-\epsilon}_{l^n}$$

and by lemma 7.14.14(i)

$$\mathrm{res}_v \delta(z+w) = 0$$

for all places $v \neq z^\sharp, w^\sharp$ of K. On the one hand, by (7.18.40), lemma 7.14.14(ii) and condition (d) of lemma 7.18.38, we have

$$\mathrm{res}_{z^\sharp} l^{t(l)}\delta(z+w) = 0.$$

On the other hand, let w' be a prime of $K[z]$ lying over $w^\sharp$; then $\mathrm{res}_{w^\sharp}(l^{t(l)}\delta(z+w))$ has the same order as $\mathrm{res}_{w'} l^{t(l)}P_z$ in ${}_{l^n}E(K[z]_{w'})$, by lemma 7.14.14(ii) and condition (c) of lemma 7.18.38. But we have by lemma 7.18.36

$$\mathrm{res}_{w'}(l^{n-t(l)-1}P_z) = 0$$

if and only if

$$\mathrm{Frob}_{w'}(L'/L) = 1;$$

but we have, as $w^\sharp$ splits completely in L/K (remark 7.18.34),

$$\mathrm{Frob}_{w'}(L'/L) = [(\tau'' j)^2]$$

hence $\mathrm{Frob}_{w'}(L'/L) = 1$ if and only if $(\tau'' j)^2 = 1$. As τ'' has order 2, $\mathrm{Frob}_{w'}(L'/L) = 1$ then holds if and only if $j^{1+\tau_\infty} = 1$ which contradicts the hypothesis (b) of lemma 7.18.38 on j. Therefore the order of $\mathrm{res}_{w'} l^{t(l)}P_z$ is at least $l^{n-2t(l)}$. Hence the order of $\mathrm{res}_{w^\sharp} l^{t(l)}\delta(z+w)$ is at least $l^{n-2t(l)}$. We have in conclusion that $l^{t(l)}\delta(z+w)$ is locally trivial at all places except at $w^\sharp$ and its restriction at the latter place has order at least $l^{n-2t(l)}$.□

7.18.41. Proposition. *Suppose that l is prime to $|\mathrm{Pic}(A)|$ and is prime to $|\mathrm{Pic}(B)|$. We have the inclusion*

$$l^{2t(l)} S^{(l^n)}(E/K)^{-\epsilon} \subseteq \mathbb{Z}\gamma(0)$$

and we have

$$l^{2t(l)} Ш(E/K)^{-\epsilon}_{l^\infty} = 0.$$

Proof. Let $s \in S^{(l^n)}(E/K)^{-\epsilon}$. Let $i \in H$ be an element such that $i^{1+\tau_\infty} \in I_n^+$ and let $\delta(z+w)$ be the cohomology class given by lemmas 7.18.38 and 7.18.39

applied to i. Applying proposition 7.16.3 to $l^{t(l)}\delta(z+w)$, we obtain that (by lemma 7.18.39)

$$\mathrm{res}_{w^\sharp} l^{2t(l)} s = 0.$$

Therefore as $\mathrm{Frob}_w(M/F) = [\tau' i]$ (by condition (a) of lemma 7.18.38) we have

$$l^{2t(l)}\hat{s}((\tau' i)^2) = 0.$$

Hence we have as τ' has order 2

$$l^{2t(l)}\hat{s}(\tau' h \tau'^{-1} h) = 0.$$

Whence we have (as $\hat{s}$ is a homomorphism $H \to E_{l^n}$)

$$l^{2t(l)}\hat{s}(h^{\tau'}) + l^{2t(l)}\hat{s}(h) = 0.$$

As s is in the $-\epsilon$ eigenspace under the action of τ_∞, this equation becomes

$$l^{2t(l)}(-\epsilon\tau_\infty)\hat{s}(h) + l^{2t(l)}\hat{s}(h) = l^{2t(l)}(1-\epsilon\tau_\infty)\hat{s}(h) = 0.$$

We obtain for all $i \in H$ such that $i^{1+\tau_\infty} \in I_n^+$

$$l^{2t(l)}(1-\epsilon\tau_\infty)\hat{s}(i) = 0. \tag{7.18.42}$$

In particular, (7.18.42) holds for all $i \in I_n$. Hence we have from (7.18.42)

$$l^{2t(l)}(1-\epsilon\tau_\infty)\hat{s}(I_n) = 0 \tag{7.18.43}$$

that is

$$l^{2t(l)}\hat{s}(I_n) \subseteq E_{l^n}^{\epsilon}.$$

But then $l^{2t(l)}\hat{s}(I_n)$ is a cyclic subgroup of E_{l^n} defined over K and hence is zero by definition 7.10.3(c) and (e). Therefore we obtain

$$l^{2t(l)}\hat{s}(I_n) = 0.$$

Hence $l^{2t(l)}\hat{s}$ induces a homomorphism $H/I_n \to E_{l^n}$. But we have that H/I_n is isomorphic to the galois group of the field extension L_n/L (see the commutative diagram (7.18.19)). Hence we have that

$$l^{2t(l)}\hat{s} \in \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L_n/L), E_{l^n}).$$

But by the corollary 7.18.10 we have

$$\mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L_n/L), E_{l^n}) \cong \mathbb{Z}\gamma(0)$$

as the field L_n is precisely the field $L_{\mathbb{Z}\gamma(0)}$ in the terminology of the corollary 7.18.10. It follows that $l^{2t(l)}s$ is an integral multiple of $\gamma(0)$. We then have the

inclusions, as s is any element of $S^{(l^n)}(E/K)^{-\epsilon}$,

$$l^{2t(l)} S^{(l^n)}(E/K)^{-\epsilon} \subseteq \mathbb{Z}\gamma(0).$$

We have the exact sequence of quasi-groups (see (7.9.3))

$$0 \to {}_*E(K) \to S^{(*)}(E/K) \to \text{Ш}(E/K)_* \to 0.$$

Hence as $l^{2t(l)} S^{(l^n)}(E/K)^{-\epsilon}$ is contained in the image of ${}_{l^n}E(K)$ we obtain

$$l^{2t(l)} \text{Ш}(E/K)^{-\epsilon}_{l^\infty} = 0. \quad \square \tag{7.18.44}$$

End of proof of theorem 7.7.5

7.18.45. Proposition. *Suppose that l is prime to $|\mathrm{Pic}(A)|$ and is prime to $|\mathrm{Pic}(B)|$. We have:*
(i) *the highest power of l dividing $[E(K) : \mathbb{Z}x_0]$ is at most $l^{6t(l)}$;*
(ii) $l^{2t(l)} \text{Ш}(E/K)_{l^\infty} = 0$;
(iii) $l^{2t(l)} \text{Ш}(E/F)_{l^\infty} = 0$.

Proof. We have from proposition 7.18.41 and corollary 7.18.31

$$l^{2t(l)} \text{Ш}(E/K)_{l^\infty} = 0.$$

We then obtain from proposition 7.9.4

$$l^{2t(l)} \text{Ш}(E/F)_{l^\infty} = 0.$$

This proves parts (ii) and (iii) of the proposition.

For part (i), from proposition 7.18.41 we have

$$l^{2t(l)} S^{(l^n)}(E/K)^{-\epsilon} \subseteq \mathbb{Z}\gamma(0)$$

and we have from proposition 7.18.28

$$l^{2t(l)} S^{(l^n)}(E/K)^{\epsilon} = 0.$$

It then follows that

$$l^{2t(l)}({}_{l^n}E(K)) \subseteq \mathbb{Z}\gamma(0).$$

That is to say we have, as $\gamma(0) = \partial P_0$, where P_0 is the image of $x_0 \in E(K)$ in ${}_{l^n}E(K)$ (see the diagram of 7.14.5)

$$l^{2t(l)} E(K) \otimes_{\mathbb{Z}} \mathbb{Z}/l^n\mathbb{Z} \subseteq \mathbb{Z}P_0 \subseteq E(K) \otimes_{\mathbb{Z}} \mathbb{Z}/l^n\mathbb{Z}.$$

We may then take the inverse limits over n of these inclusions and obtain the inclusions of $\mathbb{Z}_l$-modules, where $\mathbb{Z}_l$ is the l-adic completion of $\mathbb{Z}$, (cf. [H, pp.190-192])

$$l^{2t(l)}E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l \subseteq \mathbb{Z}_l x_0 \subseteq E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l.$$

As $\mathbb{Z}_l x_0$ is a free $\mathbb{Z}_l$-module of rank 1; it follows that $l^{2t(l)}E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l$ is a free $\mathbb{Z}_l$-module of rank 1. Furthermore by the Mordell-Weil theorem $E(K)$ is a finitely generated group; hence we obtain an isomorphism

$$E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l \quad \cong \quad \mathbb{Z}_l \oplus T$$

where T is a finite abelian l-group such that

$$l^{2t(l)}T = 0.$$

As E is an elliptic curve, the l-torsion subgroup of T is a vector space of dimension ≤ 2 over the prime field $\mathbb{F}_l$; we obtain

$$|T| \leq l^{4t(l)}.$$

The group

$$\frac{E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l}{\mathbb{Z}_l x_0}$$

is then a homomorphic image of the quotient group

$$\frac{\mathbb{Z}_l \oplus T}{l^{2t(l)}(\mathbb{Z}_l \oplus T)} \cong \frac{\mathbb{Z}_l}{l^{2t(l)}\mathbb{Z}_l} \oplus T.$$

This group has order

$$l^{2t(l)}|T| \leq l^{6t(l)}.$$

We obtain that, where $|.|_l$ denotes the usual l-adic valuation of $\mathbb{Z}$,

$$|[E(K) : \mathbb{Z}x_0]|_l \geq l^{-6t(l)}. \quad \square$$

7.19 Comments and errata for [Br2]

We would like to take this opportunity to give some comments and corrections on the first paper [Br2] of this series. The page numbers and proposition numbers are that of [Br2] unless otherwise stated.

p.490. l.↓13. The second sentence should read: "Let F be the rational function field $k(T)$ over k."

p.490. Theorem 1.1(i). The statement concerning $E(F)$ is not correct. It should read that $E(F)$ is of finite order if the sign $\epsilon = \pm 1$ in the functional equation for the L-function $L(E/F, s)$ of E/F is equal to $+1$ and is

an abelian group of rank 1 if $\epsilon = -1$. The same change should be made in the corresponding statement of Theorem 5.2.6.(i).

p.491. In this list of surfaces over finite fields, for which the Tate conjecture is known, should be included all Fermat surfaces over finite fields. This has been proved by Shioda and Katsura [SK, Theorem 2.6]. They have also proved the Tate conjecture for many higher dimensional Fermat varieties.

p.501. l.↓16-17. This definition of split multiplicative reduction should read that the closed fibre above ∞ of a ∞-minimal model of E/F is a nodal cubic where the tangents at the node are rational over the residue field $\kappa(\infty)$.

p.501. Theorem 4.1. A proof of this function field analogue of the Taniyama-Weil conjecture has been given for the general case of Tate elliptic curves over global fields of positive characteristic by Gekeler and Reversat [GR]. The original Taniyama-Weil conjecture has been proved by Wiles [W] for semi-stable elliptic curves over the rational numbers $\mathbb{Q}$.

p.504. Lemma 5.5.6. In the statement of this lemma, finitely many primes of $\mathcal{P}$ must be excluded, namely the primes $l = 2, 3$ and the primes dividing $q^2 - 1$, where $q = |k|$. The reason for excluding 2 and 3 is that the group $\mathrm{SL}(\mathbb{Z}_l)$ has no non-trivial abelian homomorphic images for $l \geq 5$ but such images exist for $l = 2$ and 3. The reason for excluding $l|q^2 - 1$ is that the implication in the proof that $M \subseteq K[0]$ implies $M \subseteq K$ need not be true otherwise. In fact this lemma 5.5.6 holds for all except finitely many prime numbers l and not just the primes l lying in $\mathcal{P}$ as is stated in the lemma.

[See proposition 7.3.8 of the present paper for an improved version of lemma 5.5.6.]

p.505. Lemma 5.5.10.(ii) This should read $\mathcal{E}_{0,z}(\kappa(z))_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}$. Similarly, p.506. l.↓2 should read $E_{l^n}^{\mathrm{Frob}_z} \cong \mathbb{Z}/l^n\mathbb{Z}$.

p.507. l.↑1-3. Let ϵ be the sign in the functional equation of E; then the Atkin-Lehner involution w_I acts on E as $-\epsilon$. The ϵ in this paper [Br2] is used confusingly for both these two opposite rôles. In Lemma 5.7.9, ϵ is the opposite of the sign of functional equation. Furthermore, p.510 l.↓2-3 should also read that ϵ is the opposite of the sign of functional equation.

p.512 l.↓21. "Then $L' \cap M = L \ldots$" this is true if $t(l) = 0$, which holds for all except finitely many l; this is sufficent to prove the main theorem 5.2.6. Nevertheless $L' \cap M \neq L$ if $t(l) \neq 0$ and in this case the proof can be completed by the modification of the same argument given in lemma 7.18.38 above.

Appendix A

Rigid analytic modular forms

This appendix is an introduction to rigid analytic modular forms of characteristic $p > 0$ and rigid analytic spaces. Rigid analytic modular forms were first introduced by Goss. The application to elliptic curves over function fields is explained in §A.13 and is the following; with the notation of theorem 4.7.1, if $f : X_0^{\mathrm{Drin}}(I) \to E$ is a finite surjective morphism of F-schemes where E is an elliptic curve over F, and if ω is a Néron differential on E then $f^*\omega$ is a rigid analytic modular form on the rigid analytic space $(X_0^{\mathrm{Drin}}(I) \otimes_F F_\infty)_{\mathrm{an}}$ associated to the curve $X_0^{\mathrm{Drin}}(I)/F$.

[We only give here a brief résumé of the definition and main properties of rigid analytic spaces and also of modular forms; in particular, most proofs are omitted. For more details see [T4], [BGR],[Hu], [Go1], and [Go2].]

A.1 Basic definitions

(A.1.1) Let L be a fixed ground field, complete with respect to a non-trivial non-archimedean absolute value denoted by $|x|$ for all $x \in L$. The absolute value $|.|$ satisfies for all $x, y \in L$

$$|xy| = |x|.|y|$$

and

$$|x + y| \leq \max(|x|, |y|).$$

The field L is complete with respect to the metric $d(x, y) = |x - y|$.

(A.1.2) Let $\overline{L}$ be the algebraic closure of L. The absolute value $|.|$ then extends uniquely to an absolute value $|.|_{\overline{F}}$ on $\overline{L}$. Let $\widehat{\overline{L}}$ denote the completion of $\overline{L}$ with respect to this absolute value $|.|_{\overline{L}}$. Then the field $\widehat{\overline{L}}$ is also algebraically closed.

M.L. Brown: LNM 1849, pp. 435–505, 2004.

(A.1.3) Let $R = \{x \in L \mid |x| \leq 1\}$. Then R is the ring of integers of L and possesses a unique maximal ideal $\mathfrak{m} = \{x \in L \mid |x| \leq 1\}$. The quotient $R/\mathfrak{m}$ is the residue field of R.

(A.1.4) Let

$$f(z) = \sum_{i=0}^{\infty} a_i z^i$$

be a formal power series with coefficients in L; that is to say $f \in L[[z]]$. Let $x \in L$; then the power series $f(x)$ converges in L if and only if $a_i x^i \to 0$ as $i \to \infty$, as the absolute value is non-archimedian.

A.2 The Tate algebra

(A.2.1) Let D^n be the polydisc

$$D^n = \{(x_1, \ldots, x_n) \in L^n \mid |x_i| \leq 1 \text{ for all } i\}.$$

Let $L\{z_1, \ldots, z_n\}$ be the ring of all formal power series in n variables $z_1, \ldots, z_n$ which converge in D^n. The algebra $L\{z_1, \ldots, z_n\}$ is called a *Tate algebra*.

For an n-tuple $\mathbf{i}$ of non-negative integers $\mathbf{i} = (i_1, \ldots, i_n)$ we write $\mathbf{z}^{\mathbf{i}}$ for the monomial $z_1^{i_1} \ldots z_n^{i_n}$; we write

$$||\mathbf{i}|| = \sum_{r=1}^{n} i_r.$$

Then we have that a formal power series $f \in L[[z_1, \ldots, z_n]]$ is an element of the Tate algebra $L\{z_1, \ldots, z_n\}$ if and only if

$$f(z_1, \ldots, z_n) = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{z}^{\mathbf{i}}$$

where

$$|a_{\mathbf{i}}| \to 0 \text{ as } ||\mathbf{i}|| \to \infty.$$

We write T_n in place of $L\{z_1, \ldots, z_n\}$.

(A.2.2) The Tate algebra T_n is noetherian. Define a norm on T_n by

$$||\sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{z}^{\mathbf{i}}|| = \max_{\mathbf{i} \in \mathbb{N}^n} |a_{\mathbf{i}}|.$$

Then this norm is multiplicative on the algebra T_n and T_n is then a Banach algebra over L with respect to this norm.

(A.2.3) For any maximal ideal J of T_n the L-algebra T_n/J can be shown to be a finite field extension of L. Let

$$\max(T_n) = \text{ the set of maximal ideals of } T_n.$$

A.3 Affinoid spaces, rigid analytic spaces

(A.3.1) Let I be an ideal of T_n. The algebra $A = T_n/I$ is called an *affinoid algebra*. The L-algebra A is noetherian and is a Banach algebra with respect to the quotient norm

$$||f|| = \inf\{||f' + g|| \mid g \in I\}, \text{ for any lifting } f' \text{ of } f.$$

(A.3.2) Let $Y \subset \max(T_n)$ denote the zero set of I: the set Y is the set of maximal ideals $\mathfrak{m}$ of T_n such that all elements of I induce zero in the residue field $T_n/\mathfrak{m}$, that is to say $\mathfrak{m} \supset I$. Denote by $\max(A)$ the set of maximal ideals of A. The natural surjection $T_n \to A$ induces a map of the maximal spectra

$$\max(A) \to \max(T_n).$$

This map induces a bijection between $\max(A)$ and Y.

(A.3.3) Let U be a subset of $X = \max(A)$ such that the functor which associates with each affinoid algebra B over L the set of homomorphisms $\phi : A \to B$ such that $\phi^*(\max(B)) \subseteq U$ is representable; then a subset U of X of this type is called an *open affinoid subset*. Thus U is such a subset of X if and only if the following two conditions hold:

(a) There is an affinoid algebra B and a homomorphism $f : A \to B$ such that the induced map $f^* : \max(B) \to \max(A)$ has its image contained in U;

(b) If C is an affinoid algebra and $g : A \to C$ is a homomorphism such that the induced map $g^* : \max(C) \to \max(A)$ has its image contained in U then there is a unique homomorphism $h : B \to C$ such that $g = h \circ f$.

(A.3.4) If $U \subseteq X$ is an open affinoid subset corresponding to the homomorphism $f : A \to B$ and $V \subseteq \max(B)$ is an open affinoid subset corresponding to the homomorphism $g : B \to C$ then $f^*(V) \subseteq U$ is an open affinoid subset of X corresponding to the homomorphism $g \circ f : A \to C$.

A.3.5. Definition. Let $f_0, \ldots, f_n \in A$ be elements such that $A = \sum_{i=0}^{n} f_i A$, that is to say $f_0, \ldots, f_n$ have no common zeros on $X = \max(A)$. The set

$$X(f_0, \ldots, f_n) = \{x \in X \mid |f_i(x)| \leq |f_0(x)|, \text{ for all } i\}$$

is an open affiniod subset of X called a *rational subset* of X.

(A.3.6) The affinoid algebra corresponding to the rational open affinoid $X(f_0, \ldots, f_n)$ of X is

$$A\{T_1, \ldots, T_n\}/(f_0 T_i - f_i,\ i = 1, \ldots, n).$$

If R_1 is a rational subset of X and R_2 is a rational subset of the affinoid R_1 then R_2 is a rational subset of X. The intersection of two rational subsets of X is also a rational subset of X.

A.3.7. Theorem. (Gerritzen-Grauert, [BGR, p.309]) *Every open affinoid subset of X is a finite union of rational subsets of X.* □

(A.3.8) An *admissible open subset* of X is a rational affinoid open subset; denote by $\mathcal{G}$ the category of admissible open subsets of X, where the morphisms $U \to V$ are just the inclusion morphisms $U \subseteq V$, if any.

A covering $\mathcal{U}$ of an admissible open subset $U \in \mathcal{G}$ is *admissible* if $\mathcal{U}$ is finite and all elements of $\mathcal{U}$ are rational open subsets of X. Let $\mathrm{cov}(U)$ denote the set of all admissible open coverings of the admissible subset U, that is to say $\mathrm{cov}(U)$ is the set of finite coverings of U by admissible open subsets.

The category of admissible subsets $\mathcal{G}$ of X together with the admissible coverings $\mathrm{cov}(U)$ of all $U \in \mathcal{G}$ form a Grothendieck topology on X in that it satisfies the following conditions:

The admissible subsets satisfy:

(a) $\emptyset, X$ are admissible subsets;

(b) for all $U, V \in \mathcal{G}$ then $U \cap V$ is admissible;

The admissible coverings satisfy:

(c) for all $\mathcal{U} \in \mathrm{cov}(U)$ and for all $V \in \mathcal{U}$ then V is an admissible subset;

(d) $\{U\}$ is an admissible covering of U;

(e) if $\mathcal{U} \in \mathrm{cov}(U)$ and if $V \subset U$ is an admissible subset then

$$\{U' \cap V \mid U' \in \mathcal{U}\}$$

is an admissible covering of V;

(f) if $(U_i)_{i\in I}$ is an admissible covering of U and if $\mathcal{U}_i$ is an admissible covering of U_i for all i then

$$\bigcup_{i\in I}\mathcal{U}_i$$

is an admissible covering of U.

(A.3.9) Let $X = \max(A)$ be equipped with its Grothendieck topology of admissible open subsets and admissible coverings, that is to say X is a *site*. A *presheaf* of abelian groups (or rings, modules etc) on the site X is then a contravariant functor

$$\mathcal{F} : \mathcal{G}^{\mathrm{opp}} \to \mathbf{Ab}$$

where **Ab** denotes the category of abelian groups.

A presheaf $\mathcal{F}$ on X is a *sheaf* if for any admissible subset U of X and for any admissible covering $\mathcal{U} = \{U_i\}_{i\in I}$ of U then the sequence

$$\mathcal{F}(U) \to \prod_i \mathcal{F}(U_i) \begin{array}{c}\longrightarrow\\[-1ex]\longrightarrow\end{array} \prod_{i,j} \mathcal{F}(U_i \cap U_j)$$

is exact.

[See [M2, Chapter 2] for more details of presheaves and sheaves for a Grothendieck topology.]

(A.3.10) Let X be the maximal spectrum $\max(A)$ of the affinoid algebra A. Denote by $\mathcal{O}(U)$ be the affinoid algebra of a rational subset $U \subset X$. The algebras $\mathcal{O}(U)$ together with their natural restriction homomorphisms form a presheaf $\mathcal{O}$ on X.

A.3.11. Theorem. *The preasheaf $\mathcal{O}$ is a sheaf. More precisely, let $\{U_\lambda\}_\lambda$ be a finite covering of X by rational affinoid subdomains $U_\lambda \subseteq X$. Denoting by $\check{H}^i(\mathcal{U}, \mathcal{O})$ the Čech cohomology of the presheaf $\mathcal{O}$ with respect to $\{U_\lambda\}_\lambda$, we have $\check{H}^0(\{U_\lambda\}_\lambda, \mathcal{O}) = A$ and $\check{H}^i(\{U_\lambda\}_\lambda, \mathcal{O}) = 0$ for all $i > 0$.* □

[See [T4, §8] or [BGR, §8.2] for the proof. For full details of Čech cohomology of a presheaf on a site see [M2, Chapter 3, §2] or for the case of the rigid analytic site, see [BGR, §8.1]; for a particular case of Čech cohomology on a site, see §5.4 above.]

(A.3.12) An *affinoid space* over L is a topological space $\max(A)$, where A is an affinoid L-algebra, and where this space is equipped with its Grothendieck topology of admissible subsets and admissible coverings and is equipped with the structure sheaf $\mathcal{O}$. The space $\max(A)$ is then a locally ringed space.

A *morphism* $\phi : \max(A) \to \max(B)$ of L-affinoid spaces is a pair (f^*, f) where $f : B \to A$ is an L-algebra homomorphism and $f^* : \max(A) \to \max(B)$ is the map induced by f.

A.3.13. Remarks. (1) If $X = \max(A)$ is an affinoid space over L then a map $\phi : X \to D^n$, where D^n is the polydisc over L (see (A.2.1)) is affinoid if and only if there are functions $f_1, \ldots, f_n \in A$ such that $\phi(x) = (f_1(x), \ldots, f_n(x))$ for all $x \in X$.

(2) That an L-algebra morphism of affinoid algebras $f : B \to A$ induces a map of the corresponding maximal spectra, that is to say $f^{-1}(\mathfrak{m})$ is a maximal ideal of B for all maximal ideals $\mathfrak{m}$ of A follows from $A/\mathfrak{m}$ being a finite extension of the ground field L. This is Hilbert's Nullstellensatz for affinoid algebras [BGR, §7.1.2].

(A.3.14) A *rigid analytic space* is triple $(X, \mathcal{G}, \mathcal{O})$ where X is a topological space equipped with a Grothendieck topology $\mathcal{G}$ and a sheaf of L-algebras $\mathcal{O}$ such that there is a covering $(X_i)_{i \in I}$ of X, with respect to the Grothendieck topology, such that each triple $(X_i, \mathcal{G}|_{X_i}, \mathcal{O}|_{X_i})$ is an affinoid space.

A morphism of rigid analytic spaces $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is an L-morphism of locally ringed spaces.

A.3.15. Remarks. (1) Let X be a rigid analytic space over L. Assume that X is reduced in that it has no nilpotent functions. Then X is said to be *connected* if a rigid function with zero Taylor series at a point is everywhere zero. The space X is said to be *geometrically connected* if it is connected when viewed as a rigid analytic space over all finite extensions of L.

(2) The Grothendieck topology on a rigid analytic space $(X, \mathcal{G}, \mathcal{O})$ in (A.3.14) is not uniquely determined by its restrictions to each open subset X_i of the covering $(X_i)_{i \in I}$ (see [BGR, §9.1.3] for more details).

A.4 Etale cohomology of rigid analytic spaces

In Drinfeld's paper [Dr1], the étale cohomology of rigid analytic spaces is defined for the first time but only for the sheaves $\mathbb{Z}/n\mathbb{Z}$ and μ_n and only for H^0 and H^1. The cohomology of rigid analytic spaces was subsequently developed by Berkovich [Be], Huber [Hu], Fresnel and van der Put [FP], Schneider and Stuhler [SS].

Drinfeld's original definition is presented in this section and the properties that Drinfeld [Dr1] states are here proved, as this is all that is necessary for these appendices A and B.

(A.4.1) Let X be a rigid analytic space over L. The following étale cohomology groups are then defined in terms of global sections of rigid analytic sheaves, where $\mathbb{Z}/n\mathbb{Z}$ is the constant sheaf and μ_n is the sheaf of nth roots of unity on X,

$$H^0_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z}) = H^0_{\text{rigid}}(X, \mathbb{Z}/n\mathbb{Z}))$$

and

$$H^0_{\text{ét}}(X, \mu_n) = H^0_{\text{rigid}}(X, \mu_n).$$

(A.4.2) The group $H^1_{\text{ét}}(X, \mu_n)$ is defined to be the group under tensor product of pairs $(\mathcal{L}, \phi)$ up to isomorphism where $\mathcal{L}$ is an invertible sheaf on X and ϕ is an isomorphism $\phi : \mathcal{O}_X \cong \mathcal{L}^{\otimes n}$.

The group $H^1_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z})$ is defined by the equation

$$H^1_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z}) = H^1_{\text{ét}}(X, \mu_n) \otimes \mu_n^{-1}$$

where μ_n^{-1} is the $\text{Gal}(L^{\text{sep}}/L)$-module

$$\mu_n^{-1} = \text{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z}).$$

(A.4.3) Let L^{sep} be the separable closure of the field L. Let $\mathcal{M}$ denote one of the sheaves $\mathbb{Z}/n\mathbb{Z}$ or μ_n. Then the cohomology groups $H^i_{\text{ét}}(X \otimes_L L^{\text{sep}}, \mathcal{M})$, for $i = 0, 1$, are then defined by the equation

$$H^i_{\text{ét}}(X \otimes_L L^{\text{sep}}, \mathcal{M}) = \varinjlim_{K} H^i_{\text{ét}}(X \otimes_L K, \mathcal{M})$$

where K runs over all finite separable extension fields of L contained in L^{sep}. The group $\text{Gal}(L^{\text{sep}}/L)$ acts on all these cohomology groups.

A.4.4. Proposition. *If $f : X \to Y$ is a finite étale morphism of rigid analytic spaces with galois group G of order prime to n then the induced map*

$$g : H^1_{\text{ét}}(Y, \mu_n) \to H^1_{\text{ét}}(X, \mu_n)^G$$

is an isomorphism.

Proof. Let $\mathcal{K}$ denote the sheaf on Y whose sections $\Gamma(U, \mathcal{K})$ are obtained by inverting the non-zero divisors of the ring $\Gamma(U, \mathcal{O})$ for all open affinoid subsets U of Y. Let $\mathcal{K}^*$ denote the corresponding sheaf of multiplicatively invertible elements of $\mathcal{K}$.

Let $\mathcal{L}$ be a line bundle on Y such that there is an isomorphism $\phi : \mathcal{L}^{\otimes n} \to \mathcal{O}_Y$. Suppose also that there is an isomorphism of $\mathcal{O}_X$-modules $\psi : \mathcal{O}_X \cong f^*\mathcal{L}$. There is an admissible open covering $\{U_i\}_i$ of Y such that $\mathcal{L}$ is represented by (U_i, f_i) where $f_i \in \Gamma(U_i, \mathcal{K}^*)$ and $f_i f_j^{-1}$ is a unit on $U_i \cap U_j$ for all $i \neq j$.

As $f^*\mathcal{L}$ is trivial, there is $h \in \Gamma(X, \mathcal{K}^*)$ such that $(f^{-1}(U_i), f_i/h)$ is equivalent to a trivial Cartier divisor, that is to say f_i/h is a unit on $f^{-1}(U_i)$ for all i. As the isomorphism class of the line bundle $f^*\mathcal{L}$ is G-invariant, we then have that for all $\sigma \in G$, f_i/h^σ is a unit on $f^{-1}(U_i)$ for all i. Hence h/h^σ is a unit on $f^{-1}(U_i)$ for all i and all σ. Hence $\epsilon(\sigma) = h^\sigma/h$ is a cocycle $G \to \Gamma(X, \mathcal{O}^*)$ and its corresponding cohomology class is in $H^1(G, \Gamma(X, \mathcal{O}^*))$.

Via the isomorphism ϕ, there is then an element $f \in \Gamma(Y, \mathcal{K}^*)$ such that f_i^n/f is a unit on U_i for all i. It follows that $h^{\sigma n}/f$ is a unit on $f^{-1}(U_i)$ for all i and all σ. That is to say there is an element $\eta \in \Gamma(X, \mathcal{O}^*)$ such that $h^n\eta = f$. We then obtain the equation for all $\sigma \in G$

$$\epsilon(\sigma)^n \eta^\sigma = \eta.$$

That is to say, $\sigma \mapsto \epsilon(\sigma)^n$ is a coboundary. Hence the class of ϵ in $H^1(G, \Gamma(X, \mathcal{O}^*))$ is annihilated by n. As it is also annihilated by $|G|$, the class of ϵ is therefore zero as $|G|$ and n are coprime. It follows that there is a unit $u \in \Gamma(X, \mathcal{O}^*)$ such that uh is G-invariant and hence is an element of $\Gamma(Y, \mathcal{O}^*)$, as $f^{-1}(U_i) \to U_i$ is a finite étale morphism for all i. It follows that f_i/uh is a unit on U_i for all i and hence $\mathcal{L}$ is a trivial line bundle. This shows that the kernel of the homomorphism g is reduced to zero.

Suppose now that $(\mathcal{I}, \psi)$ is a line bundle on X whose cohomology class lies in $H^1_{\text{ét}}(X, \mu_n)^G$ and where ψ is an isomorphism $\mathcal{I}^{\otimes n} \cong \mathcal{O}_X$. We have the two projection morphisms $\phi_1, \phi_2 : X \times_Y X \to X$. Furthermore, as X is finite and étale over Y with galois group G, the product $X \times_Y X$ is isomorphic to the disjoint union $\coprod_{\sigma \in G} X_\sigma$ of copies of X. As the isomorphism class of $\mathcal{I}$ is G-invariant, the pullbacks $\phi_1^*\mathcal{I}$ and $\phi_2^*\mathcal{I}$ are isomorphic. Furthermore, the isomorphism $\psi : \mathcal{I}^{\otimes n} \cong \mathcal{O}_X$ is also G-invariant up to isomorphism. Hence by descent, there is a line bundle $\mathcal{L}$ on Y such that $\mathcal{I} \cong f^*\mathcal{L}$ and such that there is an isomorphism $\chi : \mathcal{L}^{\otimes n} \cong \mathcal{O}_Y$ which induces the isomorphism ψ. Hence the map g is surjective. □

A.4.5. Proposition. (Kummer sequence) *Let X/L be a rigid analytic space. Then there is an exact sequence of abelian groups induced from multiplication by $n : \mathcal{O}_X^* \to \mathcal{O}_X^*$*

$$0 \to H^0_{\text{ét}}(X, \mu_n) \to H^0_{\text{rigid}}(X, \mathcal{O}_X^*) \to H^0_{\text{rigid}}(X, \mathcal{O}_X^*) \to$$

$$H^1_{\text{ét}}(X, \mu_n) \to H^1_{\text{rigid}}(X, \mathcal{O}_X^*) \to H^1_{\text{rigid}}(X, \mathcal{O}_X^*).$$

Proof. The exactness of the sequence at every point except the term $H^1(X, \mu_n)$ is obvious. In particular, it is clear that the kernel of $H^1_{\text{rigid}}(X, \mathcal{O}_X^*) \to H^1_{\text{rigid}}(X, \mathcal{O}_X^*)$ is the image of $H^1_{\text{ét}}(X, \mu_n) \to H^1_{\text{rigid}}(X, \mathcal{O}_X^*)$.

Suppose then that $(\mathcal{L}, \phi)$ is an element of $H^1(X, \mu_n)$ which is in the kernel of $H^1(X, \mu_n) \to H^1_{\text{rigid}}(X, \mathcal{O}_X^*)$. Here $\mathcal{L}$ is a line bundle on X and ϕ is an isomorphism $\mathcal{L}^{\otimes n} \cong \mathcal{O}_X$.

As $(\mathcal{L}, \phi)$ is in the kernel, we have that there is an isomorphism $\psi : \mathcal{L} \cong \mathcal{O}_X$. It follows that $\psi \circ \phi^{-1}$ is an automorphism of $\mathcal{O}_X$ and hence is given by an element of $H^0_{\text{rigid}}(X, \mathcal{O}_X^*)$. Hence the above sequence is exact.□

A.4.6. Proposition. *Let $\{X_i\}_{i\in I}$ be an admissible open covering of a rigid analytic space X with nerve of dimension ≤ 1. Then there is an exact sequence*

$$0 \to H^0_{\text{ét}}(X, \mu_n) \to \prod_i H^0_{\text{ét}}(X_i, \mu_n) \to \prod_{i\neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n) \to$$

$$H^1_{\text{ét}}(X, \mu_n) \to \prod_i H^1_{\text{ét}}(X_i, \mu_n) \to \prod_{i\neq j} H^1_{\text{ét}}(X_i \cap X_j, \mu_n)$$

Proof. It is assumed that the index set I is well ordered by $>$ and that the products $\prod_{i,j}$ are over pairs i, j such that $i > j$. That the nerve of the covering $\{X_i\}_{i\in I}$ has dimension ≤ 1, means that $X_i \cap X_j \cap X_k$ is empty for any triple of distinct indices i, j, k.

That the sequence

$$0 \to H^0_{\text{ét}}(X, \mu_n) \to \prod_i H^0_{\text{ét}}(X_i, \mu_n) \to \prod_{i\neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n)$$

is exact is then the definition of μ_n being a sheaf on X.

The coboundary map

$$\prod_{i\neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n) \to H^1_{\text{ét}}(X, \mu_n)$$

is defined as follows. Let $f_{ij} \in H^0_{\text{ét}}(X_i \cap X_j, \mu_n)$ for all $i \neq j$, where $i > j$. It is required to define an element $(\mathcal{L}, \phi)$ of $H^1_{\text{ét}}(X, \mu_n)$. On every open subscheme X_i we have the sheaf $\mathcal{O}_{X_i}$. Define an isomorphism of sheaves for every $i > j$

$$\phi_{ij} : \mathcal{O}_{X_i \cap X_j} \to \mathcal{O}_{X_i \cap X_j}$$

by $h \mapsto h f_{ij}$. We have that $\phi_{ij}^{\otimes n}$ is the identity map $\mathcal{O}_{X_i\cap X_j} \to \mathcal{O}_{X_i\cap X_j}$. We may then use the ϕ_{ij} to glue the sheaves $\mathcal{O}_{X_i}$ together to obtain a locally free rank 1 sheaf $\mathcal{L}$ on X. As $\phi_{ij}^{\otimes n}$ is the identity map for all $i > j$ we have that there is an isomorphism of sheaves of $\mathcal{O}_X$-modules $\phi : \mathcal{L}^{\otimes n} \to \mathcal{O}_X$. This pair $(\mathcal{L}, \phi) \in H^1_{\text{ét}}(X, \mu_n)$ is the image of $\{f_{ij}\}_{ij}$. It is now evident that the kernel of the coboundary map $\prod_{i\neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n) \to H^1_{\text{ét}}(X, \mu_n)$ is equal to the image of $\prod_i H^0_{\text{ét}}(X_i, \mu_n) \to \prod_{i\neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n)$.

Suppose now that $(\mathcal{L}, \phi)$ in $H^1_{\text{ét}}(X, \mu_n)$ is in the kernel of $H^1_{\text{ét}}(X, \mu_n) \to \prod_i H^1_{\text{ét}}(X_i, \mu_n)$. Then the restriction of $(\mathcal{L}, \phi)$ to each X_i is isomorphic to $\mathcal{O}_X$. But ϕ is an isomorphism $\mathcal{L}^{\otimes n} \cong \mathcal{O}_X$. Hence there is an

isomorphism for all i

$$\psi_i : \mathcal{L}|_{X_i} \cong \mathcal{O}_{X_i}.$$

such that

$$\psi_i^{\otimes n} : \mathcal{L}^{\otimes n}|_{X_i} \cong \mathcal{O}_X$$

coincides with the restriction $\phi|_{X_i}$ of ϕ for all i. We obtain that on each open subset $X_i \cap X_j$ there are isomorphisms

$$\mathcal{L}|_{X_i \cap X_j} \overset{\psi_i|_{X_j}}{\longrightarrow} \mathcal{O}_{X_i \cap X_j} \overset{\psi_j^{-1}|_{X_i}}{\longrightarrow} \mathcal{L}|_{X_j \cap X_i}.$$

We then have that $f_{ij} = \psi_i|_{X_j} \circ \psi_j^{-1}|_{X_i}$ is an isomorphism $\mathcal{O}_{X_i \cap X_j} \to \mathcal{O}_{X_i \cap X_j}$ and hence $f_{ij} \in H^0_{\text{ét}}(X_i \cap X_j, \mathcal{O}_X^*)$; by the compatibility of the $\psi_i^{\otimes n}$ with ϕ, we have that $f_{ij}^{\otimes n}$ is equal to the identity automorphism of $\mathcal{O}_{X_i \cap X_j}$. Hence we have that $\{f_{ij}\}_{ij} \in \prod_{i>j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n)$ and that $(\mathcal{L}, \phi)$ is the image of $\{f_{ij}\}_{ij}$ under the coboundary map $\prod_{i \neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n) \to H^1_{\text{ét}}(X, \mu_n)$. This proves the exactness at $H^1_{\text{ét}}(X, \mu_n)$.

Suppose now that $\prod_i (\mathcal{L}_i, \phi_i)$ in $\prod_i H^1_{\text{ét}}(X_i, \mu_n)$ is in the kernel of

$$\prod_i H^1_{\text{ét}}(X_i, \mu_n) \to \prod_{i \neq j} H^1_{\text{ét}}(X_i \cap X_j, \mu_n).$$

Then the image of $\prod_i (\mathcal{L}_i, \phi_i)$ in $\prod_{i \neq j} H^1_{\text{ét}}(X_i \cap X_j, \mu_n)$ is the product $\prod_{i \neq j} (\mathcal{L}_i \otimes \mathcal{L}_j^{-1}, \phi_i \otimes \overline{\phi}_j)$; here $\overline{\phi}_j$ denotes the isomorphism $\mathcal{L}_j^{\otimes -n} \cong \mathcal{O}_X$ obtained from ϕ_j. Hence we have that for all $i \neq j$ then $\mathcal{L}_i \otimes \mathcal{L}_j^{-1}$ is isomorphic to $\mathcal{O}_X$ on $X_i \cap X_j$; that is to say the restrictions of $\mathcal{L}_i$ and $\mathcal{L}_j$ to $X_i \cap X_j$ are isomorphic for all $i \neq j$. As this holds for all i, j there is then a locally free sheaf $\mathcal{L}$ of rank 1 on X whose restriction to X_i is isomorphic to $\mathcal{L}_i$ for all i; it follows easily that $\mathcal{L}^{\otimes n}$ is isomorphic to $\mathcal{O}_X$ on X and hence there is a pair $(\mathcal{L}, \phi)$ whose restriction to X_i is isomorphic to $(\mathcal{L}_i, \phi_i)$ for all i. □

A.5 The space Ω^d

(A.5.1) We have the following notation, as in §2.1 of the main text:

k is a finite field with $q = p^m$ elements;
C/k is an integral smooth 1-dimensional projective k-scheme, where k is the exact field of constants (a *curve*);
∞ is a closed point of C/k;
C_{aff} is the affine curve $C - \{\infty\}$;
A is the coordinate ring $H^0(C_{\text{aff}}, \mathcal{O}_{C_{\text{aff}}})$ of the affine curve C_{aff};
F is the fraction field of A (that is, the function field of C/k);
$\kappa(z)$, where z is a closed point of C, is the residue field at z.

(A.5.2) Let F_∞ be the completion of the field F at ∞; in this way, F_∞ is a local field of positive characteristic and containing F. Let $\overline{F}_\infty$ be the algebraic closure of F_∞. Let $\widehat{\overline{F}}_\infty$ be the completion of $\overline{F}_\infty$.

(A.5.3) Let

$$\Omega^d(\widehat{\overline{F}}_\infty) = \mathbb{P}_{d-1}(\widehat{\overline{F}}_\infty) \setminus \bigcup(F_\infty - \text{rational hyperplanes}).$$

That is to say, $\Omega^d(\widehat{\overline{F}}_\infty)$ is obtained from $\mathbb{P}_{d-1}(\widehat{\overline{F}}_\infty)$ by removing all hyperplanes which are rational over the subfield F_∞.

The subset Ω^d of $\mathbb{P}_{d-1}(\widehat{\overline{F}}_\infty)$ is open. Denoting a point of $\mathbb{P}_{d-1}(\widehat{\overline{F}}_\infty)$ by homogeneous coordinates $(x_1 : \ldots : x_n)$, the group $\mathrm{GL}_d(F_\infty)$ of invertible matrices $g = (a_{ij})$ with coefficients in F_∞ acts on Ω^d via the linear fractional transformations, for all $\omega \in \Omega^d$, $\omega = (\omega_1 : \ldots : \omega_d)$,

$$g.\omega = ((g\omega)_1 : \ldots : (g\omega)_d).$$

(A.5.4) Let

$$W^d = \{x \in \mathbb{A}_d(\widehat{\overline{F}}_\infty) \mid x \text{ is not contained in any hyperplane defined over } F_\infty\}.$$

The spaces W^d, Ω^d have a natural action of $\mathrm{GL}_d(F_\infty)$ as rigid analytic automorphisms.

Let $\mathbb{A}_f$ denote the ring of finite adèles, that is, the subring of the ring of adèles $\mathbb{A}$ without the component at ∞. We have $\mathbb{A}_f = \widehat{A} \otimes_A F$ where $\widehat{A}$ is the profinite completion of A.

A.5.5. Theorem. (Drinfeld) (i) *The spaces W^d, Ω^d are admissible open subsets of $\mathbb{A}_d, \mathbb{P}_{d-1}$, respectively.*
(ii) *The group $\mathrm{GL}_d(F_\infty)$ acts by rigid analytic automorphisms on W^d and Ω^d.*
(iii) *If $\Gamma \subseteq \mathrm{GL}_d(F_\infty)$ is a discrete subgroup then the quotients Ω^d/Γ and W^d/Γ have natural rigid analytic structures where the natural maps $\Omega^d \to \Omega^d/\Gamma$, $W^d \to W^d/\Gamma$ are rigid analytic morphisms.* □

A.6 The moduli scheme M_I^d

Let S be a locally noetherian A-scheme.

(A.6.1) A Drinfeld module of rank d over a locally noetherian scheme S is given by a pair $(G_\mathcal{L}, \phi)$ where $\mathcal{L}$ is a line bundle on S and ϕ is a k-algebra

homomorphism

$$\phi : A \to \mathrm{End}(G_{\mathcal{L}})$$

where $G_{\mathcal{L}}$ is the additive S-group scheme

$$G_{\mathcal{L}} = \mathbf{Spec}_{\mathcal{O}_S} \bigoplus_{n=0}^{\infty} \mathcal{L}^{\otimes n}.$$

This pair $(G_{\mathcal{L}}, \phi)$ further satisfies the conditions that if $a \in A$ and the cardinality of $A/(a)$ is equal to q^m, where $q = |k|$ and F is the Frobenius $x \mapsto x^q$, then

$$\phi(a) = aF^0 + \sum_{i=1}^{dm} \phi_i(a) F^i$$

and the section $\phi_{dm}(a)$ is nowhere zero.

(A.6.2) Let $(D_1, \phi_1), (D_2, \phi_2)$ be two Drinfeld modules over a locally noetherian scheme S. A *homomorphism* from D_1 to D_2 is a homomorphism of S-group schemes $f \in \mathrm{Hom}_S(G_{\mathcal{L}_1}, G_{\mathcal{L}_2})$ such that $f\phi_1 = \phi_2 f$.

(A.6.3) Let I be a non-zero ideal of A. A *full level I-structure* on the rank d Drinfeld module D/S is a finite flat subgroup-scheme Z/S of $G_{\mathcal{L}}/S$ and a homomorphism of A-modules

$$\psi : (I^{-1}/A)^d \to G_{\mathcal{L}}(S)$$

such that there is an equality of relative Cartier divisors

$$\sum_{m \in (I^{-1}/A)^d} \psi(m) = Z.$$

Note that $G_{\mathcal{L}}(S) = \Gamma(S, \mathcal{L})$; hence the image of the full level I-structure ψ lies in $\Gamma(S, \mathcal{L})$.

A.6.4. Theorem. (Drinfeld, [Dr1, Prop. 5.3], [DH, Chapter I, Theorem 6.2]) *Let I be a non-zero ideal of A such that the ring A/I contains at least two distinct maximal ideals. Then the functor on the category $A - \mathcal{S}ch$ of locally noetherian A-schemes given by*

$$\begin{aligned} A - \mathcal{S}ch &\to \mathcal{S}ets \\ S &\mapsto \left\{ \begin{array}{c} S - \text{ isomorphism classes of pairs } (D, Z) \text{ where } D/S \\ \text{is a Drinfeld module of rank } d \text{ and } Z/S \text{ is a} \\ \text{full level } I - \text{structure on } D \end{array} \right\} \end{aligned}$$

is representable by a scheme M_I^d of finite type over Spec A *and of relative dimension $d - 1$.* □

Compactification of M_I^2

(A.6.5) For the case where $d = 2$, the moduli scheme M_I^2 admits a compactification as described in the next theorem.

A.6.6. Theorem. (Drinfeld, [Dr1, Prop.9.3]) *The modular surface M_I^2 can be compactified into a smooth surface $\overline{M}_I^2/k$ containing M_I^2 as an open everywhere dense subscheme such that the morphism $M_I^2 \to$ Spec A extends to a proper smooth morphism $\overline{M}_I^2/k \to$ Spec A and $\overline{M}_I^2 \setminus M_I^2$ is finite over Spec A.* □

(A.6.7) If $J \subset I$ is an ideal of A contained in I then we have a transition morphism

$$M_J^d \to M_I^d.$$

Set

$$M^d = \varprojlim M_I^d$$

where the limit is over all non-zero ideals I of A such that A/I has at least two maximal ideals.

The compactification $\bar{M}_I^2$ of M_I^2 (theorem A.6.6) is compatible with the transition morphisms $M_J^2 \to M_I^2$, where $J \subset I$, and one puts

$$\bar{M}^2 = \varprojlim \bar{M}_I^2.$$

Action of $\mathrm{GL}(d, \mathbb{A}_f)/F^*$ *on* M^d

(A.6.8) Let $\mathbb{A}_f$ denote the ring of finite adèles, as in (A.5.4). Then $F^*\backslash\mathrm{GL}(d, \mathbb{A}_f)$ acts on M^d; the action is described in this way.

Let D/S be a Drinfeld module of rank d represented by the pair $(\mathcal{L}, \psi)$. Let $G_{\mathcal{L}}$ be the additive S-group scheme associated to $\mathcal{L}$ (see (A.6.1)). Let

$$\phi : (F/A)^d \to G_{\mathcal{L}}(S)$$

be a homomorphism of A-modules such that for each non-zero ideal I of A the restriction of ϕ to $(I^{-1}/A)^d$ is a full level I-structure. Let $g \in \mathrm{GL}(d, \mathbb{A}_f)$ be a matrix with coefficients in $\widehat{A}$, where $\widehat{A}$ is the profinite completion of A. Then g can be considered as an endomorphism of $(F/A)^d$. Its kernel P is a finite A-module. The divisor

$$H = \sum_{a \in P} [\phi(a)]$$

is then an A-invariant subgroup scheme of $G_{\mathcal{L}}$ and the quotient D/H is a Drinfeld module over S of rank d represented by a pair $(\mathcal{L}_1, \psi_1)$, say. Let $G_{\mathcal{L}_1}$ be the additive S-group scheme associated to $\mathcal{L}_1$. We may then define a homomorphism of A-modules $\phi_1 : (F/A)^d \to G_{\mathcal{L}_1}$ so that we have a commutative diagram

$$\begin{array}{ccc} & \overset{\phi}{} & \\ (F/A)^d & \to & G_{\mathcal{L}} \\ g \downarrow & & \downarrow \\ (F/A)^d & \to & G_{\mathcal{L}_1} \\ & \underset{\phi_1}{} & \end{array}$$

We have that for any non-zero ideal I the restriction of ϕ_1 to $(I^{-1}/A)^d$ is a full level I-structure. This defines the action on M^d of matrices in $\mathrm{GL}(2, \mathbb{A}_f)$ whose coefficients are in $\widehat{A}$. The diagonal elements of $\mathrm{GL}(2, \mathbb{A}_f)$ with coefficients in A act trivially on M^d hence we finally obtain an action of $\mathrm{GL}(2, \mathbb{A}_f)/F^*$ on M^d. This gives the first part of the next theorem A.6.9

For the case where $d = 2$, the action of $\mathrm{GL}(2, \mathbb{A}_f)/F^*$ on M^2 extends to an action on the compactification $\bar{M}^2$.

A.6.9. Theorem. (Drinfeld) (i) *There is a left action of* $\mathrm{GL}_d(\mathbb{A}_f)/F^*$ *on* M^d. (ii) *Let* $\tilde{U}_I$ *be the kernel of the natural map* $\mathrm{GL}_d(\widehat{A}) \to \mathrm{GL}_d(\widehat{A}/I\widehat{A})$. *Then we have* $\tilde{U}_I \backslash M^d = M_I^d$. □

A.7 An analytic description of M_I^d

(A.7.1) Let L be a finite extension field of F_∞, the completion of F at ∞. Let L^{sep} be the separable closure of L. A *lattice* over L is a finitely generated discrete A-submodule Λ of L^{sep} invariant with respect to $\mathrm{Gal}(L^{\mathrm{sep}}/L)$. The *rank* of a lattice Λ is the dimension of the F-vector space $\Lambda \otimes_A F$.

For 2 lattices Λ_1, Λ_2 over L of rank d, a *morphism* from Λ_1 to Λ_2 is an element $\alpha \in L$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$. Composition of morphisms is obtained by multiplication by elements of L.

(A.7.2) Let Λ be a lattice of rank d over L. Put

$$e_\Lambda(z) = z \prod_{\lambda \in \Lambda, \lambda \neq 0} \left(1 - \frac{z}{\lambda}\right).$$

Then e_Λ is an entire function on $\overline{L}$, the algebraic closure of L, and is called the *exponential function* associated to the lattice Λ.

(A.7.3) This function e_Λ has an expansion of the form, where $c_n \in L$ for all n,

$$e_\Lambda(z) = \sum_{n=0}^{\infty} c_n z^{q^n}$$

and is a surjective additive k-linear homomorphism $\overline{L} \to \overline{L}$ with kernel equal to Λ. It induces an isomorphism of rigid analytic spaces $\overline{L}/\Lambda \cong \overline{L}$. The resulting composite homomorphism $\phi : A \to \overline{L} \to \overline{L}/\Lambda \cong \overline{L}$ where the first map is the natural inclusion, the second is the quotient map by Λ, is then a Drinfeld module $D(\Lambda)$ of rank d over L.

This construction $\Lambda \to D(\Lambda)$ then gives rise to the equivalence of categories of the next theorem A.7.4.

A.7.4. Theorem. (Drinfeld, [Dr1, Prop. 3.1]) *The category of Drinfeld modules of rank d over L is isomorphic to the category of lattices of rank d over L.* □

(A.7.5) Take $\mathbb{A}_f$ to be a discrete set and put

$$\tilde{\Omega}^d = (\mathrm{GL}_d(\mathbb{A}_f) \times \Omega^d)/\mathrm{GL}_d(F)$$

$$\tilde{W}^d = (\mathrm{GL}_d(\mathbb{A}_f) \times W^d)/\mathrm{GL}_d(F).$$

(A.7.6) The isomorphism classes of rank d projective A-modules are represented by direct sums $\bigoplus_{i=1}^d I_i$ where I_i are fractionary ideals of A. Let $\mathrm{Pic}^d(A)$ denote the set of isomorphism classes of rank d projective A-modules.

(A.7.7) We have isomorphisms, where $\tilde{U}_I$ is as in theorem A.6.9,

$$\tilde{U}_I \backslash \tilde{\Omega}^d = \bigcup_{Y \in \mathrm{Pic}^d(A)} \mathrm{GL}(Y) \backslash (\Omega^d \times \mathrm{GL}_d(Y/IY))$$

$$\tilde{U}_I \backslash \tilde{W}^d = \bigcup_{Y \in \mathrm{Pic}^d(A)} \mathrm{GL}(Y) \backslash (W^d \times \mathrm{GL}_d(Y/IY)).$$

The sets $\tilde{U}_I \backslash \tilde{\Omega}^d$ and $\tilde{U}_I \backslash \tilde{W}^d$ are then disjoint unions of rigid spaces of the form $\mathrm{GL}(Y) \backslash \Omega^d$ and $\mathrm{GL}(Y) \backslash W^d$. These images of $\mathrm{GL}(Y) \backslash \Omega^d$, $\mathrm{GL}(Y) \backslash W^d$ in the above decompositions are called the *components*.

A.7.8. Remark. The quotients $\tilde{U}_I \backslash \tilde{\Omega}^d$ and $\tilde{U}_I \backslash \tilde{W}^d$ are rigid analytic spaces associated to the moduli scheme M_I^d of rank d Drinfeld modules with level I structure (see theorem A.8.7).

A.8 Rigid analytic modular forms

In this section we define rigid analytic modular forms. These were first defined by Goss [Go2]. They are modular forms associated to Drinfeld modules and with values in algebras of finite characteristic.

(A.8.1) Let $w \in \mathbb{Z}$. Let R be a noetherian A-algebra. A *modular form* over R of rank d weight w is a rule $\mathcal{F}$ which to each Drinfeld module $D = (G_{\mathcal{L}}, \phi)$ of rank d defined over a locally noetherian R-scheme S assigns a section

$$\mathcal{F}(D) \in \Gamma(S, \mathcal{L}^{-\otimes w})$$

which satisfies the two conditions for any morphism of locally noetherian R-schemes $g : S' \to S$:

(a) We have $\mathcal{F}(g^*D) = g^*\mathcal{F}(D)$.

(b) Suppose over S' there is a nowhere vanishing section α of $g^*\mathcal{L}$. Then the element

$$\mathcal{F}(g^*D).\alpha^{\otimes w} \in \Gamma(S', \mathcal{O}_{S'})$$

depends only on the S'-isomorphism class of (D, α).

A.8.2. Remarks. (1) Modular forms may be defined on the category of Drinfeld modules of rank d equipped with supplementary structures.

For example, let I be a non-zero ideal of A. A modular form $\mathcal{F}$ of full level I and weight w is defined in the same way except that $\mathcal{F}$ is a rule on pairs (D, ψ) where D is a Drinfeld module of rank d and equipped with a full level I-structure ψ.

Similarly, for modular forms of rank 2 and weight w defined on pairs (D, Z) where Z is an I-cyclic subgroup of D (see definition 2.4.2).

(2) A modular form satisfying the previous definition is more precisely called an *algebraic modular form*, to distinguish it from the analytic modular forms defined in §A.9.

A.8.3. Examples. (1) Let $a \in A$. With the notation of (A.6.1), then $\phi_i(a)$ is a form of weight $q^i - 1$.
(2) Let ψ be a full level I-structure on any Drinfeld D/S module of rank d. Then by definition ψ is a homomorphism of A-modules (see (A.6.3))

$$\psi : (I^{-1}/A)^d \to G_{\mathcal{L}}(S) = \Gamma(S, \mathcal{L}).$$

satisfying the conditions of the full level I-structure. Let α be a non-zero element of $(I^{-1}/A)^d$. Then $\psi(\alpha)$, as (D, ψ) varies, is a modular form of weight -1 and level I.
(3) Eisenstein series provide examples of modular forms (see §A.11).

A.8.4. Definition. Let H^d be the graded ring of modular forms of rank d over A. Let H^d_I be the graded ring of modular forms of rank d and level I over A.

A.8.5. Theorem. (Goss, [Go2, Theorem 1.18]) (i) *The scheme* Spec H^d *represents isomorphism classes of pairs* (D, ω) *where* $D = (G_{\mathcal{L}}, \phi)$ *is a Drinfeld module of rank* d *and* ω *is a nowhere vanishing section of* $\mathcal{L}$.
(ii) *Assume that* A/I *has at least two elements. The scheme* Spec H^d_I *represents isomorphism classes of triples* (D, ω, ψ) *where* $D = (G_{\mathcal{L}}, \phi)$ *is a Drinfeld module of rank* d *and* ω *is a nowhere vanishing section of* $\mathcal{L}$ *and where* ψ *is a full level* I*-structure on* D. □

A.8.6. Remarks. (1) The natural map Spec $H^d_I \to M^d_I$ is a principal $\mathbb{G}_m$-bundle.
(2) The rings H^d_I, H^d are regular finitely generated k-algebras of dimension $d+1$. As A-algebras they are flat and are smooth away from Spec A/I (see [Go2, Theorem 1.21]).

A.8.7. Theorem. (Drinfeld, Goss, [Go2, Theorem 1.39]) *Assume that* A/I *has at least two maximal ideals. Then there are isomorphisms of rigid analytic spaces*

$$\tilde{U}_I \backslash \tilde{\Omega}^d = (M^d_I \otimes F_\infty)_{\mathrm{an}}$$
$$\tilde{U}_I \backslash \tilde{W}^d = (\mathrm{Spec}(H^d_I) \otimes F_\infty)_{\mathrm{an}}. \ \square$$

A.9 Analytic modular forms

(A.9.1) Let Ω^d, W^d be as in §A.5. The spaces W^d, Ω^d have a natural action of $\mathrm{GL}_d(F)$ as rigid analytic automorphisms. As in (A.5.4), let $\mathbb{A}_f$ denote the ring of finite adèles, that is, the subring of the ring of adèles $\mathbb{A}$ without the component at ∞.

A.9.2. Theorem. (Goss) *Let* $\mathcal{F}$ *be a modular form of rank* d*, full level* I *and weight* w *defined over a finite extension field* K *of* F_∞*. Then* $\mathcal{F}$ *gives rise to a rigid analytic function* f *on* $\tilde{W}^d$ *defined over* K*. On each component we have* $f(cx) = c^{-w} f(x)$ *for all* $x \in W^d$ *and* $c \in \overline{F}^*_\infty$.

[This follows immediately from theorem A.8.7.] □

(A.9.3) For any projective A-module Y of rank d, put

$$\Gamma_Y = \mathrm{GL}(Y)$$

and

$$\Gamma_Y(I) = \ker(\mathrm{GL}(Y) \to \mathrm{GL}(Y/IY)).$$

Recall that we have (see (A.7.7))

$$\tilde{U}_I \backslash \tilde{W}^d = \bigcup_{Y \in \mathrm{Pic}^d(A)} \mathrm{GL}(Y) \backslash (W^d \times \mathrm{GL}_d(Y/IY)).$$

In particular, a rigid analytic function on $\tilde{U}_I \backslash \tilde{W}^d$ has a restriction to each component $\Gamma_Y(I) \backslash W^d$. for every projective A-module Y of rank d.

(A.9.4) Let $f : \tilde{W}^d \to \widehat{\overline{F}}_\infty$ be the rigid analytic function associated to the modular form $\mathcal{F}$ of rank d, full level I and weight w defined over a finite extension field K of F_∞.

Let f also denote the restriction of f to a component Ω^d by sending $x \in \Omega^d$ to $(x, 1) \in W^d$ and where the component is associated to the projective A-module Y of rank d.

Let $g \in \Gamma_Y(I)$ and let

$$g^t = \begin{pmatrix} G & b \\ c & d \end{pmatrix}$$

where G is a $d-1 \times d-1$-minor and d is a scalar. Then we have, where the dot notation is the scalar product,

$$f\left(\frac{xG + b^t}{x.c^t + d}\right) = f(x)(x.c^t + d)^w.$$

A.9.5. Definition. A rigid function $f : W^d \to \widehat{\overline{F}}_\infty$ satisfying the above transformation property of (A.9.4) is said to be an *analytic modular form* of level I, weight w and type Y.

In the particular case of rank 2, a rigid analytic modular form f of weight w, level I and type Y satisfies the transformation property for all $g \in \Gamma_Y(I)$ and where

$$g^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we have

$$f\left(\frac{ax + b}{cx + d}\right) = f(x)(cx + d)^w.$$

A.9.6. Remark. Analytic modular forms $f : W^d \to \widehat{\overline{F}}_\infty$ may be defined similarly for any discrete group of finite index Γ of $\mathrm{GL}(Y)$.

A.10 q-expansions at the cusps of $\overline{M}_I^2$

(A.10.1) Let I be a non-zero ideal of A such that A/I has at least two maximal ideals. By theorem A.8.7 and (A.7.7) we have for $d = 2$ an isomorphism of

rigid analytic spaces

$$(M_I^2 \otimes F_\infty)_{\mathrm{an}} = \bigcup_{Y \in \mathrm{Pic}^2(A)} \mathrm{GL}(Y) \backslash (\Omega^d \times \mathrm{GL}_2(Y/IY)).$$

(A.10.2) Let Y be a projective A-module of rank 2. The rigid analytic space $\Gamma_Y(I)\backslash\Omega^2$ is the analytification of a smooth connected affine curve over F_∞. This affine curve has a natural compactification to a smooth projective curve which is obtained by adding a finite set of points called the *cusps*.

More generally for any discrete subgroup of finite index Γ of $\mathrm{GL}_2(Y)$, the rigid analytic space $\Gamma\backslash\Omega^2$ is the analytification of a smooth connected affine curve over F_∞ which can be compactified by the addition of a finite set of cusps.

A.10.3. Theorem. *The cusps of $\Gamma\backslash\Omega^2$ are in bijection with the elements of $\Gamma\backslash\mathbb{P}_1(F)$. In particular, the cusps of $\mathrm{GL}_2(Y)\backslash\Omega^2$ are in bijection with* $\mathrm{Pic}(A)$. □

[For more details see [Go2, Prop. 1.78] and [PT]; see also definition B.5.14(2) and theorem B.5.18 of Appendix B].

A.10.4. Remark. A point of $\mathbb{P}_1(F)$ represents a 1-dimensional subspace over F of F^2. This line then induces a *cusp* (or an *end*) of the Bruhat-Tits building T associated to F with respect to the valuation at ∞ (see §B.5 of Appendix B).

The above theorem A.10.3 is then equivalent to the assertion that the cusps of the quotient $\Gamma\backslash T$ are in bijection with the elements of $\Gamma\backslash\mathbb{P}_1(F)$. For the case where Γ is the group $\mathrm{GL}_2(Y)$ this is proved in theorem B.5.18(i) of Appendix B.

(A.10.5) Let Y be a projective A-module of rank 2. Let $\alpha \in \mathbb{P}_1(F)$ so that α corresponds to a cusp of $\Gamma_Y(I)\backslash\Omega^2$. Select an element $\rho_\alpha \in \mathrm{SL}_2(F)$ such that

$$\rho_\alpha(\alpha) = \infty.$$

(A.10.6) Let $\Gamma_\alpha \subseteq \Gamma_Y(I)$ be the stabilizer of α, where $\Gamma_Y(I)$ is as in (A.9.3). Then $\rho_\alpha \Gamma_\alpha \rho_\alpha^{-1}$ is the group of translations by a fractional ideal C_α of A (for the proof see [Go2, Prop. 1.69]).

A.10.7. Definition. Put

$$e_\alpha(z) = z \prod_{\beta \in C_\alpha,\ \beta \neq 0} (1 - z/\beta) \text{ and } q_\alpha = 1/e_\alpha.$$

A.10.8. Theorem. (Goss, [Go2, Theorem 1.76]) *At the cusp α of $\Gamma_Y(I)\backslash\Omega^2$, q_α is an analytic local parameter.* □

(A.10.9) Let f be an analytic modular form of level I, weight w, and type Y (definition A.9.5). If

$$\rho_\alpha^{-1}(z) = \frac{az+b}{cz+d} \text{ for all } z$$

then

$$\frac{f(\rho_\alpha^{-1}(z))}{(cz+d)^w}$$

determines an analytic germ

$$\sum_{-\infty<n<+\infty} a_n q_\infty^n$$

by theorem A.10.8 where q_∞ is the analytic local parameter at ∞.

The series $\sum_{-\infty<n<+\infty} a_n q_\infty^n$ is the *analytic q-expansion* at the cusp α of f.

A.10.10. Theorem. (Goss, [Go2, Theorem 1.79]) (i) *An analytic modular form of level I, weight w, and type Y is an algebraic modular form (see (A.8.1)) if and only if at each cusp the q-expansion is finite tailed.*
(ii) *The space of analytic modular forms of full level I, weight w, type Y, and holomorphic at the cusps, is finite dimensional over $\widehat{\overline{F}}_\infty$* □

A.11 Eisenstein series

(A.11.1) Let L be a finite extension field of F_∞, the completion of F at ∞. Let L^{sep} be the separable closure of L. Let Λ be a lattice over L of rank d, that is to say Λ is a finitely generated discrete A-submodule Λ of L^{sep} invariant with respect to $\text{Gal}(L^{\text{sep}}/L)$ (see (A.7.1)).

(A.11.2) For any positive integer $j \in \mathbb{N} \setminus \{0\}$, the *Eisenstein series* $E^j(\Lambda)$ is the element of L given by

$$E^j(\Lambda) = \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \lambda^{-j}.$$

Suppose that Λ is equipped with a full level I-structure, where I is a non-zero ideal of A; that is to say, there is an isomorphism of A-modules

$$\Psi : (I^{-1}/A)^d \cong I^{-1}\Lambda/\Lambda.$$

Let x be an element of $(I^{-1}/A)^d$. The *Eisenstein series* $E^j_{x,I}(\Lambda)$ is the element

of L^{sep} given by

$$E^j_{x,I}(\Lambda) = \sum_{\substack{\alpha \in I^{-1}\Lambda,\ \alpha \neq 0 \\ \alpha \equiv \Psi(x) \pmod{\Lambda}}} \alpha^{-j}.$$

A.11.3. Examples. (1) Let Y be a projective A-module of rank 2 which is a submodule of $\widehat{\overline{F}}_\infty$. Then Y is isomorphic to $I_1 \oplus I_2$ where I_1, I_2 are invertible ideals of the Dedekind domain A. For all $z \in \Omega^2(\widehat{\overline{F}}_\infty)$ we have

$$E^j(I_1 z + I_2) = \sum_{\substack{(c_1,c_2) \in Y \\ (c_1,c_2) \neq 0}} (c_1 z + c_2)^{-j}.$$

By multiplying $I_1 z + I_2$ by elements of k^*, it is evident that $E^j(I_1 z + I_2)$ is zero unless the weight j is divisible by $|k| - 1$. Furthermore, $z \mapsto E^j(I_1 z + I_2)$ is then a function $\Omega^2 \to \widehat{\overline{F}}_\infty$ which evidently satisfies the transformation property of (A.9.4), that is to say for all $g \in \Gamma_Y(I)$ where

$$g^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we have

$$f\left(\frac{ax+b}{cx+d}\right) = f(x)(cx+d)^j.$$

(2) More generally, let $I_1, \ldots, I_d$ be invertible ideals of A. and let $Y = \bigoplus_{i=1}^d I_i$. Let $w = (w_1, \ldots, w_d) \in W^d$. Then $\Lambda(w) = \sum_i I_i w_i$ is also a lattice in $\widehat{\overline{F}}_\infty$ and is isomorphic to Y as an A-module. Suppose that there is given an isomorphism of A-modules

$$\Psi : (I^{-1}/A)^d \cong I^{-1}Y/Y.$$

That is to say, Ψ is a full level I-structure on Y. By composing Ψ with the natural isomorphism $I^{-1}\Lambda/\Lambda \cong I^{-1}\Lambda(w)/\Lambda(w)$, the isomorphism Ψ induces a full level I-structure on $\Lambda(w)$

$$\Psi(x) : (I^{-1}/A)^d \cong I^{-1}\Lambda(w)/\Lambda(w).$$

For any element x of $(I^{-1}/A)^d$, we have the Eisenstein series, $E^j(\Lambda(w))$ and $E^j_{x,I}(\Lambda(w))$; these series as functions of w are then defined on W^d.

A.11.4. Proposition. ([Go2, Theorem 2.3, Corollary 2.4]) *The functions $w \mapsto E^j(\Lambda(w))$ and $w \mapsto E^j_{x,I}(\Lambda(w))$ are rigid analytic on W^d and are rigid analytic modular forms of weight j, type Y, for the groups Γ_Y and $\Gamma_Y(I)$, respectively.* □

A.11.5. Remark. It may be shown (see [Go2]) that the functions $w \mapsto E^j(\Lambda(w))$ and $w \mapsto E^j_{x,I}(\Lambda(w))$ are algebraic modular forms in the sense of (A.8.1) and are holomorphic at the cusps.

A.12 Hecke operators

(A.12.1) Let Λ be a lattice in $\widehat{\overline{F}}_\infty$ of rank d, that is to say Λ is a finitely generated discrete A-submodule of $\widehat{\overline{F}}_\infty$ (note the difference of this definition with that of (A.7.1)).

(A.12.2) Let z be a closed point of the affine curve C_{aff}/k. Let $\mathfrak{m}_z$ be the maximal ideal of A corresponding to the point z. The *Hecke operator* T_z is then defined on the set of rank d lattices in $\widehat{\overline{F}}_\infty$ by

$$T_z(\Lambda) = \sum_{\Lambda' \supset \Lambda} \Lambda'$$

here the right hand side here is a formal sum of A-lattices Λ' of rank d in $\widehat{\overline{F}}_\infty$ such that there is an isomorphism of A-modules

$$\frac{\Lambda'}{\Lambda} \cong \frac{A}{\mathfrak{m}_z}.$$

(A.12.3) Suppose that Λ is equipped with a full level I structure, that is to say, there is an isomorphism of A-modules

$$\Psi : (I^{-1}/A)^d \cong I^{-1}\Lambda/\Lambda.$$

Let Λ' be an A-lattice of F^{sep} containing Λ and such that there is an isomorphism of A-modules $\Lambda'/\Lambda \cong A/\mathfrak{m}_z$. If z is prime to A/I then the inclusion $\Lambda \subset \Lambda'$ gives rise to an isomorphism of A-modules

$$I^{-1}\Lambda/\Lambda \cong I^{-1}\Lambda'/\Lambda'.$$

Hence Ψ lifts to a full level I-structure $\Psi' : (I^{-1}/A)^d \cong I^{-1}\Lambda'/\Lambda'$ on Λ'.

The Hecke operator T_z is then defined on the set of pairs (Λ, Ψ) where Λ is an A-lattice equipped with a full level I-structure Ψ; we have

$$T_z(\Lambda, \Psi) = \sum_{\Lambda' \supset \Lambda} (\Lambda', \Psi')$$

here the right hand side here is a formal sum of pairs (Λ', Ψ') where Λ' is an

A-lattice of rank d in L^{sep} such that there is an isomorphism of A-modules

$$\frac{\Lambda'}{\Lambda} \cong \frac{A}{\mathfrak{m}_z}$$

and Ψ' is a full level I-structure on Λ' which lifts Ψ.

(A.12.4) Let $\mathcal{F}$ be a modular form of rank d and weight w, and of full level I. Let f be the rigid analytic function on $\tilde{W}^d$ with values in $\widehat{\overline{F}}_\infty$ associated to the modular form $\mathcal{F}$ (theorem A.9.2).

Let $I_1, \ldots, I_d$ be invertible ideals of A. and let $Y = \bigoplus_{i=1}^d I_i$. Let $w = (w_1, \ldots, w_d) \in W^d$. Then $\Lambda(w) = \sum_i I_i w_i$ is also a lattice in $\widehat{\overline{F}}_\infty$ and is isomorpic to Y as an A-module. Suppose that there is given an isomorphism of A-modules

$$\Psi : (I^{-1}/A)^d \cong I^{-1}Y/Y.$$

That is to say, Ψ is a full level I-structure on Y. By composing Ψ with the natural isomorphism $I^{-1}\Lambda/\Lambda \cong I^{-1}\Lambda(w)/\Lambda(w)$, the isomorphism Ψ induces a full level I-structure on $\Lambda(w)$

$$\Psi(w) : (I^{-1}/A)^d \cong I^{-1}\Lambda(w)/\Lambda(w).$$

Assume that Y is equipped with a full level I-structure for each representative Y of the elements of $\mathrm{Pic}^d(A)$. We then define $T_z f$ via the formula: let $\Lambda(w)$, where $w \in W^d$, be a lattice isomorphic to Y. Put

$$(T_z f)(\Lambda(w), \Psi) = \sum_{\Lambda' \supset \Lambda(w)} f(\Lambda', \Psi')$$

where the right hand side here is a sum of pairs (Λ', Ψ') such that Λ' is an A-lattice of rank d in $\widehat{\overline{F}}_\infty$ equipped with an isomorphism of A-modules

$$\frac{\Lambda'}{\Lambda} \cong \frac{A}{\mathfrak{m}_z}.$$

and Ψ' is a full level I-structure on Λ' which lifts Ψ.

A.12.5. Remark. Let I be a non-zero ideal of A. Let $\widehat{A}$ be the profinite completion of A and let $\Gamma_0(I)$ be the compact open subgroup of finite index of $\mathrm{GL}_2(\widehat{A})$ of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \in I\widehat{A}$. Then $\Gamma_0(I)$ is an arithmetic subgroup of $\mathrm{GL}_2(\widehat{A})$ as it contains $\tilde{U}_I$ (definition B.4.7).

Let $\mathcal{F}$ be a modular form of rank 2 and weight w, with respect to the subgroup $\Gamma_0(I)$; that is to say an algebraic modular form of weight w on Drinfeld modules of rank 2 equipped with an I-cyclic structure (see remarks A.8.2(1), and (B.11.14) of Appendix B).

Let f be the rigid analytic function on $\tilde{W}^2$ with values in $\widehat{\overline{F}}_\infty$ associated to the modular form $\mathcal{F}$.

Let I_1, I_2 be invertible ideals of A. and let $Y = \bigoplus_{i=1}^2 I_i$. Let $w = (w_1, w_2) \in W^2$. Then $\Lambda(w) = \sum_i I_i w_i$ is also a lattice in $\widehat{\overline{F}}_\infty$ and is isomorpic to Y as an A-module. Suppose that there is given an isomorphism of A-modules

$$\Psi : I^{-1}/A \cong Y'/Y.$$

That is to say, Ψ is an I-cyclic structure on Y. By composing Ψ with the natural isomorphism $I^{-1}\Lambda/\Lambda \cong I^{-1}\Lambda(w)/\Lambda(w)$, the isomorphism Ψ induces a Hecke level I-structure on $\Lambda(w)$

$$\Psi(w) : I^{-1}/A \cong \Lambda'(w)/\Lambda(w).$$

Assume that Y is equipped with an I-cyclic structure for each representative Y of the finitely many elements of $\mathrm{Pic}^2(A)$. We then define $T_z f$ for z prime to Spec A/I via the formula: let $\Lambda(w)$, where $w \in W^2$, be a lattice isomorphic to Y. Put

$$(T_z f)(\Lambda(w), \Psi) = \sum_{\Lambda' \supset \Lambda(w)} f(\Lambda', \Psi')$$

where the right hand side here is a sum of pairs (Λ', Ψ') such that Λ' is an A-lattice of rank d in $\widehat{\overline{F}}_\infty$ equipped with an isomorphism of A-modules

$$\frac{\Lambda'}{\Lambda} \cong \frac{A}{\mathfrak{m}_z}.$$

and Ψ' is an I-cyclic structure on Λ' which lifts Ψ.

A.13 Elliptic curves over F and modular forms

(A.13.1) Let E/F be an elliptic curve with split multiplicative reduction at ∞. Let I, which is an ideal of A, be the conductor of E without the component at ∞. Then there is a finite surjective morphism of F-schemes (theorem 4.7.1; see also theorem B.11.17 of Appendix B).

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

(A.13.2) Let l be a prime number different from the characteristic of F. Let $T_l(E)$ be the l-adic Tate module of E equipped with its action by the Galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{End}_{\mathbb{Z}_l}(T_l(E)).$$

For z a place of F we write a_z for the trace of a Frobenius above z

$$a_z = \mathrm{Tr}(\rho(\mathrm{Frob}_z)|T_l(E)^{I_z})$$

where I_z denotes an inertia subgroup of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ over z and Frob_z denotes a corresponding Frobenius element above z. We then have (see examples 5.3.18(1))

$$a_z = |E_z(\kappa(z))| - 1 - |\kappa(z)|$$

where E_z denotes the closed fibre above z of the Néron model of E.

(A.13.3) The curve $X_0^{\mathrm{Drin}}(I)/F$ admits the analytic parametrisation over $\widehat{\overline{F}}_\infty$

$$\Gamma_0(I)\backslash\tilde{\Omega}^2 \to X_0^{\mathrm{Drin}}(I)(\widehat{\overline{F}}_\infty).$$

where $\Gamma_0(I)$ is the arithmetic subgroup of $\mathrm{GL}_2(\widehat{A})$ of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \in I\widehat{A}$ (see also (B.11.14) of Appendix B).

Let K be the canonical line bundle on E and let $\omega \in \Gamma(E, K)$ where $\omega \neq 0$; that is to say, ω is a non-zero differential on E and is uniquely determined up to multiplication by a scalar. Then $\psi^*\omega$ is a rigid analytic modular form on $\tilde{\Omega}^2$ with respect to the arithmetic subgroup $\Gamma_0(I)$ of $\mathrm{GL}_2(\widehat{A})$.

(A.13.4) The Hecke correspondances T_z for all closed points $z \neq \infty$ of C disjoint from Spec A/I are defined in (4.5.2) and in §A.12 on the curve $X_0^{\mathrm{Drin}}(I)$; we have that T_z acts on the elliptic curve E by multiplication by a_z for all closed points $z \neq \infty$ of C disjoint from Spec A/I (theorem 4.5.7 "Eichler-Shimura congruence"). We then obtain that T_z acts on the space of differentials $\Gamma(E, K)$ by multiplication by a_z modulo p, where p is the characteristicof F. The integer a_z satisfies the congruence

$$a_z \equiv |E_z(\kappa(z))| - 1 \pmod{p}.$$

We then have that T_z acts as multiplication by a_z on the rigid analytic modular form $\psi^*\omega$ for all z disjoint from Spec A/I and ∞. The following theorem is then an immediate consequence.

A.13.5. Theorem. *The rigid analytic modular form $\psi^*\omega$ is an eigenvector of the Hecke operators T_z for all z disjoint from Spec A/I and ∞ and the corresponding eigenvalues are the reductions modulo p of the traces a_z of the Frobenius elements for all such z.* □

[This result is given in [Br2, Theorem 4.1] for the case where F is the rational field $\mathbb{F}_q(T)$.]

Appendix B

Automorphic forms and elliptic curves over function fields

In this appendix Drinfeld's proof is given for GL_2 of global fields of positive characteristic of the Langland's conjecture for automorphic representations and galois representations which are special at ∞; furthermore, we give the application of this to elliptic curves over function fields, that is to say the analogue for function fields of the Shimura-Taniyama-Weil conjecture (see §B.11 and theorem 4.7.1 in the main text).

In the final part, we briefly state the generalisation of Drinfeld's work to the Langlands conjecture for GL_n by Lafforgue [La].

[The proof given in appendices A and B of the main theorem B.9.4 is complete except that the existence of the moduli schemes M_I^2 (theorem A.6.4) and their analytic description (theorems A.7.4 and A.8.7) are assumed. For proofs of these results on the moduli schemes M_I^2, see [Dr1] or [DH].]

B.1 The Bruhat-Tits building for PGL over a local field

(B.1.1) Let L be a non-archimedean local field with discrete valuation ring R. Let $|.|$ be the absolute value on L normalised so that $|\pi| = q^{-1}$ where π is a local parameter of R and q is the cardinality of the residue field of R.

Let V be a finite dimensional vector space over L.

A *norm* on V is a map $\alpha : V \to \mathbb{R}$ such that

(i) $\alpha(x) \geq 0$ for all $x \in V$ and $\alpha(x) = 0$ if and only if $x = 0$;
(ii) $\alpha(x + y) \leq \max(\alpha(x), \alpha(y))$ for $x, y \in V$;
(iii) $\alpha(ax) = |a|\alpha(x)$ for all $a \in L$ and all $x \in V$.

The properties (i) and (ii) say that $d(x, y) = \alpha(x-y)$ is an *ultrametric distance* on V.

(B.1.2) If α is a norm then the dialation $t\alpha$ is a norm for any real number $t > 0$. Let $N(V)$ denote the set of dialation classes of norms on V.

(B.1.3) We write $\alpha(V)$ for the set of values taken by the norm α on V. A norm α is *integral* if for some real number $t > 0$ then $t\alpha(V) \subseteq q^{\mathbb{Z}} \cup \{0\}$.

In the same way, a norm α is *rational* if for some real number $t > 0$ then $t\alpha(V) \subseteq q^{\mathbb{Q}} \cup \{0\}$.

Let Λ be an R-lattice of V (that is to say, Λ is a noetherian R-submodule of V which generates V as an L-vector space). Define

$$\alpha_\Lambda(x) = \inf\{1/|a| \mid ax \in \Lambda\}.$$

Then α_Λ is an integral norm on V (exercise B.1.9(2)). Furthermore, a norm α is in the dialation class of such a norm α_Λ constructed from a lattice Λ if and only if α is integral norm (exercise B.1.9(3)).

(B.1.4) Let $\mathrm{PGL}(V)$ denote $\mathrm{GL}(V)/L^*$. The *Bruhat-Tits building* $I(V)$ for the group $\mathrm{PGL}(V)$ over L is the simplicial complex whose vertices are the dialation classes $[\Lambda]$ of lattices Λ in V and whose simplices are sets of vertices $(v_0, \ldots, v_n)$ where up to permutation of the indices $v_i = [\Lambda(i)]$ there is a chain

$$\Lambda(0) \supset \Lambda(1) \supset \ldots \supset \pi\Lambda(0)$$

of strict inclusions. The group $\mathrm{GL}(V)$ acts as a group of automorphisms of the building $I(V)$.

[For the case of $\mathrm{SL}_2(L)$ see §3.1. For details on the apartments of this building $I(V)$ and the associated Tits system, see [Bro2].]

(B.1.5) The *geometric realisation* of the Bruhat-Tits building $I(V)_{\mathbb{R}}$ is the subset of elements $(t_v)_v$ of

$$\prod_{v \in \mathrm{vert}(I(V))} [0, 1]$$

where $\mathrm{vert}(I(V))$ is the set of vertices of $I(V)$ and such that $\{v|\ t_v \neq 0\}$ is a simplex of $I(V)$ and $\sum_v t_v = 1$.

For each simplex $\sigma = \{v_0, \ldots, v_n\}$ of $I(V)$, its *geometric realisation* $|\sigma| \subset I(V)_{\mathbb{R}}$ is the subset of $(t_v)_v \in I(V)_{\mathbb{R}}$ with $t_v = 0$ for all $v \notin \sigma$. The subset $|\sigma|$ of $I(V)_{\mathbb{R}}$ is compact for all simplices σ; the complex $I(V)_{\mathbb{R}}$ is the union of all $|\sigma|$ where σ runs over all simplices of $I(V)$ and the topology on $I(V)_{\mathbb{R}}$ is defined to be the inductive topology on this union where M is closed in $I(V)_{\mathbb{R}}$ if and only if $M \cap |\sigma|$ is closed for all simplices σ of $I(V)$. In this way $I(V)_{\mathbb{R}}$ is a CW-complex.

(B.1.6) The set $I(V)_{\mathbb{Q}} \subset I(V)_{\mathbb{R}}$ of elements $(t_v)_v$ such that $t_v \in \mathbb{Q}$ for all v, is dense in $I(V)_{\mathbb{R}}$. The set $I(V)_{\mathbb{Q}}$ corresponds to the dialation classes of rational

norms; the set $I(V)_{\mathbb{Z}}$ may be identified with the dialation classes of integral norms, that is to say with the vertices of $I(V)$.

(B.1.7) Define a map from $I(V)_{\mathbb{R}}$ to the dialation classes of norms on V

$$\Theta : I(V)_{\mathbb{R}} \to N(V)$$

in the following way. Let $\sigma = \{v_0, \ldots, v_n\}$ be a simplex of $I(V)$ and let $t = (t_v)_v \in |\sigma|$ be a point. Write $t_i = t_{v_i}$. By permuting the indices may suppose that $t_n > 0$ and that there are lattices $\Lambda(i) \in v_i$ with $\Lambda(0) \supset \Lambda(1) \supset \ldots \supset \pi\Lambda(0)$ and where all inclusions of this chain are strict. Put

$$\Theta(t) = \sup_i (q^{t_i + \ldots + t_n} \alpha_{\Lambda(i)}).$$

B.1.8. Theorem. *The map $\Theta : I(V)_{\mathbb{R}} \to N(V)$ is a bijection taking the vertices onto the set of classes of integral norms and $I(V)_{\mathbb{Q}}$ onto the set of classes of rational norms.*

[The proof of this theorem is exercise B.1.9(5) below.] □

B.1.9. Exercises. (1) Let $v_1, \ldots, v_m$ be a basis of V and let $r_1 > 0, \ldots, r_m > 0$ be real numbers. Show that the map $\alpha : V \to \mathbb{R}$ given by

$$\alpha(\sum_{i=1}^{m} a_i v_i) = \max_i r_i |a_i|$$

is a norm on V. Show that every norm on V takes this form for a choice of basis $v_1, \ldots, v_m$ and real numbers $r_i > 0$.

(2) Let Λ be an R-lattice of V. Define

$$\alpha_\Lambda(x) = \inf\{1/|a| \mid ax \in \Lambda\}.$$

Show that α_Λ is a norm on V.

(3) Show that the following are equivalent for a real number $t > 0$ and a norm α on V:

(i) $\alpha = t\alpha_\Lambda$ for some lattice Λ of V;
(ii) $\alpha(V) = t|L|$ where $t|L|$ denotes the set of values of $|.|$ multiplied by t;
(iii) for some basis $v_1, \ldots, v_m$ of V we have

$$\alpha(\sum_{i=1}^{m} a_i v_i) = t \max_i |a_i|.$$

(4) Let α be a norm on V. Put $S = \alpha(V) \cap]1, q]$, where $]1, q]$ is the semi-open interval of the real line joining 1 and q. For any $r \in S$, put $\Lambda(r) = B(0, qr)$, the open ball in V of centre 0 and radius qr.

(i) Show that $\Lambda(r)$ is a lattice of V for all $r \in S$.
(ii) Show that $\dim_L(V) \geq \sharp S$, where $\sharp S$ denotes the cardinality of the set S, and that $\alpha = \sup_{r\in S}(r\alpha_{\Lambda(r)})$.

(5) Prove theorem B.1.8 above.
[To show that Θ is bijective, use part (ii) of the preceding exercise B.1.9(4).]

(6) Let R be a discrete subring of a local field K archimedean or non-archimedean. Assume that K/R is a compact abelian group. Let W be a finite dimensional vector space over K; then W is a normed vector space over K and its topology is uniquely determined.
(i) Suppose that the subgroup G of W is *discrete*, that is to say there is a neighbourhood N of 0 in W such that $N \cap G = \{0\}$. Let M be a neighbourhood of 0 of W such that $M + M \subseteq N$. Show that if $M + x \cap M + y \neq \emptyset$ where $x, y \in G$ then we have $x = y$.
(ii) If Λ is a discrete R-module contained in W show that $\dim_K(\Lambda \otimes_R K) \leq \dim_K(W)$.
(iii) Suppose that Λ is a projective R-submodule of W. Show that Λ is discrete if and only if the natural map $\Lambda \otimes_R K \to W$ is injective.

B.2 The building map on Ω^d

(B.2.1) The notation we use is principally that of §2.1, namely: let

C be a smooth geometrically irreducible projective curve over a finite field k of characteristic p;
F be the field of functions of C/k;
∞ be a place of F;
$C_{\text{aff}} = C \setminus \{\infty\}$ be the affine curve obtained from C by removing ∞;
$A = \Gamma(C_{\text{aff}}, \mathcal{O}_C)$ be the coordinate ring of C_{aff};
$\mathbb{A}$ be the adèle ring of F;
$\mathbb{A}_f$ be the ring of finite adèles of F (see (A.5.4));
F_∞ be the completion of F at ∞;
O_∞ be the ring of valuation integers of F_∞;
q_∞ be the order of the residue field of O_∞;
$|.|$ be the valuation on F_∞ given by ∞ and normalised so that if π_∞ is a local parameter at ∞ then $|\pi_\infty| = q_\infty^{-1}$;
$\widehat{\overline{F}}_\infty$ be the completion of the algebraic closure $\overline{F}_\infty$ of F_∞;
$\Omega^d(\widehat{\overline{F}}_\infty) = \mathbb{P}_{d-1}(\widehat{\overline{F}}_\infty) \setminus \bigcup(F_\infty - \text{rational hyperplanes})$ (see (A.5.3)).

The valuation $|.|$ has a unique extension to the field $\widehat{\overline{F}}_\infty$ which is also denoted $|.|$. If S is a subset of $\widehat{\overline{F}}_\infty$, write $|S|$ for the set of real numbers which are absolute values of elements of S.

(B.2.2) Let $z = (z_1, \dots, z_d) \in \Omega^d(\widehat{\overline{F}}_\infty)$. The function on F_∞^d given by

$$\alpha_z : \ a = (a_1, \dots, a_d) \mapsto \alpha_z(a) = |\sum_{i=1}^{d} a_i z_i|$$

is a norm on the d-dimensional F_∞-vector space F_∞^d (exercise B.2.3(1)).

Define the building map λ by

$$\lambda : \Omega^d \to I(F_\infty^d)_{\mathbb{Q}}, \ z \mapsto \lambda(z) = \text{ dialation class of } \alpha_z.$$

The image of λ lies in the subset $I(F_\infty^d)_{\mathbb{Q}}$ of $I(F_\infty^d)_{\mathbb{R}}$ because the absolute values of elements of $\widehat{\overline{F}}_\infty$ lie in $q_\infty^{\mathbb{Q}} \cup \{0\}$.

B.2.3. Exercises. (1) Let $z = (z_1, \dots, z_d) \in \widehat{\overline{F}}_\infty^d$. Show that the map on F_∞^d given by

$$a = (a_1, \dots, a_d) \mapsto \alpha_z(a) = |\sum_{i=1}^{d} a_i z_i|$$

is a norm on the F_∞-vector space F_∞^d if and only if $z \in \Omega^d(\widehat{\overline{F}}_\infty)$. Show that for $c \in \widehat{\overline{F}}_\infty$ and $z \in \widehat{\overline{F}}_\infty^d$ we have $\alpha_{cz} = |c|\alpha_z$.

(2) Show that the map $\lambda : \Omega^d \to I(F_\infty^d)_{\mathbb{Q}}$ is $\mathrm{GL}_d(F_\infty)$-equivariant for actions on the left. Deduce that for any subgroup Γ of $\mathrm{GL}_d(F_\infty)$, there is a corresponding quotient map

$$\lambda_\Gamma : \Gamma\backslash\Omega^d \to \Gamma\backslash I(F_\infty^d)_{\mathbb{R}}.$$

(3) For 2 norms α, β on the vector space $V = F_\infty^d$ over F_∞, define the distance $\rho(\alpha, \beta)$ by the formula

$$\rho(\alpha, \beta) = \log_{q_\infty}\big(\sup_{x \in V, x \neq 0} \frac{\alpha(x)}{\beta(x)}\big) + \log_{q_\infty}\big(\sup_{x \in V, x \neq 0} \frac{\beta(x)}{\alpha(x)}\big).$$

Show that $\rho(\alpha, \beta)$ depends only on the dialation classes of α and β. Show that ρ is a metric on the space of dialation classes $N(V)$ of norms on V.

(4) (i) Let $M \supset N \supset \pi_\infty^r M$ be lattices of $V = F_\infty^d$ over O_∞ and let α_M, α_N be their corresponding norms on V (exercises B.1.9(2)). If $\pi_\infty M \not\supset N \not\supset \pi_\infty^{r-1} M$ show that $\rho(\alpha_M, \alpha_N) = r$.

(ii) Show that a set of lattices $M_0, \dots, M_r$ of V determines a simplex in the building $I(F_\infty^d)_{\mathbb{R}}$ if and only if $\rho(\alpha_{M_i}, \alpha_{M_j}) = 1$ for all $i \neq j$.

[Under the isomorphism $\Theta : I(V)_{\mathbb{R}} \to N(V)$ of theorem B.1.8, it follows from this exercise that the metric ρ is induced by the standard metric on the Euclidean Bruhat-Tits building $I(V)_{\mathbb{R}}$.]

(5) Let α be the norm associated to the standard lattice O_∞^d contained in F_∞^d. Let $z = (z_1, \dots, z_d) \in \Omega^d(\widehat{\overline{F}}_\infty)$ and suppose that $|z_i|/|z_j| \notin q^{\mathbb{Z}}$ for all $i \neq j$. Show that

$$\rho(\lambda(z), \alpha) = \log_{q_\infty} \frac{\max_i |z_i|}{\min_j |z_j|}.$$

B.3 Fibres of the building map on Ω^2

(B.3.1) For the case where $d = 2$, the Bruhat-Tits building $I(F_\infty^2)_{\mathbb{R}}$ is a *tree* T (a contractible 1-dimensional simplicial complex; see for example figures 1,2,3,4 of §3.8). The standard metric ρ on T is such the distance between adjacent vertices is equal to 1 (exercise B.2.3(3) and (4); see also §3.1).

For any element $u \in \widehat{\overline{F}}_\infty$, the *imaginary norm* $|u|_{\mathrm{im}}$ of u is defined to be

$$|u|_{\mathrm{im}} = \inf_{a \in F_\infty} |u - a|.$$

[This is the analogue for $\widehat{\overline{F}}_\infty$ of the imaginary parts of numbers in the complex upper half-plane.]

B.3.2. Proposition. *Let α be the norm associated to the standard lattice O_∞^2 contained in F_∞^2. Let $\lambda : \Omega^2 \to T$ be the building map. Then for all $u \in \Omega^2$ we have*

$$\rho(\lambda(u), \alpha) = \begin{cases} -\log_{q_\infty} |u|_{\mathrm{im}}, & \text{if } |u| \leq 1 \\ -\log_{q_\infty} |1/u|_{\mathrm{im}}, & \text{if } |u| \geq 1. \end{cases}$$

Proof. Put

$$S = O_\infty^2 \setminus \pi_\infty O_\infty^2.$$

The building map $\lambda : \Omega^2 \to T$ is given by (see (B.2.2))

$$\lambda(u)(a, b) = |a + ub| \quad \text{for all } (a, b) \in F_\infty^2, u \in \Omega^2.$$

If $|u| \leq 1$ then we have

$$\sup_{(a,b) \in S} |a + bu| = 1.$$

Furthermore, we have

$$\inf_{(a,b) \in S} |a + bu| = \inf_{|a| \leq 1, |b| = 1} |a + bu|$$

$$= \inf_{a \in O_\infty} |a + u| = |u|_{\mathrm{im}}.$$

Therefore we have (by exercise B.2.3(3))

$$\rho(\lambda(u), \alpha) = \log_{q_\infty}(1/|u|_{\mathrm{im}})$$

as required.

If $|u| \geq 1$ then we have by the first part

$$\rho(\lambda(u), \alpha) = \rho(\lambda(1/u), \alpha) = -\log_{q_\infty}(1/|u|_{\mathrm{im}})$$

as required.□

(B.3.3) The reduction map $r : \mathbb{P}_1(\widehat{F}_\infty) \to \mathbb{P}_1(\overline{\mathbb{F}}_{q_\infty})$, where $\overline{\mathbb{F}}_{q_\infty}$ is the algebraic closure of $\mathbb{F}_{q_\infty}$, admits a section $s : \mathbb{P}_1(\overline{\mathbb{F}}_{q_\infty}) \to \mathbb{P}_1(\widehat{F}_\infty)$ such that $s(0) = 0$ and $s(\infty) = \infty$ and rs is the identity on $\mathbb{P}_1(\overline{\mathbb{F}}_{q_\infty})$.

For a metric space, we write $B^*(x, c)$ for the closed ball with centre x and radius c and we write $B(x, c)$ for the corresponding open ball; for the point z at infinity of $\mathbb{P}_1(\widehat{F}_\infty)$, write $B(z, c) = \{z\} \cup \{u \in \widehat{F}_\infty |\ |u| > 1/c\}$.

B.3.4. Corollary. *Let x be the vertex of T corresponding to the standard lattice O_∞^2 contained in F_∞^2. For c a real number in $[0, 1[$ we have that $\lambda^{-1}(B^*(x, c))$ is equal to $\mathbb{P}_1(\widehat{F}_\infty)$ minus $q_\infty + 1$ disjoint open discs; more precisely we have*

$$\lambda^{-1}(B^*(x, c)) = \mathbb{P}_1(\widehat{F}_\infty) \setminus \bigcup_{x \in \mathbb{P}_1(\mathbb{F}_\infty)} B(s(x), q_\infty^{-c}).$$

Proof. Let $u \in \Omega^2$. Suppose first that $|u| \leq 1$. By proposition B.3.2, we have $u \in \lambda^{-1}(B^*(x, c))$ if and only if

$$q_\infty^{-1} < q_\infty^{-c} \leq |u|_{\mathrm{im}} \leq 1.$$

This is the case if and only if u does not lie in one of the $(q_\infty + 1)$ discs $B(s(x), q_\infty^{-c})$ for all $x \in \mathbb{P}_1(\mathbb{F}_\infty)$, as required.

The case where $|u| > 1$ now follows from this and proposition B.3.2 where we note that u lies in one of the discs $B(s(x), q_\infty^{-c})$, where $x \in \mathbb{P}_1(\mathbb{F}_\infty)$, if and only if $1/u$ does so. □

B.3.5. Exercises. (1) Show that $|.|_{\mathrm{im}}$ has the following properties.

(i) For $u \in \widehat{F}_\infty$, we have $|u|_{\mathrm{im}} = 0$ if and only if $u \in F_\infty$.

(ii) For $u \in \widehat{F}_\infty$ and $c \in F_\infty$, we have $|cu|_{\mathrm{im}} = |c||u|_{\mathrm{im}}$.

(iii) If $u \in \widehat{F}_\infty$ and $|u| \notin q_\infty^{\mathbb{Z}}$ then $|u|_{\mathrm{im}} = |u|$.

(iv) Suppose that $u \in \widehat{F}_\infty$ and $|u| = 1$; let $r(u)$ denote the residue class of u in $\overline{\mathbb{F}}_{q_\infty}$. We have $|u|_{\mathrm{im}} = 1$ if and only if $r(u) \in \overline{\mathbb{F}}_{q_\infty} \setminus \mathbb{F}_{q_\infty}$.

(2) Let m be an integer ≥ 0 and let c be a real number in the interval $[m, m + 1[$. Let x be the vertex of T corresponding to the standard lattice O_∞^2 contained in F_∞^2. Show that $\lambda^{-1}(B^*(x, c))$ is equal to $\mathbb{P}_1(\widehat{F}_\infty)$ minus $(q_\infty + 1)q_\infty^m$ discs of radius q_∞^{-c}.

(3) Let x be the vertex of T corresponding to the standard lattice O_∞^2. Let $y \in \mathbb{P}_1(\mathbb{F}_{q_\infty})$ and let y^* be the corresponding open edge emanating from x. Show that all the points of $B(s(y), 1) \setminus B^*(s(y), q_\infty^{-1})$ of Ω^2 project via λ onto the edge y^*. Describe similarly the inverse images in Ω^2 by λ of all the open edges of T.

Replacing $\mathbb{P}_1(\widehat{F}_\infty)$ by the complex Riemann sphere $\mathbb{P}_1(\mathbb{C})$ and replacing corresponding open discs by complex open discs, explain why Ω^2, equipped with the

building map $\lambda : \Omega^2 \to T$, resembles intuitively the boundary of a tubular neighbourhood of the tree T in 3-dimensional Euclidean space (see [DH, pp.63-64]).

B.4 Structures of level H on Drinfeld modules; the moduli scheme M_H^d

(B.4.1) Let U be a non-empty open subscheme of the projective curve C/k. as in (B.2.1). Let S be a finite set of closed points of U. A locally free sheaf $\mathcal{E}$ of rank n on U is *trivialised over* $U \setminus S$ if there is an isomorphism of sheaves of $\mathcal{O}_C$-modules

$$\mathcal{E}|_{U\setminus S} \cong \mathcal{O}_C^n|_{U\setminus S}.$$

(B.4.2) Let V be the localisation of $\mathcal{E}$ at the generic point of U. Then V is a vector space of dimension n over the function field F of C/k. Then $\mathcal{E}$ defines for all closed points x of U a finitely generated $\mathcal{O}_{C,x}$-submodule $L(x)$ of V, where $\mathcal{O}_{C,x}$ is the local ring of C at x.

Let F_x denote the completion of the field F at x. Let $\widehat{\mathcal{O}}_{C,x}$ denote the completion of the discrete valuation ring $\mathcal{O}_{C,x}$; thus F_x is the fraction field of $\widehat{\mathcal{O}}_{C,x}$. We obtain a commutative diagram of bijections

$$\begin{array}{ccc} \mathrm{GL}_n(F)/\mathrm{GL}_n(\mathcal{O}_{C,x}) & \longrightarrow & \{\mathcal{O}_{C,x}-\text{lattices in } F^n\} \\ \downarrow & & \downarrow \\ \mathrm{GL}_n(F_x)/\mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}) & \longrightarrow & \{\widehat{\mathcal{O}}_{C,x}-\text{lattices in } F_x^n\} \end{array}$$

(B.4.3) If $\mathcal{E}$ is trivialised over $U \setminus S$ then there is a basis $x_1, \ldots, x_n$ of V such that for all points x of $U \setminus S$ we have

$$L(x) = \bigoplus_{i=1}^{n} x_i \mathcal{O}_{C,x}.$$

This gives the diagram of bijections where the vertical map is a homeomorphism

$$\begin{array}{ccc} \displaystyle\prod_{x\in S} \mathrm{GL}_n(F_x)/\mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}) & \to & \left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{locally free sheaves of rank} \\ n \text{ on } U \text{ trivialised over } U\setminus S \end{array} \right\} \\ \downarrow & & \\ \displaystyle\prod_{x\in S} \mathrm{GL}_n(F_x) \times \prod_{x\in U\setminus S} \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}) / \prod_{x\in U} \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}) & & \end{array}$$

(B.4.4) Let I be an ideal of A. Let $\mathcal{I}$ be the corresponding sheaf of ideals of $\mathcal{O}_C$. Suppose that $\mathcal{E}$ is equipped with a full level I-structure; that is to say

there is an isomorphism of $\mathcal{O}_C$-modules

$$\mathcal{E} \otimes_{\mathcal{O}_C} \mathcal{O}_C/\mathcal{I} \cong (\mathcal{O}_C/\mathcal{I})^n.$$

Assume that the support of Spec A/I is contained in the finite set of points S. For all $x \in U$ put

$$\mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}, I) = \ker\{\mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}) \to \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}/I\widehat{\mathcal{O}}_{C,x})\}.$$

We then have the diagram of bijections

$$\prod_{x\in S} \mathrm{GL}_n(F_x)/\mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}, I) \to \left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{locally free sheaves of rank} \\ n \text{ on } U \text{equipped with a} \\ \text{trivialisation over } U \setminus S \\ \text{with full level } I \text{ structure} \end{array} \right\}$$

$$\downarrow$$

$$\prod_{x\in S} \mathrm{GL}_n(F_x) \times \prod_{x\in U\setminus S} \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x})/ \prod_{x\in U} \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}, I)$$

(B.4.5) Take now the particular case where $U = C \setminus \{\infty\}$. We have, where $\mathbb{A}_f$ is the ring of finite adèles (see (A.5.4)),

$$\mathrm{GL}_n(\mathbb{A}_f) = \varinjlim_S \prod_{x\in S} \mathrm{GL}_n(F_x) \times \prod_{x\in C\setminus S} \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x})$$

where the limit runs over all finite subsets S of closed points of the open subscheme $C \setminus \{\infty\}$ of C/k. We obtain

$$\mathrm{GL}_n(\mathbb{A}_f)/ \prod_{x\in C\setminus\{\infty\}} \mathrm{GL}_n(\widehat{\mathcal{O}}_{C,x}, I) = \left\{ \begin{array}{c} \text{isomorphism classes of locally free} \\ \text{sheaves on } C \setminus \{\infty\} \text{ of rank } n \\ \text{equipped with a trivialisation outside} \\ \text{Spec } (A/I) \text{ with full level } I \text{ structure} \end{array} \right\}.$$

(B.4.6) Let $\widehat{A}$ be the profinite completion of A; then we have an isomorphism of groups which is a homeomorphism

$$\mathrm{GL}_d(\widehat{A}) \cong \prod_{x\in C\setminus\{\infty\}} \mathrm{GL}_d(\widehat{O}_{C,x}).$$

For any ideal I of A, let $\tilde{U}_I$ be the kernel of the natural map $\mathrm{GL}_d(\widehat{A}) \to \mathrm{GL}_d(\widehat{A}/I\widehat{A})$ (as in theorem A.6.9).

B.4.7. Definition. An *arithmetic subgroup* H of $\mathrm{GL}_d(\widehat{A})$ is a compact open subgroup of $\mathrm{GL}_d(\widehat{A})$ such that H contains a compact open subgroup of the form $\tilde{U}_I$ for some non-zero ideal I of A.

(B.4.8) Let H be an arithmetic subgroup of $\mathrm{GL}_d(\widehat{A})$. Then H contains a normal subgroup of finite index $\tilde{U}_I$ for some non-zero ideal I of A; furthermore, by taking a subgroup of $\tilde{U}_I$ if necessary, it may be supposed that A/I contains at least 2 maximal ideals.

Let M_I^d be the fine moduli scheme of rank d Drinfeld modules equipped with a full level I-structure. By (A.6.8) there is an action of $\mathrm{GL}_d(\mathbb{A}_f)/F^*$ on M^d. We define M_H^d to be the quotient scheme of M^d under H

$$M_H^d = (M^d)^H.$$

As the quotient $H/\tilde{U}_I$ is a finite group, we obtain

$$M_H^d = (M_I^d)^{H/\tilde{U}_I}.$$

The quotient M_H^d of the scheme M_I^d by the finite group $H/\tilde{U}_I$ exists and is of finite type over A. We say that scheme M_H^d is the *moduli scheme of Drinfeld modules with an H-structure*.

B.4.9. Proposition. *Let $S \subset \mathrm{GL}_d(\mathbb{A}_f)$ be a finite set of representatives of the double cosets $H\backslash\mathrm{GL}_d(\mathbb{A}_f)/\mathrm{GL}_d(F)$. The isomorphism of rigid analytic spaces*

$$(M_I^d \otimes F_\infty)_{\mathrm{an}} \cong \tilde{U}_I\backslash\tilde{\Omega}^d$$

induces bijections

$$M_H^d(\widehat{\overline{F}}_\infty) = H\backslash\tilde{\Omega}^d$$

$$= \coprod_{x\in S} \Omega^d/(xHx^{-1} \cap \mathrm{GL}_d(F))$$

where the disjoint union here is over the finitely representatives of S.

Proof. The first bijection $M_H^d(\widehat{\overline{F}}_\infty) = H\backslash\tilde{\Omega}^d$ follows immediately from theorem A.8.7 and the definition $M_H^d = (M_I^d)^{H/\tilde{U}_I}$. For the second bijection, we have

$$\tilde{\Omega}^d = (\mathrm{GL}_d(\mathbb{A}_f) \times \Omega^d)/\mathrm{GL}_d(F).$$

Hence we obtain

$$H\backslash\tilde{\Omega}^d = H\backslash(\mathrm{GL}_d(\mathbb{A}_f) \times \Omega^d)/\mathrm{GL}_d(F)$$

$$= H\backslash((\coprod_{yH\in\mathrm{GL}_d(\mathbb{A}_f)/H} yH) \times \Omega^d)/\mathrm{GL}_d(F)$$

$$= \coprod_{x\in S} \Omega^d/(xHx^{-1} \cap \mathrm{GL}_d(F)). \quad \square$$

B.5 Action of arithmetic subgroups of $\mathbf{GL_2}(F)$ on T

We consider the action of the subgroup $\mathrm{GL}_2(A)$ of $\mathrm{GL}_2(F)$ on the Bruhat-Tits building $I(F^2)$ with respect to the valuation on F arising from ∞. The main results of this section are theorem B.5.18 and corollary B.5.19 which are used to prove the isomorphism of cuspidal cohomology of proposition B.7.10 (see also exercise B.7.16(1)).

B.5.1. Remarks. (1) It is assumed in this section that the ground field k is finite. Nevetheless, most of the results here are valid with minor modifications for any ground field.

[For more details on the results of this section, see [S4, Chapitre II, §2].]

(2) The tree $I(F^2)$ is that associated to the global field F with respect to the discrete valuation corresponding to the point ∞. The tree $I(F^2)$ is isomorphic to the tree $I(F_\infty^2)_\mathbb{R}$ corresponding to the local field F_∞, the completion of F at ∞. Nevertheless, the two corresponding *buildings* are not isomorphic as $I(F_\infty^2)_\mathbb{R}$ contains many more apartments than $I(F^2)$. This is unimportant for the application to cuspidal cohomology in proposition B.7.10 and exercise B.7.16(1).

(B.5.2) Let R be the local ring $\mathcal{O}_{C,\infty}$ of the curve C/k at ∞. Put

$$d = \deg_k(\infty).$$

Let $\mathcal{I}_\infty$ be the sheaf of ideals of $\mathcal{O}_C$ corresponding to the closed point ∞. We write T for the tree $I(F^2)_\mathbb{R}$.

A locally free sheaf of rank 1 on C is called a *line bundle*. Note that as k is a finite field the greatest common divisor of the degrees of k-rational divisors on C is equal to 1. An *isomorphism* between sheaves on C will always mean an isomorphism of sheaves of $\mathcal{O}_C$-modules.

(B.5.3) Let Λ be an R-lattice in F^2. Associated to Λ is the vertex x_Λ of the tree T and the coherent sheaf of $\mathcal{O}_C$-modules $\mathcal{E}_\Lambda$ on the projective curve C/k defined by the properties:

(a) $\mathcal{E}_\Lambda$ is a subsheaf of the constant sheaf F^2 on C;
(b) at every point x of C_{aff} the localisation $\mathcal{E}_{\Lambda,x}$ is equal to A_x^2, where A_x is the localisation of the ring A at x;
(c) the localisation $\mathcal{E}_{\Lambda,\infty}$ at ∞ is equal to Λ.

As a sheaf is uniquely determined by its stalks, the existence and uniqueness of the coherent sheaf $\mathcal{E}_\Lambda$ defined by these properties is clear.

(B.5.4) Two locally free sheaves $\mathcal{E}, \mathcal{E}'$ on C are *$\mathcal{I}_\infty$-equivalent* if there is an integer $n \in \mathbb{Z}$ such that $\mathcal{E}'$ is isomorphic to $\mathcal{E} \otimes_{\mathcal{O}_C} \mathcal{I}_\infty^n$.

A locally free sheaf of rank n on C_{aff} is *trivial* if it is isomorphic to the sheaf associated to the free A-module A^n of rank n.

B.5.5. Proposition. *The applications $\Lambda \to x_\Lambda$ and $\Lambda \to \mathcal{E}_\Lambda$ induce a bijection between the vertices of $\mathrm{GL}_2(A)\backslash T$ and the set of $\mathcal{I}_\infty$-equivalence classes of locally free sheaves of rank 2 on C whose restrictions to C_{aff} are trivial.*

Proof. By construction, the restriction of the sheaf $\mathcal{E}_\Lambda$ to C_{aff} is trivial.

If $\alpha \in F^*$ and $n = v(\alpha)$ where v is the valuation on F corresponding to ∞, then we have an isomorphism of sheaves of $\mathcal{O}_X$-modules $\mathcal{E}_{\alpha\Lambda} \cong \mathcal{I}_\infty^{\otimes n} \otimes_{\mathcal{O}_C} \mathcal{E}_\Lambda$.

If Λ, Λ' are R-lattices in F^2 then the sheaves $\mathcal{E}_\Lambda$ and $\mathcal{E}_{\Lambda'}$ are isomorphic if and only if there is $g \in \mathrm{GL}_2(A)$ such that $g\Lambda = \Lambda'$, because the subgroup of $\mathrm{GL}_2(F)$ stabilising the sublattice A^2 is $\mathrm{GL}_2(A)$. □

B.5.6. Lemma. *Let $\mathcal{E}$ a locally free sheaf of rank 2 on C. Write $\det(\mathcal{E})$ for the locally free sheaf of rank 1 which is the determinant of $\mathcal{E}$. The following conditions are equivalent:*

(a) *the restriction to C_{aff} of $\mathcal{E}$ is trivial;*
(b) *the restriction of $\det(\mathcal{E})$ to C_{aff} is trivial;*
(c) *there is $n \in \mathbb{Z}$ such that $\det(\mathcal{E})$ is isomorphic to $\mathcal{I}_\infty^{\otimes n}$.*

Proof. The equivalence of (a) and (b) results from C being of dimension 1; more precisely, the projective modules of rank 2 over the Dedekind domain A are isomorphic to $A \oplus M$ where M is an invertible ideal of A.

The equivalence of (b) and (c) is evident.□

B.5.7. Proposition. *The correspondence $\Lambda \to \mathcal{E}_\Lambda$ induces a bijection between the vertices of $\mathrm{GL}_2(A)\backslash T$ and the set of isomorphism classes of locally free sheaves of rank 2 on C such that $\det(\mathcal{E})$ is isomorphic to $\mathcal{O}_C$ or $\mathcal{I}_\infty$.*

Proof. Let $\mathcal{E}$ be a locally free sheaf of rank 2 on C such that the restriction to C_{aff} is trivial. Then by lemma B.5.6, there is an isomorphism $\det(\mathcal{E}) \cong \mathcal{I}_\infty^{\otimes n}$ for some $n \in \mathbb{Z}$. As we have $\det(\mathcal{E} \otimes_{\mathcal{O}_C} \mathcal{I}_\infty^m) \cong \mathcal{I}_\infty^{n+2m}$ the result follows. □

Sub-bundles of rank 2 bundles

(B.5.8) The line bundles on C form a group $\mathrm{Pic}(C)$. Let J/k denote the jacobian of C; then $J(k)$ is the finite group of k-rational points of J as k is finite. We have the exact sequence obtained from the degree homomorphism $\mathrm{Pic}(C) \to \mathbb{Z}$

$$0 \;\to\; J(k) \;\to\; \mathrm{Pic}(C) \;\overset{\deg}{\to}\; \mathbb{Z} \;\to\; 0.$$

B.5.9. Definitions. (1) Let $\mathcal{E}$ be a locally free sheaf of rank 2 on C. Let $\mathcal{L}$ be a line bundle on C which is a subsheaf of $\mathcal{E}$. Then $\mathcal{L}$ is contained in a unique line bundle $\mathcal{L}'$ which is a subsheaf of $\mathcal{E}$ and which is maximal with respect to this inclusion property. This subsheaf $\mathcal{L}'$ can be defined as the subsheaf which is the intersection of $\mathcal{E}$ with the line of the generic fibre of $\mathcal{E}$ containing $\mathcal{L}$.

When $\mathcal{L} = \mathcal{L}'$, then $\mathcal{L}$ is said to be *sub-bundle* of $\mathcal{E}$; in this case when $\mathcal{L}$ is a line sub-bundle, of $\mathcal{E}$, the quotient sheaf $\mathcal{E}/\mathcal{L}$ is also a line bundle.
(2) Let $\mathcal{L}$ be a line bundle. Put

$$\Delta(\mathcal{E}, \mathcal{L}) = \mathcal{E} \otimes_{\mathcal{O}_C} \mathcal{L}^{-1}$$

and put

$$N(\mathcal{E}, \mathcal{L}) = -\deg(\Delta(\mathcal{E}, \mathcal{L})).$$

When $\mathcal{L}$ is a line sub-bundle of $\mathcal{E}$, we then have

$$N(\mathcal{E}, \mathcal{L}) = \deg(\mathcal{L}) - \deg(\mathcal{E}/\mathcal{L}) = 2\deg(\mathcal{L}) - \deg(\mathcal{E}) = \deg(\mathcal{L} \otimes_{\mathcal{O}_C} (\mathcal{E}/\mathcal{L})^{-1}).$$

Furthermore, we have that $\Gamma(C, \Delta(\mathcal{E}, \mathcal{L}))$ is the space of $\mathcal{O}_C$-module homomorphisms $\mathcal{L} \to \mathcal{E}$ and if $\mathcal{L}$ is a line sub-bundle, of $\mathcal{E}$, then $H^1(C, \mathcal{L} \otimes_{\mathcal{O}_C} (\mathcal{E}/\mathcal{L})^{-1})$ is the space of isomorphism classes of extensions of $\mathcal{L}$ by $\mathcal{E}/\mathcal{L}$.

Put

$$N(\mathcal{E}) = \sup N(\mathcal{E}, \mathcal{L})$$

where the supremum runs over all line sub-bundles $\mathcal{L}$ of $\mathcal{E}$.

B.5.10. Proposition. (i) *If $\mathcal{E}$ contains a sub-bundle $\mathcal{L}$ of rank 1 such that $N(\mathcal{E}, \mathcal{L}) > 0$ then this sub-bundle is unique.*
(ii) *Let g be the genus of the curve C/k. We have that $N(\mathcal{E})$ is finite and*

$$N(\mathcal{E}) \geq -2g.$$

Proof. (i) Suppose that $\mathcal{E}$ contains another rank 1 sub-bundle $\mathcal{L}'$ such that $N(\mathcal{E}, \mathcal{L}') > 0$. We then have

$$\deg(\Delta(\mathcal{E}, \mathcal{L}')/(\mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1})) = -\frac{1}{2}N(\mathcal{E}, \mathcal{L}) - \frac{1}{2}N(\mathcal{E}, \mathcal{L}') < 0.$$

Hence we have

$$\Gamma(C, \Delta(\mathcal{E}, \mathcal{L}')/(\mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1})) = 0.$$

Hence the exact sequence

$$0 \to \Gamma(C, \mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1}) \to \Gamma(C, \mathcal{E} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1}) \to \Gamma(C, \Delta(\mathcal{E}, \mathcal{L}')/(\mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1}))$$

shows that the non-zero element of $\Gamma(C, \mathcal{E} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1})$ corresponding to the injection $\mathcal{L}' \to \mathcal{E}$ is also an element of $\Gamma(C, \mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1})$; that is to say the

injection $\mathcal{L}' \to \mathcal{E}$ factors through the injection $\mathcal{L} \to \mathcal{E}$. As $\mathcal{L}'$ is a rank 1 sub-bundle of $\mathcal{E}$ it follows that $\mathcal{L}' = \mathcal{L}$.

(ii) Select a line bundle $\mathcal{L}$ on C/k such that

$$\frac{1}{2}\deg(\mathcal{E}) - g \leq \deg(\mathcal{L}) < \frac{1}{2}\deg(\mathcal{E}) + 1 - g.$$

This is possible as the greatest common divisor of the degrees of line bundles on C/k is equal to 1. Then we have

$$-2g \leq N(\mathcal{E}, \mathcal{L}) < 2 - 2g.$$

By the Riemann-Roch theorem we have

$$\dim \Gamma(C, \Delta(\mathcal{E}, \mathcal{L})) \geq -N(\mathcal{E}, \mathcal{L}) + 2 - 2g \geq 1.$$

Hence there is an injection of sheaves of $\mathcal{O}_C$-modules $\mathcal{L} \to \mathcal{E}$. Let $\mathcal{L}'$ be the line sub-bundle of $\mathcal{E}$ containing the image of $\mathcal{L}$, that is to say $\mathcal{L}'$ is the maximal subsheaf of $\mathcal{E}$ which is a line bundle containing the image of $\mathcal{L}$. Then we have

$$\deg(\mathcal{L}') \geq \deg(\mathcal{L}).$$

Hence we have

$$N(\mathcal{E}, \mathcal{L}') \geq N(\mathcal{E}, \mathcal{L}) \geq -2g.$$

We obtain

$$N(\mathcal{E}) \geq -2g.$$

Suppose that $N(\mathcal{E}, \mathcal{L})$ were not bounded as $\mathcal{L}$ runs over all rank 1 sub-bundles of $\mathcal{E}$. Then there would be a rank 1 sub-bundle $\mathcal{J}$ of $\mathcal{E}$ such that $N(\mathcal{E}, \mathcal{J}) > 0$; hence by part (i), $\mathcal{J}$ would be the unique sub-bundle with $N(\mathcal{E}, \mathcal{J}) > 0$ and hence $N(\mathcal{E}, \mathcal{L})$ would be bounded, a contradiction. Hence we must have that $N(\mathcal{E})$ is finite. □

B.5.11. Definition. A locally free sheaf $\mathcal{E}$ of rank 2 on C is *decomposable* if it is the direct sum of 2 line bundles on C. Such a decomposition is unique up to an automorphism of $\mathcal{E}$ (exercise B.5.21(2)).

B.5.12. Proposition. *A locally free sheaf $\mathcal{E}$ of rank 2 on C such that $N(\mathcal{E}) > 2g - 2$ is decomposable.*

Proof. As $N(\mathcal{E}) > 2g - 2$, there is a rank 1 sub-bundle $\mathcal{L}$ of the locally free sheaf $\mathcal{E}$ of rank 2 such that $N(\mathcal{E}, \mathcal{L}) > 2g - 2$. Put $\mathcal{L}' = \mathcal{E}/\mathcal{L}$. Then $\mathcal{E}$ is an extension of the line bundle $\mathcal{L}'$ by the line bundle $\mathcal{L}$ and the extension is classified by an element of the space $H^1(C, \mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1})$. As we have

$$\deg(\mathcal{L} \otimes_{\mathcal{O}_C} \mathcal{L}'^{-1}) = N(\mathcal{E}, \mathcal{L}) > 2g - 2$$

this cohomology group is zero by Serre duality. Therefore this extension is trivial. □

The graph $\mathrm{GL}_2(A)\backslash T$

(B.5.13) A *graph* G is a set $\mathrm{vert}(G)$ of vertices and a set $\mathrm{line}(G)$ of lines where the two extremities of every line are vertices in $\mathrm{vert}(G)$; $\mathrm{line}(G)$ may be considered as a subset of $\mathrm{vert}(G)^2 \times E$ for some set E, in particular, two vertices may be joined by more than one line.

B.5.14. Definitions. (1) Let $\mathrm{Pic}(A)$ be the group of locally free sheaves of rank 1 on $\mathrm{Spec}\ A$. The finite group $\mathrm{Pic}(A)$ is isomorphic to the quotient of $\mathrm{Pic}(C)$ by the subgroup generated by $\mathcal{I}_\infty$ and, from (B.5.8), it lies in the exact sequence

$$0 \ \to \ J(k) \ \to \ \mathrm{Pic}(A) \ \overset{\deg}{\to} \ \mathbb{Z}/d\mathbb{Z} \ \to \ 0$$

where $d = \deg_k(\infty)$. Let $c \in \mathrm{Pic}(A)$. Then there is a unique element $c^* \in \mathrm{Pic}(C)$ which extends c and such that

$$0 \leq \deg(c^*) < d.$$

Let $\mathcal{F}_c$ be the line bundle on C of class c^*; this line bundle is determined uniquely up to isomorphism. We put

$$f_c = \deg(\mathcal{F}_c).$$

(2) For $c \in \mathrm{Pic}(A)$, the *cusp* Δ_c is the subgraph of $\mathrm{GL}_2(A)\backslash T$ defined as follows. Let $\mathcal{F}_c$ be the line bundle defined above and let $n \in \mathbb{Z}$. Put

$$\mathcal{F}'_{n,c} = \mathcal{I}_\infty^{\otimes n} \otimes_{\mathcal{O}_C} \mathcal{F}_c^{-1}, \quad \mathcal{E}_{c,n} = \mathcal{F}_c \bigoplus \mathcal{F}'_{n,c}.$$

Then $\mathcal{E}_{c,n}$ restricted to C_{aff} is trivial (lemma B.5.6) and so by proposition B.5.7 it defines a vertex $x_{c,n}$ of $\mathrm{GL}_2(A)\backslash T$. We have

$$\deg(\mathcal{E}_{c,n}) = -nd \text{ and } N(\mathcal{E}_{c,n}, \mathcal{F}_c) = 2f_c + nd.$$

The inclusion $\mathcal{I}_\infty^{\otimes n} \subseteq \mathcal{I}_\infty^{\otimes(n+1)}$ defines the inclusion of $\mathcal{E}_{c,n}$ in $\mathcal{E}_{c,n+1}$. Hence this gives a line $y_{c,n}$ joining $x_{c,n}$ to $x_{c,n+1}$. In the same way, there is a line $\overline{y}_{c,n}$ joining $x_{c,n}$ with $x_{c,n-1}$.

B.5.15. Proposition. *The vertices $x_{c,n}$, for all $c \in \mathrm{Pic}(A)$ and all $n \geq 1$, are distinct.*

Proof. If $n \geq 1$ then $N(\mathcal{E}_{c,n}, \mathcal{F}_c) > 0$ which shows that $\mathcal{F}_c$ is the unique rank 1 sub-bundle of maximal degree of $\mathcal{E}_{n,c}$ (proposition B.5.10). Suppose then that

$x_{c,n} = x_{b,m}$ where $b, c, \in \mathrm{Pic}(A)$ and $n \geq 1$, $m \geq 1$. By proposition B.5.5, it follows that for some integer s there is an isomorphism

$$\mathcal{E}_{c,n} \cong \mathcal{E}_{b,m} \otimes_{\mathcal{O}_C} \mathcal{I}_\infty^{\otimes s}.$$

Therefore there are isomorphisms, by the uniqueness of the decomposition of $\mathcal{E}_{c,n}$ as a sum of line bundles (see exercise B.5.21(2)),

$$\mathcal{F}_c \cong \mathcal{F}_b \otimes_{\mathcal{O}_C} \mathcal{I}_\infty^{\otimes s} \text{ and } \mathcal{F}'_{c,n} \cong \mathcal{F}'_{b,m} \otimes_{\mathcal{O}_C} \mathcal{I}_\infty^{\otimes s}.$$

As $\mathcal{F}_c$ is uniquely determined in its $\mathcal{I}_\infty$-equivalence class, by the definition of $\mathcal{F}_c$ it follows that $c = b$ and $s = 0$. Hence we have $m = n$. □

B.5.16. Proposition. *If $N(\mathcal{E}_{n,c}, \mathcal{F}_c) = nd + 2f_c > 2g - 2 + d$ then the only lines of $\mathrm{GL}_2(A)\backslash T$ emanating from $x_{c,n}$ are $y_{c,n}$ and $\overline{y}_{c,n}$.*

Proof. Let $\mathcal{E}$ be a locally free sheaf of rank 2 corresponding to the vertex x of $\mathrm{GL}_2(A)\backslash T$. Then the lines of $\mathrm{GL}_2(A)\backslash T$ with origin x correspond to the orbits of the group $\mathrm{Aut}(\mathcal{E})$ acting on the space of k-lines of the fibre $\mathcal{E}(\infty)$ of $\mathcal{E}$ at ∞, this fibre being a vector space over $\kappa(\infty)$ of dimension 2. When we take $x = x_{c,n}$, $\mathcal{E} = \mathcal{E}_{c,n}$, the fibre of $\mathcal{E}$ at ∞ is the direct sum of two lines

$$\mathcal{E}_{c,n}(\infty) \cong D \oplus D'$$

where D is the fibre of $\mathcal{F}_c$ and D' is the fibre of $\mathcal{F}'_c$ at ∞. The line D corresponds to the line $y_{c,n}$ and the line D' to the line $\overline{y}_{c,n}$. If we put $G = \mathrm{Aut}(\mathcal{E}_{c,n})$, then the proposition is equivalent to the assertion that every line of $D \oplus D'$ distinct from D is G-conjugate to D'.

The group G contains automorphisms of the form $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ where s is a section of the line bundle

$$\mathcal{H} = \mathcal{H}om(\mathcal{F}'_{c,n}, \mathcal{F}_c) \cong \mathcal{F}_c^{\otimes 2} \otimes_{\mathcal{O}_C} \mathcal{I}_\infty^{\otimes -n}.$$

Such an automorphism acts on the fibre $D \oplus D'$ by the unipotent matrix $\begin{pmatrix} 1 & s(\infty) \\ 0 & 1 \end{pmatrix}$ where $s(\infty)$ denotes the value of the section s at ∞.

The degree of $\mathcal{H}$ satisfies

$$\deg(\mathcal{H}) = nd + 2f_c > 2g - 2 + d$$

and we have the exact sequence

$$\Gamma(C, \mathcal{H}) \to \Gamma(C, \mathcal{H} \otimes \frac{\mathcal{O}_C}{\mathcal{I}_\infty}) \to H^1(C, \mathcal{I}_\infty \otimes_{\mathcal{O}_C} \mathcal{H}).$$

We then have $H^1(C, \mathcal{I}_\infty \otimes_{\mathcal{O}_C} \mathcal{H}) = 0$ as

$$\deg(\mathcal{I}_\infty \otimes_{\mathcal{O}_C} \mathcal{H}) > 2g - 2.$$

The homomorphism

$$\Gamma(C, \mathcal{H}) \to \Gamma(C, \mathcal{H} \otimes \frac{\mathcal{O}_C}{\mathcal{I}_\infty})$$

of evaluation at ∞ is therefore surjective. Hence every line of $D \oplus D'$ distinct from D is G-conjugate to D'. □

B.5.17. Definition. (1) Put

$$m = \sup(2g - 2 + d, 3d - 2).$$

Let n_c be the largest integer such that $dn_c + 2f_c \leq m$, that is to say $N(\mathcal{E}_{n,c}, \mathcal{F}_c) \leq m$. We have, as may be checked,

$$(a)\ n_c \geq 1$$

$$(b)\ dn_c > 2g - 2 - 2f_c$$

(2) Let Δ_c be the subgraph of $\mathrm{GL}_2(A)\backslash T$ having for vertices the points $x_{c,n}$, $n \geq n_c$ and for lines $y_{c,n}$, $n \geq n_c$. Then Δ_c is an infinite half-line with origin $x_c = x_{c,n}$ where $n = n_c$.

The inequality (a) together with proposition B.5.15 shows that the paths Δ_c are disjoint. The inequality (b) together with proposition B.5.16 shows that Δ_c intersects the rest of $\mathrm{GL}_2(A)\backslash T$ only at the point x_c.

(3) Let Y_m be the sub-graph of $\mathrm{GL}_2(A)\backslash T$ whose vertices correspond to locally free sheaves $\mathcal{E}$ of rank 2 such that $N(\mathcal{E}) \leq m$ and whose lines are those of $\mathrm{GL}_2(A)\backslash T$ both extremities of which lie in Y_m.

As $N(\mathcal{E}_{c,n_c}) = 2f_c + dn_c$ is $\leq m$, the points x_c are vertices of Y_m.

B.5.18. Theorem. (i) *The graph* $\mathrm{GL}_2(A)\backslash T$ *is a union of subgraphs* Y_m *and* Δ_c *for all* $c \in \mathrm{Pic}(A)$.
(ii) *We have* $\mathrm{vert}(Y_m) \cap \mathrm{vert}(\Delta_c) = \{x_c\}$ *and* $\mathrm{line}(Y_m) \cap \mathrm{line}(\Delta_c) = \emptyset$.
(iii) *The graph* Y_m *is finite.*

Proof. (i) Let x be a vertex of $\mathrm{GL}_2(A)\backslash T$ and let $\mathcal{E}$ be the locally free sheaf of rank 2 corresponding to x. If $N(\mathcal{E}) \leq m$ then x is a vertex of Y_m by definition of Y_m. If $N(\mathcal{E}) \geq m$ there is a line sub-bundle $\mathcal{L}$ of $\mathcal{E}$ such that $N(\mathcal{E}, \mathcal{L}) \geq m$. As $m > 2g - 2$, proposition B.5.12 shows that $\mathcal{L}$ is a direct factor of $\mathcal{E}$. Therefore $\mathcal{E} = \mathcal{L} \oplus \mathcal{L}'$. Let $c \in \mathrm{Pic}(A)$ be the class of the restriction of $\mathcal{L}$ to C_{aff}. Tensoring $\mathcal{E}$ by a power of $\mathcal{I}_\infty$ if necessary, we may assume that $\mathcal{L} = \mathcal{F}_c$ (definition B.5.15). As $\det(\mathcal{E})$ is a power of $\mathcal{I}_\infty$ (lemma B.5.6), we then have that $\mathcal{L}'$ is isomorphic to $\mathcal{I}_\infty^{\otimes n} \otimes_{\mathcal{O}_C} \mathcal{F}_c^{-1}$ where $n \in \mathbb{Z}$. That is to say, $\mathcal{E} \cong \mathcal{E}_{c,n}$

and $x = x_{c,n}$. The hypothesis $N(\mathcal{E}, \mathcal{L}) \geq m$ means that $2f_c + nd \geq m$; in view of the definition of n_c, this implies that $n \geq n_c$ and shows that x is a vertex of Δ_c. We therefore have

$$\mathrm{vert}(\mathrm{GL}_2(A)\backslash T) = \mathrm{vert}(Y_m) \cup \bigcup_{c \in \mathrm{Pic}(A)} \mathrm{vert}(\Delta_c).$$

Suppose now that y is a line of $\mathrm{GL}_2(A)\backslash T$. If the two extremities of y lie in Y_m then y is a line of the graph Y_m by definition of Y_m. If one of the extremities does not lie in Y_m, it is a vertex $x_{c,n}$ of one of the Δ_c and we have $x_{c,n} \neq x_c$ whence $n \geq n_c + 1$ and

$$(n-1)d \geq n_c d > 2g - 2 - 2f_c$$

(see (b)). By proposition B.5.16, this gives that y is a line of Δ_c. Therefore we have

$$\mathrm{line}(\mathrm{GL}_2(A)\backslash T) = \mathrm{line}(Y_m) \cup \bigcup_c \mathrm{line}(\Delta_c).$$

(ii) Let $x_{c,n} \in \mathrm{vert}(Y_m) \cap \mathrm{vert}(\Delta_c)$. As $x_{c,n}$ lies in Y_m we have $N(\mathcal{E}_{c,n}) \leq m$, that is to say that $2f_c + dn \leq m$. In view of the definition of n_c and the hypothesis that $n \geq n_c$, as $x_{c,n} \in \mathrm{vert}(\Delta_c)$, this implies that $n = n_c$ and we then have $\mathrm{vert}(Y_m) \cap \mathrm{vert}(\Delta_c)$ is reduced to one point $x_{c,n}$.

That we have $\mathrm{line}(Y_m) \cap \mathrm{line}(\Delta_c) = \emptyset$ is evident because no vertex of Δ_c can have both extremities equal to x_c.

(iii) The vertices of $\mathrm{GL}_2(A)\backslash T$ corresponding to indecomposable bundles on C are vertices of Y_m as all vertices of Δ_c correspond to decomposable bundles. This subset of $\mathrm{vert}(Y_m)$ is finite by exercise B.5.21(1).

Furthermore, the decomposable bundles $\mathcal{E} = \mathcal{L} \oplus \mathcal{L}'$ on C corresponding to vertices in Y_m satisfy $-2g \leq N(\mathcal{E}) \leq m$ and $\det(\mathcal{E})$ is isomorphic to $\mathcal{O}_C$ or $\mathcal{I}_\infty$ (see proposition B.5.7); it follows that both $\deg(\mathcal{L})$ and $\deg(\mathcal{L}')$ are bounded. Hence there are only finitely many isomorphism classes of such decomposable bundles $\mathcal{E}$. Hence this subset of $\mathrm{vert}(Y_m)$ corresponding to decomposable bundles is also finite. Therefore Y_m is finite. □

B.5.19. Corollary. *The inclusion $Y_m \to \mathrm{GL}_2(A)\backslash T$ is a homotopy equivalence. The graph Y_m is connected and finite.*

Proof. The only point to check is the connectedness of Y_m. This holds as Y_m is obtained from a quotient of a tree.□

B.5.20. Corollary. *Suppose that Γ is a subgroup of $\mathrm{GL}_2(A)$ of finite index. Then the graph $\Gamma\backslash T$ is homotopic to a finite connected graph.*

Proof. As there are surjective morphisms of graphs $T \to \Gamma\backslash T \to \mathrm{GL}_2(A)\backslash T$ where the second morphism is a finite covering and T is a tree, this result follows from the preceding corollary. □

B.5.21. Exercises. (1) (i) Let $\mathcal{L}, \mathcal{L}'$ be two line bundles on C. Show that there are only finitely many isomorphism classes of extensions of $\mathcal{L}$ by $\mathcal{L}'$.

(ii) Let $c \in \mathrm{Pic}(C)$. Show that there are only finitely many isomorphism classes of indecomposable locally free sheaves $\mathcal{E}$ of rank 2 such that $\det(\mathcal{E})$ is of class c.

[Show that $N(\mathcal{E})$ takes only finitely many values, by propositions B.5.10 and B.5.12, and then use (i).]

(iii) Show that that part of $\mathrm{GL}_2(A)\backslash T$ which corresponds to indecomposable rank 2 locally free sheaves on C is finite.

[It is essential for this exercise that the ground field k be finite.]

(2) Suppose that the locally free sheaf $\mathcal{E}$ of rank 2 on C is decomposable. Show that the decomposition $\mathcal{E} = \mathcal{L}_1 \oplus \mathcal{L}_2$ as a sum of 2 line bundles $\mathcal{L}_1$, $\mathcal{L}_2$ on C is unique up to automorphism of $\mathcal{E}$.

[Let $\mathcal{J}_1 \oplus \mathcal{J}_2$ be a second decomposition of $\mathcal{E}$ and consider $\Gamma(C, \mathcal{L}_i \otimes_{\mathcal{O}_C} \mathcal{J}_j^{-1})$ for all i, j.]

(3) Suppose that C is the projective line $\mathbb{P}_1$ over the finite field k. Let d be the degree over k of the point ∞. Let $\mathcal{F}$ be a line bundle on C of degree 1.

(i) Show that every locally free sheaf $\mathcal{E}$ of rank 2 on C is decomposable and that there are integers $a, b \in \mathbb{Z}$ such that $\mathcal{E} \cong \mathcal{E}_{a,b}$ where

$$\mathcal{E}_{a,b} \cong \mathcal{F}^{\otimes a} \oplus \mathcal{F}^{\otimes b}.$$

[Use propositions B.5.10 and B.5.12.]

(ii) Show that the restriction of $\mathcal{E}_{a,b}$ to $C \setminus \{\infty\}$ is trivial if and only if $a \equiv -b \pmod{d}$. Denote by $v(a, b)$ the vertex of $\mathrm{GL}_2(A)\backslash T$ corresponding to $\mathcal{E}_{a,b}$ in this case where $a \equiv -b \pmod{d}$.

(iii) Show that the distinct vertices of $\mathrm{GL}_2(A)\backslash T$ are precisely the vertices $v(nd - b, b)$, where $n, b \in \mathbb{N}$, $0 \leq b < d$, $n \geq 1$, and where $n \geq 2$ if $d \geq d/2$.

(iv) Show that if $d = 1$ then $\mathrm{GL}_2(A)\backslash T$ is the infinite half line $v(n, 0)$, $n \in \mathbb{N}$, where there is at most one line joining a pair of vertices.

Show that if $d = 2$, then $\mathrm{GL}_2(A)\backslash T$ is the infinite line with vertices $v(2n, 0)$, $v(2n+1, 1)$, $n \in \mathbb{N}$, where there is at most one line joining a pair of vertices.

[For the cases where $d > 2$ see [S4, §2.4 and Exercice 2.4(2)].]

B.6 Cohomology of Ω^2 and harmonic cochains

The étale cohomology of rigid analytic spaces is defined in §A.4 only for H^0 and H^1 and for the coefficients the group μ_n of nth roots of unity and the group $\mathbb{Z}/n\mathbb{Z}$ where n is any integer prime to the characteristic of the ground field; this is all that is required for this appendix.

[For more details on the étale cohomology of rigid analytic spaces, see [Be] and [Hu].]

B.6.1. Proposition. *Let $D_0, \ldots, D_m$ be $m+1$ pairwise disjoint open discs in $\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ of radius in $|\widehat{\overline{F}}_\infty|$. Let n be an integer prime to the characteristic of the field F_∞. Then the rigid analytic space*

$$X = \mathbb{P}_1(\widehat{\overline{F}}_\infty) \setminus \bigcup_{i=0}^{m} D_i$$

has cohomology given by

(a) $H^0_{\text{ét}}(X \otimes_{F_\infty} F_\infty^{\text{sep}}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$;
(b) $H^1_{\text{ét}}(X \otimes_{F_\infty} F_\infty^{\text{sep}}, \mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^m$.

Proof. (a) The open unit disc $\{x|\ |x| < 1\}$ is geometrically connected, as it is the maximal spectrum of the Tate algebra $F_\infty\{x\}$ (see §A.2); hence every open disc in $\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ is geometrically connected. Since $X \cup D_1 \cup \ldots D_m = \mathbb{P}_1(\widehat{\overline{F}}_\infty) \setminus D_0$ is a disc and hence geometrically connected and since the spherical boundaries of the D_i are geometrically connected, it follows that X is geometrically connected.
(b) Every divisor on X is principal hence we have $H^1_{\text{rigid}}(X, \mathcal{O}_X^*) = 0$. The set of rational functions without poles on X is everywhere dense in $H^0_{\text{rigid}}(X, \mathcal{O}_X)$. If $f \in H^0_{\text{rigid}}(X, \mathcal{O}_X)$ and $\sup_{x\in X} |f(x)-1| < 1$ then evidently $f = g^n$ for some $g \in H^0_{\text{rigid}}(X, \mathcal{O}_X)$. Therefore every element of $H^0_{\text{rigid}}(X, \mathcal{O}_X^*) \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ can be represented by a rational function. Furthermore, the natural homomorphism $H^0_{\text{rigid}}(X, \mathcal{O}_X^*) \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to H^1_{\text{ét}}(X, \mu_n)$ is surjective by proposition A.4.5.

If f is a rational function on $\mathbb{P}_1/F_\infty$ whose divisor in $\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ is contained in precisely one of the discs D_i then there is $c \in F_\infty$ such that $\sup_{x\in X} |cf(x) - 1| < 1$ (see exercise B.6.4); hence we have $cf = g^n$ for some $g \in H^0_{\text{rigid}}(X, \mathcal{O}_X)$. We then obtain a surjective homomorphism

$$\phi : (\mathbb{Z}/n\mathbb{Z})^m \to H^1_{\text{ét}}(X, \mu_n)/[F_\infty^*/F_\infty^{*n}].$$

The algebra $F_\infty\{z, z^{-1}\}$ (see §A.2) has maximal spectrum which is a circle B of radius 1 given by $|z| = 1$. Let j be an integer such that n does not divide j and let $\mathfrak{m}$ be the maximal ideal of O_∞. If z^j were an nth power in $F_\infty\{z, z^{-1}\}$, we would have $z^j = f^n$ where $\| f \| = 1$ and where $\| \cdot \|$ is the norm on $F_\infty\{z, z^{-1}\}$ (see §A.2); it would follow that z^j (modulo $\mathfrak{m}$) would be an nth power in $\kappa(\infty)[z, z^{-1}]$ which is not the case. Hence z^j is not an nth power in $F_\infty\{z, z^{-1}\}$. It follows that

$$H^1_{\text{ét}}(B, \mu_n)/[F_\infty^*/F_\infty^{*n}] \cong \mathbb{Z}/n\mathbb{Z}.$$

Let S_i be the boundary of D_i for all i. Then S_i is a circle of radius c_i, say, where $c_i \in |\widehat{\overline{F}}_\infty|$. We then obtain the isomorphism

$$H^1_{\text{ét}}(S_i, , \mu_n)/[F_\infty^*/F_\infty^{*n}] \cong \mathbb{Z}/n\mathbb{Z}.$$

It follows that the homomorphism ϕ is an isomorphism and we then obtain the exact sequence

$$0 \to F_\infty^*/F_\infty^{*n} \to H^1_{\text{ét}}(X, \mu_n) \to (\mathbb{Z}/n\mathbb{Z})^m \to 0.$$

Passing to the separable algebraic closure of F_∞ gives the isomorphism

$$H^1_{\text{ét}}(X \otimes_{F_\infty} F_\infty^{\text{sep}}, \mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^m. \quad \square$$

B.6.2. Definition. Let M be an abelian group and let G be a (possibly infinite) graph (see definition B.5.13). Let E be the set of *oriented edges* of G. The edge with the opposite orientation to an edge $e \in E$ is denoted $e^* \in E$.

The group of 1-cochains $C^1(G, M)$ is the subgoup of M^E of elements c such that $c(e^*) = -c(e)$.

The group of *harmonic cochains* $\mathcal{H}^1_{\text{harm}}(G, M)$ is the subgroup of $c \in C^1(G, M)$ such that the sum of the values of the cochain c on all edges emanating from a single vertex is equal to 0 and where this holds for every vertex of G.

B.6.3. Proposition. *Denote by T the Bruhat-Tits building $I(F_\infty^2)_{\mathbb{R}}$ (see §B.3). Let n be an integer prime to the characteristic of the field F_∞. The building map $\lambda : \Omega^2 \to T$ induces isomorphisms which are compatible with the action of* $\mathrm{GL}_2(F_\infty)$

$$H^0_{\text{ét}}(\Omega^2 \times_{F_\infty} F_\infty^{\text{sep}}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$

$$H^1_{\text{ét}}(\Omega^2 \times_{F_\infty} F_\infty^{\text{sep}}, \mu_n) \cong \mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z}).$$

The group $\mathrm{Gal}(F_\infty^{\text{sep}}/F_\infty)$ *acts trivially on both groups.*

Proof. Put $X = \Omega^2$. Define an admissible affine covering $X = \bigcup_{i \in I} X_i$ of X where I is the set of vertices and edges (the simplices) of the tree T as follows. If i is a vertex v, then X_i is $\lambda^{-1}(B^*(v, 1/3))$ and if i is an edge e then X_i is equal to

$$\lambda^{-1}\big(e \setminus \bigcup_v B(v, 1/4)\big)$$

where the union is over all vertices of T. The nerve of this covering has vertices I and is the first barycentric subdivision of the simplicial complex T. Furthermore this covering is $\mathrm{GL}_2(F_\infty)$-invariant.

We have by corollary B.3.4 and exercise B.3.5(3) that if i is a vertex then X_i is $\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ minus $(q_\infty + 1)$ closed discs and if i is an edge then X_i is

$\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ minus two disjoint closed discs. Furthermore, if i is a vertex and j is an edge emanating from i then we have that $X_i \cap X_j$ is $\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ minus two disjoint closed discs.

For two simplices $i, j \in I$, the space $X_i \cap X_j$ is isomorphic to a space of the type considered in proposition B.4.1. Since $X_i \cap X_j$ is geometrically connected and the tree T is connected, it follows that $X = \Omega^2$ is geometrically connected. This proves the isomorphism $H^0_{\text{ét}}(\Omega^2 \times_{F_\infty} F_\infty^{\text{sep}}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

Let E be the subset of I of elements $i \in I$ corresponding to the edges. Choose orientations for each edge $i \in E$. Select isomorphisms for all edges $i \in E$

$$H^1_{\text{ét}}(X_i, \mu_n) \cong \mathbb{Z}/n\mathbb{Z}$$

by proposition B.6.1 and exercise B.3.5(3). Furthermore, if i is a vertex we have an isomorphism by proposition B.6.1

$$H^1_{\text{ét}}(X_i, \mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^{q_\infty}.$$

We have for all $i \neq j$

$$H^1_{\text{ét}}(X_i \cap X_j, \mu_n) \cong 0$$

unless i is a vertex and j is an edge emanating from i (or vice versa); in the latter case we have

$$H^1_{\text{ét}}(X_i \cap X_j, \mu_n) \cong \mathbb{Z}/n\mathbb{Z}$$

by proposition B.6.1. By proposition A.4.6 we have the exact sequence

$$0 \to H^0_{\text{ét}}(X, \mu_n) \to \prod_{i \in I} H^0_{\text{ét}}(X_i, \mu_n) \to \prod_{i \neq j} H^0_{\text{ét}}(X_i \cap X_j, \mu_n)$$

$$\to H^1_{\text{ét}}(X, \mu_n) \to \prod_{i \in I} H^1_{\text{ét}}(X_i, \mu_n) \to \prod_{i \neq j} H^1_{\text{ét}}(X_i \cap X_j, \mu_n).$$

We have the composite homomorphism

$$H^1_{\text{ét}}(X, \mu_n) \to \prod_{i \in I} H^1_{\text{ét}}(X_i, \mu_n) \to \prod_{i \in E} H^1_{\text{ét}}(X_i, \mu_n) \cong \prod_{i \in E} \mathbb{Z}/n\mathbb{Z}.$$

This provides an isomorphism

$$H^1_{\text{ét}}(X, \mu_n) \to \mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z})$$

where this map is injective, by the previous exact sequence and proposition B.6.1, and the image consists precisely of those functions in $\prod_{i \in E} \mathbb{Z}/n\mathbb{Z}$, extended to be alternating on all ordered edges, which are harmonic.□

B.6.4. Exercise. Let f be a rational function on $\mathbb{P}_1/F_\infty$ defined over F_∞ whose divisor in $\mathbb{P}_1(\widehat{\overline{F}}_\infty)$ is contained in the open disc $D = \{z| \ |z - a| < |b|\}$ where $a, b \in F_\infty^{\text{sep}}$ and where z is a parameter on $\mathbb{P}_1/F_\infty$. Let $X = \mathbb{P}_1(\widehat{\overline{F}}_\infty) \setminus D$. Show that there is $\alpha \in F_\infty$ such that $\sup_{x \in X} |\alpha f(x) - 1| < 1$.

B.7 Cohomology of the moduli space M_H^2

(B.7.1) Let U_I be the congruence subgroup of $\mathrm{GL}_2(A)$ corresponding to the ideal I of A, that is to say

$$U_I = \ker\{\mathrm{GL}_2(A) \to \mathrm{GL}_2(A/I)\}.$$

Thus the subgroup U_I consists of those matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in A$ and $b, c \in I$ and whose determinant is a unit of A. As in §A.6, we put

$$\tilde{U}_I = \ker\{\mathrm{GL}_2(\widehat{A}) \to \mathrm{GL}_2(\widehat{A}/I\widehat{A})\}.$$

The building map λ induces a morphism

$$U_I\backslash\Omega^2 \to U_I\backslash T.$$

(B.7.2) Put

$$\tilde{T} = \mathrm{GL}_2(F)\backslash(T \times \mathrm{GL}_2(\mathbb{A}_f)).$$

where $\mathrm{GL}_2(\mathbb{A}_f)$ is considered as a discrete set. As in (A.7.5), we put

$$\tilde{\Omega}^2 = \mathrm{GL}_2(F)\backslash(\Omega^2 \times \mathrm{GL}_2(\mathbb{A}_f)).$$

We have by theorem A.8.7 that if A/I has at least two maximal ideals then there is an isomorphism of rigid analytic spaces

$$\tilde{U}_I\backslash\tilde{\Omega}^2 = (M_I^2 \otimes F_\infty)_{\mathrm{an}}.$$

(B.7.3) Let H be an arithmetic subgroup of $\mathrm{GL}_2(\widehat{A})$ (see §B.4). Then there is a corresponding moduli scheme M_H^2 where we have (proposition B.4.9), for $S \subset \mathrm{GL}_2(\mathbb{A}_f)$ a finite set of representatives of the double cosets $H\backslash\mathrm{GL}_2(\mathbb{A}_f)/\mathrm{GL}_2(F)$,

$$M_H^2(\widehat{\overline{F}}_\infty) = H\backslash\mathrm{GL}_2(\mathbb{A}_f) \times \Omega^2(\widehat{\overline{F}}_\infty)/\mathrm{GL}_2(F) =$$

$$= \coprod_{x \in S} \Omega^2/(xHx^{-1} \cap \mathrm{GL}_2(F))$$

where the disjoint union here is over the finitely representatives of S.

We say that this space M_H^2 is the moduli space of Drinfeld modules "equipped with an H-structure".

Put

$$H_x = xHx^{-1} \cap \mathrm{GL}_2(F)$$

for any double coset $Hx\mathrm{GL}_2(F)$ of $H\backslash\mathrm{GL}_2(\mathbb{A}_f)/\mathrm{GL}_2(F)$.

B.7.4. Proposition. *Assume that the stabiliser in H_x of any vertex or edge of T is a p-group. We have the cohomology sequence, where the coefficients are in $\mathbb{Z}/n\mathbb{Z}$ or μ_n,*

$$(B.7.5) \qquad 0 \to H^1(H_x\backslash T) \to H^1_{\text{ét}}(H_x\backslash \Omega^2) \to \mathcal{H}^1_{\text{harm}}(T)^{H_x} \otimes \mu_n^{-1} \to 0.$$

Proof. Let n be an integer prime to the characteristic p of F. The group H_x acts on the Bruhat-Tits tree $T = I(F^2_\infty)_{\mathbb{R}}$. The building map modulo H_x is then

$$\lambda_{H_x} : H_x\backslash \Omega^2 \to H_x\backslash T.$$

The Leray spectral sequence of this map is the covering space spectral sequence whose exact sequence of terms low degree gives the exact sequence, with coefficients in $\mathbb{Z}/n\mathbb{Z}$ or μ_n,

$$0 \to H^1(H_x\backslash T) \to H^1_{\text{ét}}(H_x\backslash \Omega^2) \to H^1_{\text{ét}}(\Omega^2)^{H_x} \to H^2(H_x\backslash T)$$

As H_x acts on T with stabilizer subgroups of edges and vertices which are p-groups the groups $H^*(H_x\backslash T)$ are the cohomology groups of the discrete group H_x with coefficients in in $\mathbb{Z}/n\mathbb{Z}$ or μ_n. As T is a tree, we have furthermore that $H^2(H_x\backslash T) = 0$.

By proposition B.6.3, the group $H^1_{\text{ét}}(\Omega^2, -)^{H_x}$ is isomorphic to $\mathcal{H}^1_{\text{harm}}(T, -)^{H_x}$ the group of H_x-invariant harmonic cochains with coefficients in μ_n^{-1} or $\mathbb{Z}/n\mathbb{Z}$. □

B.7.6. Corollary. *Assume that the stabiliser in H_x of any vertex or edge of T is a p-group. We have the cohomology sequence, where the coefficients are in $\mathbb{Z}/n\mathbb{Z}$ or μ_n,*

$$(B.7.7) \qquad 0 \to H^1(H\backslash \tilde{T}) \to H^1_{\text{ét}}(M^2_H \otimes F^{\text{sep}}_\infty) \to \mathcal{H}^1_{\text{harm}}(\tilde{T})^H \otimes \mu_n^{-1} \to 0.$$

Proof. This follows from the isomorphism of rigid analytic spaces $H\backslash\tilde{\Omega}^2 = (M^2_H \otimes F_\infty)_{\text{an}}$ (theorem A.8.7 and (B.7.1)). □

B.7.8. Definition. The *cuspidal cohomology* $\mathcal{H}^1_{!\ \text{harm}}(T, \mathbb{Z}/n\mathbb{Z}, H_x)$ is the subgroup of $\mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z})^{H_x}$ of harmonic H_x-invariant cochains with compact support modulo H_x. Similarly, the cuspidal cohomology $\mathcal{H}^1_{!\ \text{harm}}(\tilde{T}, \mathbb{Z}/n\mathbb{Z}, H)$ is the subgroup of $\mathcal{H}^1_{\text{harm}}(\tilde{T}, \mathbb{Z}/n\mathbb{Z})^H$ of harmonic H-invariant cochains of $\tilde{T}$ with compact support modulo H.

The cuspidal cohomology $H^1_!(M^2_H \otimes F^{\text{sep}}_\infty, \mathbb{Z}/n\mathbb{Z})$ is then defined by the exact sequence (B.7.7) to be the subgroup of $H^1_{\text{ét}}(M^2_H \otimes F^{\text{sep}}_\infty, \mathbb{Z}/n\mathbb{Z})$ of classes with image in $\mathcal{H}^1_{!\ \text{harm}}(\tilde{T}, \mathbb{Z}/n\mathbb{Z}, H) \otimes \mu_n^{-1}$.

B.7.9. Proposition. *Let I_0 be the inertia subgroup of the galois group $Gal(F_\infty^{\mathrm{sep}}/F_\infty)$. Assume that the stabiliser in H_x of any vertex or edge of T is a p-group. Then $(\sigma, x) \mapsto \sigma x - x$, for $\sigma \in I_0$*

$$I_0 \times H^1_{\text{ét}}(H_x\backslash\Omega^2, \mathbb{Z}/n\mathbb{Z}) \to H^1_{\text{ét}}(H_x\backslash\Omega^2, \mathbb{Z}/n\mathbb{Z})$$

induces a homomorphism

$$f_n : \mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z})^{H_x} \to H^1(H_x\backslash T, \mathbb{Z}/n\mathbb{Z}).$$

This map associates to a H_x-invariant harmonic cochain on T the cohomology class of the corresponding cochain on $H_x\backslash T$.

Proof. In the short exact sequence obtained from (B.7.5) by taking coefficients in $\mathbb{Z}/n\mathbb{Z}$

$$0 \to H^1(H_x\backslash T, \mathbb{Z}/n\mathbb{Z}) \to H^1_{\text{ét}}(H_x\backslash\Omega^2, \mathbb{Z}/n\mathbb{Z}) \to \mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z})^{H_x} \otimes \mu_n^{-1} \to 0$$

the inertia group I_0 acts trivially on the extremities $H^1(H_x\backslash T, \mathbb{Z}/n\mathbb{Z})$ and $\mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z})^{H_x} \otimes \mu_n^{-1}$. It follows that $(\sigma, x) \mapsto \sigma x - x$ defines a map

$$\frac{I_0}{I_0^n} \times H^1_{\text{ét}}(H_x\backslash\Omega^2, \mathbb{Z}/n\mathbb{Z}) \to H^1(H_x\backslash T, \mathbb{Z}/n\mathbb{Z})$$

which is bilinear and $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$-equivariant. The group I_0/I_0^n may be identified with μ_n; hence $\mu_n \times H^1(H_x\backslash T, \mathbb{Z}/n\mathbb{Z})$ lies in the kernel of this map and we obtain a homomorphism

$$f_n : \mathcal{H}^1_{\text{harm}}(T, \mathbb{Z}/n\mathbb{Z})^{H_x} \to H^1(H_x\backslash T, \mathbb{Z}/n\mathbb{Z}).$$

This map associates to a H_x-invariant harmonic cochain on T the cohomology class of the corresponding cochain on $H_x\backslash T$. □

B.7.10. Proposition. *Let l be a prime number distinct from the characteristic of F. Assume that the stabiliser in H_x of any vertex or edge of T is a p-group. Letting n run over all powers l^i of l and tensoring with $\mathbb{Q}_l$, the homomorphisms $\varinjlim f_{l^i} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ above induce an isomorphism of cuspidal cohomology*

$$\varinjlim f_{l^i} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l : \mathcal{H}^1_{!\ \text{harm}}(T, \mathbb{Q}_l, H_x) \to H^1(H_x\backslash T, \mathbb{Q}_l).$$

Proof. Let l be a prime number distinct from the characteristic of F. The quotient $H_x\backslash T$ is a graph, possibly with multiple edges joining two vertices. Let A be the affine coordinate ring $\Gamma(C\backslash\{\infty\}, \mathcal{O}_C)$ of the affine curve $C\backslash\{\infty\}$. As H_x is a subgroup of finite index in $\mathrm{GL}_2(A)$, by theorem B.5.18 and corollary

B.5.20, there is a finite subgraph Y of $H_x\backslash T$ where $(H_x\backslash T) - Y$ consists of a finite number of half-lines. Letting n run over all powers l^i of l and tensoring with $\mathbb{Q}_l$, we obtain that the homomorphisms f_n above induce an isomorphism of cuspidal cohomology (exercise B.7.16(1))

$$\mathcal{H}^1_{!\ \mathrm{harm}}(T, \mathbb{Q}_l, H_x) \to H^1(H_x\backslash T, \mathbb{Q}_l). \quad \square$$

B.7.11. Proposition. *Assume that for all x the stabiliser in H_x of any vertex or edge of T is a p-group. For all integers n prime to p, we have the short exact sequence of cuspidal cohomology*
(*B*.7.12)
$$0 \to H^1(H\backslash\tilde{T}, \frac{\mathbb{Z}}{n\mathbb{Z}}) \to H^1_!(M_H^2 \otimes F_\infty^{\mathrm{sep}}, \frac{\mathbb{Z}}{n\mathbb{Z}}) \to \mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \frac{\mathbb{Z}}{n\mathbb{Z}}, H) \otimes \mu_n^{-1} \to 0.$$

In the limit we obtain the non-split exact sequence of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$*-modules for any prime number l distinct from p*

$$0 \to H^1(H\backslash\tilde{T}, \mathbb{Q}_l) \to H^1_!(M_H^2 \otimes F_\infty^{\mathrm{sep}}, \mathbb{Q}_l) \to \mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \mathbb{Q}_l, H) \otimes \mathbb{Q}_l(-1) \to 0.$$

Proof. The exact sequence (B.7.7) restricted to cuspidal cohomology provides the exact sequence (B.7.12). Taking the projective limit of this sequence as n runs over all integers l^i, and tensoring this with $- \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ we obtain the final exact sequence. The sequence is non-split as by propositions B.7.9 and B.7.10, the invariant subgroup of $H^1_!(M_H^2 \otimes F_\infty^{\mathrm{sep}}, \mathbb{Q}_l)$ under the inertia subgroup I_0 of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ is precisely $H^1(H\backslash\tilde{T}, \mathbb{Q}_l)$. $\square$

(B.7.13) Let π_∞ be a local parameter of O_∞. Let l be a prime number distinct from the characteristic p of F_∞. Let μ_{l^i} be the multiplicative subgroup of F_∞^{sep} of $l^i$the roots of unity. Let $L(i)$ be the subfield of F_∞^{sep} given by $F_\infty(\pi_\infty^{1/l^i}, \mu_{l^i})$.

The field extension $L(i)/F_\infty$ is galois and the galois group is generated by two elements ϕ_i and u_i which satisfy the relation $\phi_i u_i \phi_i^{-1} = u_i^{q_\infty}$. The element u_i acts as

$$u_i(\pi^{1/l^i}) = \zeta\pi^{1/l^i}$$

where ζ is a primitive l^ith root of unity. The element ϕ_i is any element of the galois group $\mathrm{Gal}(L(i)/F_\infty)$ which induces the Frobenius automorphism $x \mapsto x^{q_\infty}$ on the extension of residue fields.

The fields $L(i)$ form a direct system $L(i) \subset L(i+1)$ for all i; the elements ϕ_i, u_i for all i may then be chosen to be compatible with respect to these inclusions that is to say the restrictions of ϕ_{i+1}, u_{i+1} to $L(i)$ are equal to ϕ_i, u_i, respectively.

The field $L = \bigcup_{i\in\mathbb{N}} L(i)$ is galois over F_∞ and its galois group is profinite and topologically generated by two elements ϕ, u which induce elements ϕ_i, u_i

of the group $\mathrm{Gal}(L(i)/F_\infty)$ for all i. The elements ϕ, u satisfy the relation $\phi u \phi^{-1} = u^{q_\infty}$.

B.7.14. Definition. The *special representation* $\mathrm{sp}_{\mathrm{Gal}}$ of the Galois group $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ is the 2-dimensional representation over $\mathbb{Q}_l$ which factors through the profinite galois group $\mathrm{Gal}(L/F)$; this group is topologically generated by the two elements ϕ and u with $\phi u \phi^{-1} = u^{q_\infty}$. This representation

$$\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty) \to \mathrm{GL}(\mathrm{sp}_{\mathrm{Gal}})$$

is given explicitly by the formulae

$$\phi \mapsto \begin{pmatrix} 1 & 0 \\ 0 & q_\infty^{-1} \end{pmatrix}$$

$$u \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The representation $\mathrm{sp}_{\mathrm{Gal}}$ has an invariant 1-dimensional subrepresentation and is the unique representation of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$, up to isomorphism, for which there is a non-split exact sequence (exercise B.7.16(2))

$$0 \to \mathbb{Q}_l \to \mathrm{sp}_{\mathrm{Gal}} \to \mathbb{Q}_l(-1) \to 0.$$

B.7.15. Proposition. *Assume that the stabiliser in H_x of any vertex or edge of T is a p-group. We have an isomorphism of* $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$*-modules*

$$H^1_!(M_H^2 \otimes F_\infty^{\mathrm{sep}}, \mathbb{Q}_l) \cong \mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \mathbb{Q}_l, H) \otimes_{\mathbb{Q}_l} \mathrm{sp}_{\mathrm{Gal}}.$$

Proof. From proposition B.7.10., we have the isomorphism

$$\mathcal{H}^1_{!\ \mathrm{harm}}(T, \mathbb{Q}_l, H_x) \to H^1(H_x \backslash T, \mathbb{Q}_l).$$

where $H_x = xHx^{-1} \cap \mathrm{GL}_2(F)$ for any coset xH of H in $\mathrm{GL}_2(\mathbb{A}_f)$. It follows from (B.7.3) that we have an isomorphism

$$\mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \mathbb{Q}_l, H) \to H^1(H \backslash \tilde{T}, \mathbb{Q}_l).$$

Hence from proposition B.7.11 we obtain the non-split exact sequence of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$-modules

$$0 \to \mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \mathbb{Q}_l, H) \to H^1_!(M_H^2 \otimes F_\infty^{\mathrm{sep}}, \mathbb{Q}_l) \to \mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \mathbb{Q}_l, H) \otimes \mathbb{Q}_l(-1) \to 0.$$

The result now follows immediately. □

B.7.16. Exercises. (1) Let G be a graph (possibly with multiple edges joining pairs of vertices) on which the group U acts as a group of automorphisms. Let R

be a ring. The *valency* of a vertex of G is the number of edges emanating from that vertex. Assume that every vertex of G has finite valency and that the valency of every non-isolated vertex of G is a unit of the ring R.

(i) Show that $U\backslash G$ is also a graph.

(ii) Assume that $U\backslash G$ is a finite graph. Let

$$f : \mathcal{H}^1_{\mathrm{harm}}(G, R)^U \to H^1(U\backslash G, R)$$

be the map associating a harmonic U-invariant cochain on G to the corresponding cochain on $U\backslash G$. Show that f is an isomorphism.

(iii) Let $\mathcal{H}^1_{!\ \mathrm{harm}}(G, R, U)$ denote the group of harmonic cochains on G invariant by U and with compact support modulo U. Let

$$f_! : \mathcal{H}^1_{!\ \mathrm{harm}}(G, R, U) \to H^1(U\backslash G, R)$$

be the map associating a harmonic U-invariant cochain on G to the corresponding cochain on $U\backslash G$. Suppose that there is a finite subgraph Y of $U\backslash G$ such that $(U\backslash G) - Y$ consists of a finite number of disjoint half lines. [A half line is a graph isomorphic to $\mathbb{N}$ where there is an edge joining every pair of consecutive integers.] Show that $f_!$ is an isomorphism.

(2) Let V be a 2-dimensional $\mathbb{Q}_l$-representation of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ which is a non-split extension

$$0 \to \mathbb{Q}_l \to V \to \mathbb{Q}_l(-1) \to 0$$

of the 1-dimensional representations $\mathbb{Q}_l$ and $\mathbb{Q}_l(-1)$ of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$. Show that V is isomorphic to the special representation $\mathrm{sp}_{\mathrm{Gal}}$.

B.8 Harmonic cochains and the special representation of $\mathbf{GL_2}(\boldsymbol{F_\infty})$

(B.8.1) For any $x \in \mathbb{P}_1(F_\infty)$, considered as a 1-dimensional subspace of F_∞^2, denote the quotient linear homomorphism by

$$\gamma_x : F_\infty^2 \to F_\infty^2/x.$$

If Λ is a lattice of F_∞^2 then $\gamma_x(\Lambda)$ as also a lattice in F_∞^2/x.

(B.8.2) For an ordered edge e of T represented by a pair of O_∞-lattices $L_0 \supset L_1$, let $P(e)$ denote the subset of $x \in \mathbb{P}_1(F_\infty)$ such that $\gamma_x(L_1) = \gamma_x(L_0)$.

The sets $P(e)$ generate the Boolean algebra of all open compact subsets of $\mathbb{P}_1(F_\infty)$ (exercise B.8.13).

B.8.3. Remarks. (1) Denote by T the Bruhat-Tits building $I(F_\infty^2)_{\mathbb{R}}$ (see §B.3). For an oriented edge e of T (see (B.6.2)) represented by an ordered pair of lattices $L_0 \supset L_1$ the opposite edge e^* is represented by $L_1 \supset \pi_\infty L_0$. We then

have the inclusions of lattices in the 1-dimensional F_∞-space F_∞^2/x

$$\pi_\infty \gamma_x(L_0) = \gamma_x(\pi_\infty L_0) \subset \gamma_x(L_1) \subset \gamma_x(L_0).$$

It follows that either $\gamma_x(\pi_\infty L_0) = \gamma_x(L_1)$ or that $\gamma_x(L_1) = \gamma_x(L_0)$ but not both equalities simultaneously. In particular, we have a partition of $\mathbb{P}_1(F_\infty)$ as $P(e) \cup P(e^*)$.

(2) The elements of $\mathbb{P}_1(F_\infty)$ may be identified with the *ends* of the tree T.

A point x of $\mathbb{P}_1(F_\infty)$ corresponds to a 1-dimensional subspace aF_∞. Let O_∞^2 be the standard lattice of F_∞^2. Then the end associated to x is the half line in T given by the classes of the lattices $\pi_\infty^{-n} a O_\infty + O_\infty^2$ for $n \in \mathbb{N}$.

Let e be an oriented edge of T. Then the subset $P(e)$ of $\mathbb{P}_1(F_\infty)$, under this identification with ends, is precisely the set of ends of T beginning with the edge e.

(B.8.4) For a ring R, define a map from the harmonic 1-cochains of T into the set of R-valued measures on $\mathbb{P}_1(F_\infty)$

$$\mathcal{H}^1_{\mathrm{harm}}(T, R) \to \mathrm{Meas}(\mathbb{P}_1(F_\infty), R)$$

$$c \mapsto \mu_c$$

by $\mu_c(P(e)) = c(e)$.

B.8.5. Proposition. *The map $c \mapsto \mu_c$ is an isomorphism*

$$\mathcal{H}^1_{\mathrm{harm}}(T, R) \cong \mathrm{Meas}(\mathbb{P}_1(F_\infty), R)_0$$

from the set of R-valued harmonic cochains of T onto the set of R-valued measures on $\mathbb{P}_1(F_\infty)$ of total mass zero.

Proof. Let $e_1, \ldots, e_s$ be the ordered edges emanating from a vertex. The harmonic condition $c(e_1^*) = \sum_{i=2}^s c(e_i)$ (see exercise B.8.13) gives the equation

$$\mu_c(P(e_1^*)) = \sum_{i=2}^{s} \mu_c(P(e_i))$$

It follows that μ_c is a finitely additive function on the set of compact open subsets of $\mathbb{P}_1(F_\infty)$, as the sets $P(e)$ generate the Boolean algebra of all open compact subsets of $\mathbb{P}_1(F_\infty)$. From the partition $\mathbb{P}_1(F_\infty) = P(e) \cup P(e^*)$ (see remarks B.8.3) we obtain that $\mu_c(\mathbb{P}_1(F_\infty)) = 0$.

The inverse of $c \mapsto \mu_c$ is given by $\mu \to c_\mu$ where $c_\mu(e) = \mu(P(e))$. The harmonic condition for the cochain c_μ follows from the finite additivity of μ and that $\mu(\mathbb{P}_1(F_\infty)) = 0$ (see exercise B.8.13(iii)). □

B.8.6. Remark. The measures on $\mathbb{P}_1(F_\infty)$ with values in R are linear functionals on the space of R-valued locally constant functions on $\mathbb{P}_1(F_\infty)$. This

space denoted $C^\infty(\mathbb{P}_1(F_\infty), R)$ is a representation space of $\mathrm{GL}_2(F_\infty)$ and is related to the special representation of the group $\mathrm{GL}_2(F_\infty)$.

B.8.7. Definition. Let R be a ring. Then the *special representation* $V_{\mathrm{sp}}(R)$ of $\mathrm{GL}_2(F_\infty)$ with values in R is the module

$$V_{\mathrm{sp}}(R) = C^\infty(\mathbb{P}_1(F_\infty), R)/R$$

that is to say $V_{\mathrm{sp}}(R)$ is the $\mathrm{GL}_2(F_\infty)$-representation on the space of locally constant functions

$$\mathbb{P}^1(F_\infty) \to R$$

factored out by the constant functions R.

The action of $\mathrm{GL}_2(F_\infty)$ on $V_{\mathrm{sp}}(R)$ is given by

$$(sf)(x) = f(s^{-1}x)$$

for $f \in C^\infty(\mathbb{P}_1(F_\infty), R)$, $x \in \mathbb{P}_1(F_\infty)$ and $s \in \mathrm{GL}_2(F_\infty)$. If R is the field $\overline{\mathbb{Q}}_l$, the algebraic closure of the l-adic field $\mathbb{Q}_l$, then this representation $V_{\mathrm{sp}}(R)$ is an admissible irreducible representation of $\mathrm{GL}_2(F_\infty)$.

B.8.8. Proposition. *The map $c \mapsto \mu_c$ is an isomorphism*

$$\mathcal{H}^1_{\mathrm{harm}}(T, R) \cong \mathrm{Hom}_R(V_{\mathrm{sp}}(R), R)$$

where $\mathrm{Hom}_R(V_{\mathrm{sp}}(R), R)$ is the R-module dual of V_{sp}.

Proof. To the element c is attached the measure μ_c by proposition B.8.5. For any locally constant function $f \in C^\infty(\mathbb{P}_1(F_\infty), R)$ we may integrate with respect to the measure μ_c and obtain $\displaystyle\int_{\mathbb{P}_1(F_\infty)} f d\mu_c \in R$. As the measure μ_c has total mass zero, the map $f \mapsto \displaystyle\int_{\mathbb{P}_1(F_\infty)} f d\mu_c$ then induces an element $\mathrm{Hom}_R(V_{\mathrm{sp}}(R), R)$. The map is evidently bijective. □

B.8.9. Proposition. *There is a natural isomorpism of R-modules*

$$\mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(R), C^\infty(\mathrm{GL}_2(F_\infty), R)) \cong \mathrm{Hom}_R(V_{\mathrm{sp}}(R), R)$$

given by, where i is the identity of the group $\mathrm{GL}_2(F_\infty)$,

$$\{\psi : f \mapsto \psi(f)\} \mapsto \{f \mapsto \psi(f)(i)\}, \quad \text{for } f \in V_{\mathrm{sp}}(R).$$

Proof. The inverse map is given by, for $f \in V_{\mathrm{sp}}(R)$ and $\phi \in \mathrm{Hom}_R(V_{\mathrm{sp}}(R), R)$,

$$\{f \mapsto \phi(f)\} \mapsto \{f \mapsto \{s \mapsto \phi(sf) \text{ for all } s \in \mathrm{GL}_2(F_\infty)\}\}. \quad \square$$

B.8.10. Notation. (1) Let Γ be a subgroup of $\mathrm{GL}_2(F_\infty)$. Then Γ acts on the tree T, the space $\mathbb{P}_1(F_\infty)$, and the representation V_{sp}. Hence the isomorphisms of propositions B.8.5, B.8.8, B.8.9 restrict to isomorphisms of Γ-invariant subgroups

$$\mathcal{H}^1_{\mathrm{harm}}(T, R)^\Gamma \cong \mathrm{Hom}_R(V_{\mathrm{sp}}(R), R)^\Gamma$$
$$\cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(R), C^\infty(\mathrm{GL}_2(F_\infty)/\Gamma, R)).$$

(2) Assume now that Γ is a subgroup of $\mathrm{GL}_2(A)$ of finite index. Let f be a locally constant function on $\mathrm{GL}_2(F_\infty)/\Gamma$. For each parabolic subgroup P over the global field F of $\mathrm{GL}_2(F)$ with unipotent radical U we put

$$f_P(x) = \int_{u \in U/(\Gamma \cap U)} f(xu)du.$$

The subgroup U is conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ by an element of $\mathrm{GL}_2(F)$.

B.8.11. Definition. A locally constant function f on $\mathrm{GL}_2(F_\infty)/\Gamma$ is *cuspidal* if $f_P(x) = 0$ for all parabolic subgroups P of $\mathrm{GL}_2(F)$.

Write $L_0(\mathrm{GL}_2(F_\infty)/\Gamma, R)$ for the subspace of cuspidal elements of $C^\infty(\mathrm{GL}_2(F_\infty)/\Gamma, R)$.

B.8.12. Proposition. *The isomorphism of proposition B.8.8 and B.8.10*

$$\mathcal{H}^1_{\mathrm{harm}}(T, R)^\Gamma \cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(R), C^\infty(\mathrm{GL}_2(F_\infty)/\Gamma, R))$$

restricts to an isomorphism

$$\mathcal{H}^1_{!\ \mathrm{harm}}(T, R, \Gamma) \cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(R), L_0(\mathrm{GL}_2(F_\infty)/\Gamma, R)).$$

[As in (B.7.8), the group $\mathcal{H}^1_{!\ \mathrm{harm}}(T, R, \Gamma)$ denotes the group of harmonic cochains which are Γ-invariant and have compact support modulo Γ.]

Proof. Let $f \in C^\infty(\mathrm{GL}_2(F_\infty)/\Gamma, R)$ be the image of an element of $V_{\mathrm{sp}}(R)$ by a homomorphism in $\mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(R), C^\infty(\mathrm{GL}_2(F_\infty)/\Gamma, R))$. Then the function f is cuspidal if and only if it has compact suppport modulo Γ and the centre of $\mathrm{GL}_2(F_\infty)$ (see [Ha, 1.2.3]). $\square$

B.8.13. Exercise. Let z be a parameter on the projective line $\mathbb{P}_1/F_\infty$.
(i) Show that there is an ordered edge e of the Bruhat-Tits tree T such that $P(e)$ is the open unit disc $\{z \in F_\infty | \ |z| < 1\}$.

(ii) Show that any finite open disc $\{z|\ |z-a|<c\}$, and any open disc at infinity $\{z|\ |z|>c\}$, is of the form $P(e)$ for some ordered edge e of the tree T.
(iii) Let e be an ordered edge of T and e^* be the edge with the opposite orientation. Show that $\mathbb{P}_1(F_\infty) = P(e) \cup P(e^*)$ is a partition of $\mathbb{P}_1(F_\infty)$. If $e_1, \ldots, e_s$ are the ordered edges issuing from a vertex show that there is a partition of $\mathbb{P}_1(F_\infty)$

$$\mathbb{P}_1(F_\infty) = \bigcup_{i=1}^{s} P(e_i)$$

and that there is a partition of $P(e_1^*)$

$$P(e_1^*) = \bigcup_{i=2}^{s} P(e_i)$$

(iv) Shows that the subsets $P(e)$ of $\mathbb{P}_1(F_\infty)$ generate the Boolean algebra of all compact open subsets of $\mathbb{P}_1(F_\infty)$.

B.9 Automorphic forms and the main theorem

(B.9.1) Let $\overline{\mathbb{Q}}_l$ be the algebraic closure of the l-adic field $\mathbb{Q}_l$, where l is a prime number distinct from the characteristic of F. Let $\mathbb{A}$ denote the adèle ring of the global field F.

The space

$$\mathcal{A}_0 = L_0(\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A}))$$

of cuspidal automorphic forms with values in $\overline{\mathbb{Q}}_l$ is the set of functions

$$f : \mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A}) \to \overline{\mathbb{Q}}_l$$

such that

(a) f is invariant by a compact open subgroup;

(b) the $\mathrm{GL}_2(F_\infty)$-transforms of f generate a finite direct sum of irreducible representations;

(c) f is cuspidal, that is to say

$$\int_{\mathbb{A}/F} f(x \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}) dz = 0$$

for all $x \in \mathrm{GL}_2(\mathbb{A})$.

Let f be a function satisfying the conditions (a) and (b). Then f is in $\mathcal{A}_0$ if and only if f has compact support modulo the centre of GL_2 (see [Ha, 1.2.3]).

B.9.2. Proposition. *We have an isomorphism*

$$\mathcal{H}^1_{\mathrm{harm}}(T, C^\infty(\mathrm{GL}_2(\mathbb{A}_f), \overline{\mathbb{Q}}_l))$$

$$\cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), C^\infty(\mathrm{GL}_2(\mathbb{A}_f) \times \mathrm{GL}_2(F_\infty), \overline{\mathbb{Q}}_l)).$$

Proof. We put

$$R = C^\infty(\mathrm{GL}_2(\mathbb{A}_f), \overline{\mathbb{Q}}_l)$$

in proposition B.8.12, where $\mathbb{A}_f$ denotes the ring of finite adèles. □

B.9.3. Proposition. *Let H be an arithmetic subgroup of $\mathrm{GL}_2(\widehat{A})$, where $\widehat{A}$ is the profinite completion of A. Assume that the stabiliser in H_x of any vertex or edge of T is a p-group. There is isomorphism of (centralizer(H) in $\mathrm{GL}_2(\mathbb{A}_f)) \times \mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$-representations*

$$\theta_H : H^1_!(M^2_H \otimes F_\infty^{\mathrm{sep}}, \overline{\mathbb{Q}}_l) \cong$$

$$\mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), L_0(\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/H, \overline{\mathbb{Q}}_l)) \otimes_{\mathbb{Q}_l} \mathrm{sp}_{\mathrm{Gal}}.$$

Proof. From proposition B.9.2 we have an isomorphism

$$\theta : \mathcal{H}^1_{\mathrm{harm}}(T, C^\infty(\mathrm{GL}_2(\mathbb{A}_f), \overline{\mathbb{Q}}_l))$$

$$\cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), C^\infty(\mathrm{GL}_2(\mathbb{A}_f) \times \mathrm{GL}_2(F_\infty), \overline{\mathbb{Q}}_l)).$$

We have from proposition B.7.15 the isomorphism

$$H^1_!(M^2_H \otimes F_\infty^{\mathrm{sep}}, \overline{\mathbb{Q}}_l) \cong \mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \overline{\mathbb{Q}}_l, H) \otimes_{\mathbb{Q}_l} \mathrm{sp}_{\mathrm{Gal}}.$$

We have the two coset descriptions of M^2_H (proposition B.4.9)

$$M^2_H(\widehat{\overline{F}}_\infty) = \mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A}_f) \times \Omega^2(\widehat{\overline{F}}_\infty)/H$$

$$= \coprod_{xH \in \mathrm{GL}_2(\mathbb{A}_f)/H} \Omega^2(\widehat{\overline{F}}_\infty)/(xHx^{-1} \cap \mathrm{GL}_2(F)).$$

Put, as in proposition B.7.4, $H_x = xHx^{-1} \cap \mathrm{GL}_2(F)$ for any coset xH of H in $\mathrm{GL}_2(\mathbb{A}_f)$.

From proposition B.8.12, we have the isomorphism

$$\mathcal{H}^1_{!\mathrm{harm}}(T, \overline{\mathbb{Q}}_l, H_x) \cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), L_0(\mathrm{GL}_2(F_\infty)/H_x, \overline{\mathbb{Q}}_l)).$$

Hence we obtain the isomorphisms

$$\mathcal{H}^1_{!\ \mathrm{harm}}(\tilde{T}, \overline{\mathbb{Q}}_l, H)$$

$$\cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), L_0(\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(F_\infty) \times \mathrm{GL}_2(\mathbb{A}_f)/H, \overline{\mathbb{Q}}_l)$$

$$\cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), L_0(\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/H, \overline{\mathbb{Q}}_l).$$

We obtain an isomorphism

$$\theta_H : H^1_!(M^2_H \otimes F^{\mathrm{sep}}_\infty, \overline{\mathbb{Q}}_l) \cong$$

$$\mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), L_0(\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/H, \overline{\mathbb{Q}}_l)) \otimes_{\mathbb{Q}_l} \mathrm{sp}_{\mathrm{Gal}}. \quad \square$$

B.9.4. Main Theorem. *We have an isomorphism of* $\mathrm{GL}_2(\mathbb{A}_f) \times \mathrm{Gal}(F^{\mathrm{sep}}_\infty/F_\infty)$*-representations where the limit runs over all arithmetic subgroups* H *of* $\mathrm{GL}_2(\widehat{A})$

$$\varinjlim H^1_!(M^2_H \times F^{\mathrm{sep}}_\infty, \overline{\mathbb{Q}}_l) \cong \mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), \mathcal{A}_0) \otimes_{\mathbb{Q}_l} \mathrm{sp}_{\mathrm{Gal}}.$$

Proof. The subgroups $\tilde{U}_I$ are cofinal in the category of arithmetic subgroups of $\mathrm{GL}_2(\widehat{A})$; the groups $\tilde{U}_I$ satisfy the condition that the stabiliser in H_x of any vertex or edge of T is a p-group. Hence the theorem follows from proposition B.9.3 by passing to the limit over all H, where H runs over all arithmetic subgroups of $\mathrm{GL}_2(\widehat{A})$. $\square$

B.9.5. Remarks. (1) This last theorem is one of the principal results of Drinfeld's paper [Dr1].
(2) A fundamental result [J-L, prop. 11.1.1] in the theory of automorphic forms for GL_2, is that the representation of $\mathrm{GL}_2(\mathbb{A})$ on $\mathcal{A}_0$ decomposes as a sum of admissible irreducible representations with multiplicity 1

$$\mathcal{A}_0 = \bigoplus_{\pi \in \Pi} \pi$$

where Π is a set of irreducible admissible representations of the adèle group $\mathrm{GL}_2(\mathbb{A})$.

Each representation π in Π decomposes as a tensor product $\pi = \otimes_v \pi_v$ over all places v of F where π_v is an irreducible admissible representation with a $\mathrm{GL}_2(O_v)$-invariant vector for all but finitely many places v of F, where O_v denotes the completion of the local ring $O_{X,v}$ of X at v.

B.9.6. Corollary. *We have an isomorphism of* $\mathrm{GL}_2(\mathbb{A}_f) \times \mathrm{Gal}(F^{\mathrm{sep}}_\infty/F_\infty)$*-representations*

$$\varinjlim H^1_!(M^2_H \times F^{\mathrm{sep}}_\infty, \overline{\mathbb{Q}}_l) \cong \left(\bigoplus_{\substack{\pi \in \Pi \\ \pi_\infty \cong V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)}} \bigotimes_{v \neq \infty} \pi_v \right) \otimes \mathrm{sp}_{\mathrm{Gal}}.$$

Proof. The module $V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)$ is an admissible irreducible representation of $\mathrm{GL}_2(F_\infty)$. For a representation $\pi \in \mathit{\Pi}$ over $\overline{\mathbb{Q}}_l$ of $\mathrm{GL}_2(\mathbb{A})$, we have $\mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), \pi)$ is equal to zero unless the component π_∞ of π is isomorphic to $V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)$. This gives the isomorphism of the corollary where $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ acts trivially on $(\bigotimes_{v\neq\infty} \pi_v) \otimes \mathrm{sp}_{\mathrm{Gal}}$ except for the last component $\mathrm{sp}_{\mathrm{Gal}}$. □

(B.9.7) Let $\mathit{\Pi}_\infty$ be the subset of $\mathit{\Pi}$ of irreducible admissible representations of the adèle group $\mathrm{GL}_2(\mathbb{A})$. which are isomorphic to the special representation $V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)$, at ∞.

(B.9.8) Let $\mathit{\Sigma}_\infty$ be the set of isomorphism classes of 2-dimensional $\overline{\mathbb{Q}}_l$-representations of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$$

which are ramified at only finitely many places of F and such that the restriction of ρ to the subgroup $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ is isomorphic to the special representation $\mathrm{sp}_{\mathrm{Gal}}$.

B.9.9. Corollary. *There is a map*

$$\mathit{\Pi}_\infty \longrightarrow \mathit{\Sigma}_\infty, \quad \pi \mapsto \sigma(\pi)$$

and an isomorphism of $\mathrm{GL}_2(\mathbb{A}_f) \times \mathrm{Gal}(F^{\mathrm{sep}}/F)$*-modules*

$$\varinjlim H^1_!(M^2_H \times_F F^{\mathrm{sep}}, \overline{\mathbb{Q}}_l) \cong \bigoplus_{\pi\in\mathit{\Pi}_\infty} \Big[(\bigotimes_{v\neq\infty} \pi_v) \otimes \sigma(\pi) \Big].$$

Proof. The group $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ is a subgroup of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$. It follows that as a $\mathrm{GL}_2(\mathbb{A}_f) \times \mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$-module, the cohomology group $\varinjlim H^1_!(M^2_H \times F^{\mathrm{sep}}, \overline{\mathbb{Q}}_l)$ is isomorphic to $\bigoplus_{\substack{\pi\in\mathit{\Pi} \\ \pi_\infty \cong V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)}} [(\bigotimes_{v\neq\infty} \pi_v) \otimes \mathrm{sp}_{\mathrm{Gal}}]$ from the previous corollary B.9.6. The action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ commutes with the action of $\mathrm{GL}_2(\mathbb{A}_f)$; for any $\pi \in \mathit{\Pi}_\infty$, the module $\bigotimes_{v\neq\infty} \pi_v$ is an irreducible representation of $\mathrm{GL}_2(\mathbb{A}_f)$ hence the group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts on the 2-dimensional $\overline{\mathbb{Q}}_l$-space $\mathrm{sp}_{\mathrm{Gal}}$, where this representation depends on π. Denoting this representation of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ by $\sigma(\pi)$, we obtain the isomorphism of the corollary.□

B.10 The Langlands correspondence $\pi \longrightarrow \sigma(\pi)$

(B.10.1) Let W be the Weil group of the global field F; that is to say, W consists of elements of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ whose image in $\widehat{\mathbb{Z}}$ belongs to $\mathbb{Z}$ under the

restriction homomorphism to $\mathrm{Gal}(k^{\mathrm{sep}}/k) \cong \widehat{\mathbb{Z}}$. The topology on W is that induced by the embedding $W \subseteq \mathrm{Gal}(F^{\mathrm{sep}}/F) \times \mathbb{Z}$.

If v is a place of F, let F_v denote the completion of F at v. Let W_v denote the Weil group of F_v, that is to say, W_v consists of elements of $\mathrm{Gal}(F_v^{\mathrm{sep}}/F_v)$ whose image in $\widehat{\mathbb{Z}}$ belongs to $\mathbb{Z}$ under the restriction homomorphism to $\mathrm{Gal}(k^{\mathrm{sep}}/k) \cong \widehat{\mathbb{Z}}$.

(B.10.2) Let E be a number field, that is to say a finite extension field of $\mathbb{Q}$. Denote by $\Psi(E)$ the set of isomorphism classes of compatible systems $\{\rho_\lambda\}_\lambda$ of absolutely irreducible 2-dimensional λ-adic representations of W

$$\rho_\lambda : W \to \mathrm{GL}_2(E_\lambda)$$

where λ runs over all non-archimedean places of E which do not divide the characteristic of F.

The system of representations $\{\rho_\lambda\}_\lambda$ of the Weil group W is *compatible* if for every place v of F and every element $g \in W$ then the trace $\mathrm{tr}(\rho_\lambda(g))$ belongs to E and is independent of the place λ.

(B.10.3) Put

$$\Psi = \varinjlim_{E} \Psi(E)$$

where E runs over all number fields.

Let Ψ_∞ denote the subset of Ψ of compatible systems of representations which are isomorphic to the special representation $\mathrm{sp}_{\mathrm{Gal}}$ at ∞ (see also (B.9.8)).

(B.10.4) Let Π be the set of isomorphism classes of irreducible admissible cuspidal representations of $\mathrm{GL}_2(\mathbb{A})$ over $\overline{\mathbb{Q}}_l$. Let Π_∞ be the subset of Π of representations which are isomorphic to the special representation $V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)$ at ∞, as in (B.9.7).

(B.10.5) Let E be a number field and $\rho = \{\rho_\lambda\}_\lambda$ be an element of $\Psi(E)$ and let $\pi \in \Pi$. The representation π is said to be *compatible with* ρ if for some place λ of E and almost all places v of F then

$$L(s - \frac{1}{2}, \pi_v) = \det(1 - f_v q_v^{-s}, \rho_\lambda)^{-1}$$

where L denotes the Jacquet-Langlands L-function, $f_v \in W$ is a geometric frobenius element at v and q_v is the order of the residue field of F_v at v.

Let $\rho = \{\rho_\lambda\}_\lambda$ be an element of Ψ and let $\pi \in \Pi$. The π is said to be *compatible with* ρ if there is a number field E and an element ρ_E of $\Psi(E)$ such that ρ is the image of ρ_E and π is compatible with ρ_E.

B.10.6. Theorem. (Drinfeld) *Let Γ be the subset of pairs $(\rho, \pi) \in \Psi_\infty \times \Pi_\infty$ such that π is compatible with ρ. Then Γ is the graph of a bijection $\Psi_\infty \cong \Pi_\infty$.*

Sketch proof. The surjectivity of the projection $\Gamma \to \Psi_\infty$ is a consequence of results of [D1]. The projection $\Gamma \to \Psi_\infty$ is injective because an irreducible cuspidal representation of $\mathrm{GL}_2(\mathbb{A})$ is uniquely determined by all but finitely many local components.

That $\Gamma \to \Pi_\infty$ is injective follows from the Čebotarev density theorem. It remains to prove the surjectivity of $\Gamma \to \Pi_\infty$.

Let $\pi \in \Pi_\infty$. By theorem 8.3 and corollary 8.8, there is a representation $\sigma(\pi)$. It remains to show that π is compatible with $\sigma(\pi)$; for this see [Dr1] or [DH]. □

B.10.7. Remark. Drinfeld [Dr2, Dr3] also proves that the compatibility of representations of Π and Ψ induces a bijection $\Pi \to \Psi$. For this, Drinfeld introduces the moduli schemes of stukas; Drinfeld modules are special cases of Drinfeld's stukas, but this is not an obvious consequence of the definition of stukas.

Lafforgue has generalised Drinfeld's proof to GL_n for all integers n (see [La] or §B.12 below).

B.11 Elliptic curves as images of Drinfeld modular curves

The conductor of an elliptic curve

(B.11.1) Let L be a local field of residue characteristic p. For a finite galois extension of fields J/L, let G be the galois group of J/L. Let R be the valuation ring of the field J and let $\mathfrak{p}$ be the maximal ideal of R. The ith higher ramification group is then

$$G_i = \{\sigma \in G |\ \ v(\alpha^\sigma - \alpha) \geq i + 1 \text{ for all } \alpha \in R\}.$$

That is to say, G_i is the normal subgroup of G which acts trivially on $R/\mathfrak{p}^{i+1}$. In particular, G_0 is the inertia subgroup of G. Put $g_i = |G_i|$.

(B.11.2) Let l be a prime number distinct from the residue characteristic of L. Let $\mathbb{F}$ be a finite field of characteristic l. Let W be a finite dimensional representation over $\mathbb{F}$ of $\mathrm{Gal}(J/L)$ that is to say a homomorphism

$$\rho : \mathrm{Gal}(J/L) \longrightarrow \mathrm{End}_{\mathbb{F}}(W).$$

Let I be the inertia subgroup of $\mathrm{Gal}(J/L)$. The *tame part of the conductor*

of ρ is equal to

$$\epsilon(\rho) = \dim_{\mathbb{F}} W/W^I.$$

The *wild part of the conductor* (or the *Swan conductor*) of ρ is equal to

$$\mathrm{sw}(\rho) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \dim_{\mathbb{F}} \left(\frac{W}{W^{G_i}} \right).$$

The *exponent of the conductor* of ρ is then equal to

$$f(\rho) = \epsilon(\rho) + \mathrm{sw}(\rho).$$

(B.11.3) Let E be an elliptic curve defined over the local field L of residue characteristic p. Let $T_l(E)$ be the l-adic Tate module of E/L; put $V_l = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Then V_l is equipped with an action by $\mathrm{Gal}(L^{\mathrm{sep}}/L)$

$$\rho : \mathrm{Gal}(L^{\mathrm{sep}}/L) \longrightarrow \mathrm{End}_{\mathbb{Q}_l}(V_l).$$

Let I be the inertia subgroup of $\mathrm{Gal}(L^{\mathrm{sep}}/L)$. The *tame part of the conductor* of E is equal to

$$\epsilon(E) = \dim_{\mathbb{Q}_l} V_l/V_l^I.$$

Let $E[l]$ be the l-torsion subgroup of E. Let $J = L(E[l])$, that is to say J is the smallest field of rationality over L of the l-torsion points of E. Thus $E[l]$ is a 2-dimensional vector space over $\mathbb{Z}/l\mathbb{Z}$.

The *wild part of the conductor* of E/L is equal to

$$\delta(E) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \dim_{\mathbb{Z}/l\mathbb{Z}} \left(\frac{E[l]}{E[l]^{G_i}} \right).$$

The *exponent of the conductor* of E/L is then

$$f(E/L) = \epsilon(E) + \delta(E).$$

The conductor is independent of the choice of prime number l (see [Si2, Chap. 6, Theorem 10.2]). The conductor $f(E/L)$ is zero if E/L has good reduction.

(B.11.4) Suppose that E is an elliptic curve defined over a global field K. The *conductor* of E/K is then the divisor

$$f(E/K) = \sum_v f(E \otimes_K K_v/K_v).v$$

where the sum runs over all non-archimedean places v of K and where $f(E \otimes_K K_v/K_v)$ is the local exponent of the conductor of $E \otimes_K K_v$ over the local field K_v and where K_v denotes the completion of K at v. This sum

is finite as the curve E/K has good reduction at all but finitely many places of K.

Elliptic curves with split multiplicative reduction

(B.11.5) With the notation of (B.2.1) Let $O_{C,\infty}$ be the local ring of the curve C/k at ∞. Let F_∞ be the completion of F at ∞. Let $|.|$ be the corresponding valuation on the local field F_∞.

(B.11.6) Let E/F be an elliptic curve (that is to say a 1-dimensional abelian variety). The curve E/F has *split multiplicative reduction at* ∞ if the closed fibre over ∞ of the minimal proper smooth model $\mathcal{C}$ of E at ∞ has a node and the tangents at the node are rational over the residue field $\kappa(\infty)$ at ∞.

[See [Si1] for more details.]

(B.11.7) If E/F has split multiplicative reduction at ∞, then the curve E/F is a Tate curve at ∞. That is to say, there is an element $x \in F_\infty^*$, such that $|x|_\infty < 1$, and an isomorphism of rigid analytic tori

$$F_\infty^*/x^{\mathbb{Z}} \cong E(F_\infty).$$

[See [Si2, Chapter V] for more details.]

B.11.8. Proposition. *Suppose that E/F has split multiplicative reduction at ∞. For any prime number l distinct from the characteristic of F, let $T_l(E)$ be the Tate module of E/F. Then there is a non-split exact sequence of* $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$*-modules*

$$0 \to T_l(\mu) \to T_l(E) \to \mathbb{Z}_l \to 0.$$

where $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ *acts trivially on* $\mathbb{Z}_l$.

Proof. There is an isomorphism of abelian groups compatible with the action of $G = \mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ for some element $x \in F_\infty^*$ with $|x|_\infty < 1$

$$F_\infty^{\mathrm{sep}\,*}/x^{\mathbb{Z}} \to E(F_\infty^{\mathrm{sep}}).$$

The l^n-torsion of E is isomorphic to $(\mathbb{Z}/l^n\mathbb{Z})^2$. Fix an l^nth root ζ of x in F_∞^{sep}. The l^n-torsion of $F_\infty^{\mathrm{sep}\,*}/x^{\mathbb{Z}}$ is isomorphic to

$$H = \mu_{l^n}\zeta^{\mathbb{Z}}.$$

It follows that there is a non-split exact sequence of $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$-modules

$$0 \to \mu_{l^n} \to E_{l^n}(F_\infty^{\mathrm{sep}}) \to \mathbb{Z}/l^n\mathbb{Z} \to 0.$$

where $\mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$ acts trivially on $\mathbb{Z}$. Passing to the projective limit gives the exact sequence of the proposition.□

B.11.9. Corollary. *The representation of* $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ *on the l-adic cohomology* $H^1_{\acute{e}t}(E\times_F F^{\mathrm{sep}},\mathbb{Q}_l)$ *is isomorphic to the special representation* $\mathrm{sp}_{\mathrm{Gal}}$ *at* ∞. *The exponent of the conductor of* E *at* ∞ *is equal to* 1. □

Analogue of the Shimura-Taniyama-Weil conjecture for elliptic curves over F

(B.11.10) Let E/F be an elliptic curve. Then for all prime numbers l distinct from the characteristic of F, the cohomology groups $H^1_{\acute{e}t}(E\times_F F^{\mathrm{sep}},\mathbb{Q}_l)$ provide a compatible system of 2-dimensional l-adic representations of the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$

$$\rho_l : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \mathrm{End}_{\mathbb{Q}_l}(H^1_{\acute{e}t}(E\times_F F^{\mathrm{sep}},\mathbb{Q}_l)).$$

For all places v of F, we put (see examples 5.3.18(1))

$$a_v = \mathrm{Tr}(\rho(\mathrm{Frob}_v)|H^1_{\acute{e}t}(E\times_F F^{\mathrm{sep}},\mathbb{Q}_l)^{I_v})$$

where I_v is an inertia subgroup of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ at v. Let E_v denote the reduction at v of the Néron model of E/F. Then we have

$$a_v = |E_v(\kappa(v))| - 1 - |\kappa(v)|.$$

(B.11.11) The local L-function at v of the elliptic curve E is then defined to be, where q_v is the order of the residue field $\kappa(v)$,

$$L_v(s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1} \text{ if } E \text{ has good reduction at } v$$

$$L_v(s) = (1 - a_v q_v^{-s})^{-1} \text{ if } E \text{ has bad reduction at } v.$$

The global L-function of E/F is then defined to be

$$L(E,s) = \prod_v L_v(s)$$

where the product runs over all places v of F.

(B.11.12) Suppose that the elliptic curve E/F is not isotrivial.

For each place v of F (see [D2, §3]), the representation of $\mathrm{Gal}(F_v^{\mathrm{sep}}/F_v)$ on $H^1_{\acute{e}t}(E\times_F F^{\mathrm{sep}},\mathbb{Q}_l)$ defines an irreducible admissible representation $\pi_v(E)$ of $\mathrm{GL}_2(F_v)$. As the representations $H^1_{\acute{e}t}(E\times_F F^{\mathrm{sep}},\mathbb{Q}_l)$ are compatible for all l

distinct from p, the representation $\pi_v(E)$ is defined over $\mathbb{Q}$ and is independent of l. Let $\pi_v(E)$ also denote the corresponding representation over $\overline{\mathbb{Q}}_l$. The centre F_v^* of $\mathrm{GL}_2(F_v)$ acts as the quasi-character $\omega_2 : a \mapsto |a|_v^2$ on $\pi_v(E)$ where $|.|_v$ is the normalised absolute value of F_v. For all but finitely many places v, the representation $\pi_v(E)$ has a $\mathrm{GL}_2(O_v)$-invariant vector, where O_v is the valuation ring of the local field F_v.

By [D1, Exemple 9.6] and [JL, theorem 11.3, 11.5] the tensor product $\pi(E) = \bigotimes_v \pi_v(E)$ is then a direct factor of the representation

$$L_0(\omega_2, \mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}), \overline{\mathbb{Q}}_l)$$

in the space of cuspidal locally constant $\overline{\mathbb{Q}}_l$-valued functions with compact support on $\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})$ transforming the centre via the quasi-character ω_2. The representation $\pi(E)$ has by construction the same local L-factors as $\{\rho_l\}_l$. That is to say, $\pi(E)$ is compatible with $\{\rho_l\}_l$. Furthermore the conductor of $\pi(E)$ is equal to the conductor of the representation ρ_l provided by the curve E/F (see [D2, §3.2(C)]).

(B.11.13) Suppose now that E/F has split mutliplicative reduction at ∞; in particular, E/F is not isotrivial. The conductor of E is then equal to $\mathrm{div}(I)+\infty$, where I is an ideal of A and $\mathrm{div}(I)$ is the divisor on C/k associated to I.

The component $\pi_\infty(E)$ at ∞ of the automorphic representation $\pi(E)$ attached to E/F is then isomorphic to the special representation $V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)$.

(B.11.14) Let $\Gamma_0(I)$ be the Hecke subgroup of $\mathrm{GL}_2(\widehat{A})$, where $\widehat{A}$ is the profinite completion of A; that is to say, the subgroup given by

$$\Gamma_0(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{A}) \mid \ c \equiv 0 \ (\mathrm{mod}\ I\widehat{A}) \right\}.$$

Then $\Gamma_0(I)$ is an arithmetic subgroup of $\mathrm{GL}_2(\widehat{A})$; in particular, it contains the principal congruence subgroup $\tilde{U}_I$. We write $\mathrm{sp}_{\mathrm{Gal}}(\overline{\mathbb{Q}}_l)$ for the special representation over $\overline{\mathbb{Q}}_l$, that is to say,

$$\mathrm{sp}_{\mathrm{Gal}}(\overline{\mathbb{Q}}_l) = \mathrm{sp}_{\mathrm{Gal}} \otimes_{\mathbb{Q}_l} \overline{\mathbb{Q}}_l.$$

Write Γ in place of $\Gamma_0(I)$. The group Γ satisfies the hypothesis of proposition B.9.3 that the stabiliser in Γ_x of any vertex or edge of T is a p-group. By proposition B.9.3 we have for the arithmetic subgroup Γ an isomorphism of (centralizer(Γ) in $\mathrm{GL}_2(\mathbb{A}_f)) \times \mathrm{Gal}(F_\infty^{\mathrm{sep}}/F_\infty)$-representations

$$\theta_\Gamma : H_!^1(M_\Gamma^2 \otimes F_\infty^{\mathrm{sep}}, \overline{\mathbb{Q}}_l) \cong$$

$$\mathrm{Hom}_{\mathrm{GL}_2(F_\infty)}(V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l), L_0(\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\Gamma, \overline{\mathbb{Q}}_l)) \otimes_{\overline{\mathbb{Q}}_l} \mathrm{sp}_{\mathrm{Gal}}(\overline{\mathbb{Q}}_l).$$

The representation $L_0(\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\Gamma, \overline{\mathbb{Q}}_l)$ decomposes as a direct sum of irreducible representations of multiplicity 1 [JL, proposition 11.1.1]

$$L_0(\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\Gamma, \overline{\mathbb{Q}}_l) \cong \bigoplus_{\pi\in\Pi_\Gamma} \pi$$

where Π_Γ is a set of irreducible admissible representations of $\mathrm{GL}_2(\mathbb{A})$. As $\pi(E)$ is a direct factor of $L_0(\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\Gamma, \overline{\mathbb{Q}}_l)$ and as $\pi_\infty(E)$ is isomorphic to $V_{\mathrm{sp}}(\overline{\mathbb{Q}}_l)$ it follows that there is an isomorphism of (centralizer(Γ) in $\mathrm{GL}_2(\mathbb{A}_f)) \times \mathrm{Gal}(F^{\mathrm{sep}}/F)$-representations

$$\theta_\Gamma^* : H^1_!(M^2_\Gamma \otimes_F F^{\mathrm{sep}}, \overline{\mathbb{Q}}_l) \cong \left\{ (\bigotimes_{v\neq\infty} \pi_v(E)) \otimes \sigma(\pi(E)) \right\} \oplus \bigoplus_{\pi\in\Pi'_\Gamma} (\bigotimes_{v\neq\infty} \pi_v) \otimes \sigma(\pi)$$

where Π'_Γ is a subset of Π_Γ. Here $\sigma(\pi(E))$ is a 2-dimensional representation over $\overline{\mathbb{Q}}_l$ of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ compatible with $\pi(E)$. Hence $\sigma(\pi(E))$ is isomorphic over $\overline{\mathbb{Q}}_l$ to the l-adic representation ρ_l given by E (see (B.11.10)).

Let $X_0^{\mathrm{Drin}}(I)/F$ be the smooth projective curve obtained from M^2_Γ by adjoining the cusps. Let $T_l(X_0^{\mathrm{Drin}}(I)/F)$ be the l-adic Tate module of the jacobian of $X_0^{\mathrm{Drin}}(I)/F$. As $H^1_!(M^2_\Gamma \otimes F^{\mathrm{sep}}, \overline{\mathbb{Q}}_l(1))$ is isomorphic to $T_l(X_0^{\mathrm{Drin}}(I)) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l$, we obtain a surjective homomorphism of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-modules

$$T_l(X_0^{\mathrm{Drin}}(I)) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l \to T_l(E) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l.$$

B.11.15. Theorem. (Zarhin, [Z1], [Z2], S. Mori) *Let A, B be abelian varieties over F and let l be a prime number distinct from the characteristic of F. Let $T_l(A), T_l(B)$ be the Tate modules of A, B, respectively. Then there is an isomorphism*

$$\mathrm{Hom}_F(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong \mathrm{Hom}_{\mathrm{Gal}(F^{\mathrm{sep}}/F)}(T_l(A), T_l(B)). \quad \square$$

(B.11.16) By this theorem of Zarhin, completed for the case of characteristic 2 by S. Mori, we obtain the next theorem, which is a restatement of theorem 4.7.1 of the main text.

B.11.17. Theorem. *Suppose that E/F has split mutliplicative reduction at ∞. Let I, which is an ideal of A, be the conductor of E/F without the component at ∞. Then there is a finite surjective morphism of F-schemes*

$$X_0^{\mathrm{Drin}}(I) \to E. \quad \square$$

B.11.18. Remarks. (1) Let A, B be abelian varieties over a field K which is finitely generated over its prime subfield. Let l be a prime number distinct

from the characteristic of K. Let $T_l(A), T_l(B)$ be the Tate modules of A, B, respectively. Then "the isogeny conjecture" is that there is an isomorphism (see [T1, p.98])

$$\mathrm{Hom}_K(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong \mathrm{Hom}_{\mathrm{Gal}(K^{\mathrm{sep}}/K)}(T_l(A), T_l(B)).$$

The conjecture states that if a group homomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules $f : A[l^\infty] \to B[l^\infty]$, is given, where $A[l^\infty]$ and $B[l^\infty]$ denote the l-power torsion subgroups of A, B, respectvely, then for all integers n there is a homomorphism of abelian varieties $f_n : A \to B$ over K where f_n coincides with f on points of order l^n.

(2) The result stated in the theorem B.11.15 is the "isogeny conjecture" for global fields of positive characteristic. Zarhin proved the isogeny conjecture for abelian varieties over function fields of characteristic $p \neq 2$ (see [Z1], [Z2]); the proof for $p = 2$ was completed by S. Mori (see [Mo] Chapitre XII, Corollaire 2.4, Théorème 2.5). Faltings [F] proved the "isogeny conjecture" for abelian varieties over number fields.

(3) In [GR], the theorem 4.7.1 is also proved for elliptic curves over global fields of positive characteristic. The method of [GR] is different from that explained above (see remark 4.7.2).

B.11.19. Examples. The following examples are taken from [GR]. Suppose that $q = 2$ and F is the rational field $\mathbb{F}_2(T)$. Let ∞ be the point at infinity of F with residue field $\mathbb{F}_2$.

(1) Let $I = T^2(T-1)\mathbb{F}_2[T]$. Then $X_0^{\mathrm{Drin}}(I)$ has genus 1. Let E/F be the elliptic curve with Weierstrass equation

$$Y^2 + TXY = X^3 + TX.$$

This has j-invariant $T^8/(T-1)^2$ and conductor $I.\infty$. It has split multiplicative reduction at ∞. It follows from theorem 4.7.1 that there is an isogeny of elliptic curves (in fact there is an isomorphism)

$$X_0^{\mathrm{Drin}}(I) \to E.$$

(2) Let $I = T^3\mathbb{F}_2[T]$. Then $X_0^{\mathrm{Drin}}(I)$ also has genus 1. Let E/F be the elliptic curve with Weierstrass equation

$$Y^2 + TXY = X^3 + T^2.$$

This has j-invariant T^4 and conductor $I.\infty$. It has split multiplicative reduction at ∞. It follows from theorem 4.7.1 that there is an isogeny of elliptic curves

$$X_0^{\mathrm{Drin}}(I) \to E.$$

In fact $X_0^{\mathrm{Drin}}(I)$ is isomorphic to E.

(3) Let $I = T(T^2+T+1)\mathbb{F}_2[T]$. Then $X_0^{\mathrm{Drin}}(I)$ has genus 2. Let E_1/F be the elliptic curve with Weierstrass equation

$$Y^2 + (T+1)XY + Y = X^3 + T(T^2+T+1).$$

Let E_2/F be the elliptic curve with Weierstrass equation

$$Y^2 + (T+1)XY + Y = X^3 + X^2 + T + 1.$$

Then E_1 has j-invariant $(T+1)^{12}/[T(T^2+T+1)]^3$ and E_2 has j-invariant $(T+1)^{12}/T^5(T^2+T+1)$. The curves E_1, E_2 have split multiplicative reduction at ∞. The jacobian of the curve $X_0^{\mathrm{Drin}}(I)$ is isogenous to $E_1 \times E_2$.

B.12 The Langlands conjecture for GL_n over function fields (according to Lafforgue)

Lafforgue [La] has extended the method of Drinfeld for proving the Langlands conjecture for GL_2 to GL_n for all integers $n \geq 1$. Lafforgue considers instead of moduli schemes of Drinfeld modules, the cohomology of moduli schemes of Drinfeld's stukas.

(B.12.1) To state the main result of Lafforgue, with the notation of (B.2.1), fix a prime number l different from the characteristic of F. For every integer $r \geq 1$, let $\mathcal{A}^r(F)$ denote the set of automorphic irreducible cuspidal representations π of $\mathrm{GL}_r(\mathbb{A})$ of which the central character χ_π is of finite order. Let $\mathcal{G}_l^r(F)$ denote the set of l-adic representations of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ which are unramified everywhere except for finitely many places and are irreducible of dimension r and such that the determinant representation is of finite order. The Langlands correspondence for the function field F can then be stated as follows.

B.12.2. Theorem. (Lafforgue) *For every integer $r \geq 1$ we have:*

(i) *To every automorphic cuspidal representation $\pi \in \mathcal{A}^r(F)$ there is associated a unique Galois representation $\sigma_\pi \in \mathcal{G}_l^r(F)$ which is unramified at every place x of C where π is unramified and has eigenvalues for the Frobenius equal to the eigenvalues of Hecke $z_1(\pi), \ldots, z_r(\pi)$ of π.*

(ii) *Conversely, to every Galois representation $\sigma \in \mathcal{G}_l^r(F)$ there is associated a unique automorphic cuspidal representation $\pi_\sigma \in \mathcal{A}^r(F)$ where the Hecke eigenvalues $z_1(\pi), \ldots, z_r(\pi)$ of π_σ are equal to the eigenvalues for the Frobenius of σ.* □

(B.12.3) Lafforgue also proves the Ramanujan-Petersson conjecture for the automorphic cuspidal representations of $\mathcal{A}^r(F)$ as well as the Generalised

Riemann Hypothesis for the corresponding L-functions of these automorphic representations for function fields. The precise statement is as follows.

B.12.4. Theorem. (Lafforgue)

(i) *(Ramanujan-Petersson conjecture) For every integer $r \geq 1$ and every automorphic cuspidal representation $\pi \in \mathcal{A}^r(F)$ the local factors π_x of π are tempered at all places x of C. In particular, at every place $x \in C$ where π_x is unramified, its Hecke eigenvalues satisfy*

$$|z_i(\pi_x)| = 1 \quad \textit{for all} \quad 1 \leq i \leq r.$$

(ii) *(Generalised Riemann Hypothesis) For every pair of cuspidal automorphic representations $\pi \in \mathcal{A}^r(F)$ and $\pi' \in \mathcal{A}^{r'}(F)$ of ranks $r, r' \geq 1$, all zeros of the global L-function $L(\pi \times \pi', Z)$ are on the circle*

$$|Z| = |k|^{-1/2}. \quad \square$$

References

[Be] Berkovich, V: Etale cohomology for non-archimedean analytic spaces. Publ. Math. IHES 78 (1993), 5-161

[BD] Bucur, I., Deleanu, A.: Introduction to the Theory of Categories and Functors. Wiley, London 1968.

[BDa] Bertolini, M., Darmon, H.: Kolyvagin's descent and Mordell-Weil groups over ring class fields. Journal für die reine und angewandte Mathematik 412 (1990), 63-74

[BGR] Bosch S, Güntzer U., Remmert R.: Non-Archimedean Analysis, Springer Verlag. New York-Heidelberg-Berlin 1984

[Br1] Brown M.L.: Singular moduli and supersingular moduli of Drinfeld modules. Invent. Math. 110 (1992), 419-439

[Br2] Brown, M.L.: On a conjecture of Tate for elliptic surfaces over finite fields. Proc. London Math. Soc. 69 (1994), 489-514

[Br3] Brown, M.L.: Automorphic forms and Drinfeld-Heegner points. In preparation

[Bro1] Brown K.S.: Cohomology of Groups. Springer Verlag. New York-Heidelberg-Berlin 1982

[Bro2] Brown K.S.: Buildings. Springer Verlag. New York 1989

[CF] Cassels, J.W.S., Frohlich, A. Editors, Algebraic Number Theory. Academic Press, London-New York 1967

[C] Cohn, P.M.: Universal Algebra. Harper and Row, New York 1965

[CR] Curtis, C.W., Reiner, I.: Methods of Representation Theory. Vol. 1. J. Wiley. New York-Chichester-Brisbane-Toronto 1981

[CW] Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), 223-251

[Dr1] Drinfeld, V.G.: Elliptic modules. Math. USSR-Sb. 23 (1974), 561-592

[Dr2] Drinfeld, V.G.: Elliptic modules II. Math. USSR-Sb. 31 (1977), 159-170

[Dr3] Drinfeld, V.G.: Langland's conjecture for GL(2) over functional fields. Proceedings of the International Congress of Mathematicians, Helsinki, 1978

[D1] Deligne, P.: Les constantes des équations fonctionnelles des fonctions L. In: Lecture Notes in Math. No. 349, Springer Verlag, Berlin 1973, pp. 501-597

[D2] Deligne, P.: Formes modulaires et représentations de GL(2). In: Modular Functions of One Variable II. Lecture Notes in Math. No. 349, Springer Verlag, Berlin 1973, pp.55-105

[DH] Deligne, P., Husemoller, D.: Survey of Drinfel'd modules. In: Current Trends in Arithmetical Algebraic Geometry (ed. K.A. Ribet), Contemporary Mathematics 67 (American Mathematical Society, Providence R.I., 1987), pp.25-91

[DM] Deligne, P., Mumford, D.; The irreducibility of the space of curves of given genus. Publ. Math. I.H.E.S. 36 (1969), 75-109

[DR] Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. In: Modular Functions of One Variable II. Lecture Notes in Mathematics No. 349, pp. 143-316. Springer Verlag Berlin-Heidelberg-New York 1973

[F] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. 73 (1983), 349-366

[FP] Fresnel, J., van der Put, M.: Géométrie Analytique Rigide et Applications. (Progress in Mathematics. Vol 18). Birkhäuser. Boston-Basel-Stuttgart 1981.

[G] Gekeler, E-U.: Drinfeld Modular Curves. Lecture Notes in Mathematics 1231. Springer Verlag. Berlin-Heidelberg-New York-Tokyo 1986

[GB1] Gross, B.H.: Heegner points on $X_0(N)$. In: Modular Forms (ed. R.A. Rankin), Ellis Horwood, Chichester, 1989, pp.87-105

[GB2] Gross, B.H.: Kolyvagin's work on modular elliptic curves. In: L-functions and Arithmetic (eds. J.H. Coates and M.J. Taylor) Cambridge University Press, 1990, pp.235-256

[GR] Gekeler, E.-U., Reversat, M.: Jacobians of Drinfeld modular curves. J. reine angew. Math. 476 (1996), 27-93

[Go1] Goss, D.: The algebraist's upper half plane. Bulletin Amer. Math. Soc. 2 (1980), 391-415

[Go2] Goss, D.: π-adic Eisenstein series for function fields. Compositio Math. 41 (1980), 3-38

[Go3] Goss, D.: Basic Structures of Function Field Arithmetic. Modern Surveys in Mathematics Vol. 35. Springer Verlag. Berlin-Heidelberg-New York 1996

[Go4] Goss, D.: Can a Drinfeld module be modular?. Journal of the Ramanujan Mathematical Society 17 (2002), 221-260

[Gro] Grothendieck, A.: Le groupe de Brauer III. In: Dix Exposés sur la Cohomologie des Schémas. North Holland, Amsterdam, 1968, 88-188

[Ha] Harder, G.: Chevalley groups over function fields and automorphic forms. Ann. of Math. 100 (1974), 249-306

[H] Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematices no. 52. Springer Verlag. Berlin-Heidelberg-New York 1977

[Hu] Huber, R.: Etale Cohomology of Rigid Analytic Varieties and Adic Spaces. Vieweg. Brauchschweig/Wiesbaden 1996

[HS] Hochschild, G.P., Serre, J-P.: Cohomology of group extensions. Trans. Amer. Math. Soc. 74 (1953), 110-134

[I] Igusa, J.I.: Fibre systems of jacobian varieties III. (Fibre sytems of elliptic curves). Amer. J. Math. 81 (1959), 453-476

[JL] Jacquet, H., Langlands, R.P.: Automorphic Forms on GL(2). Lecture Notes in Math. 114. Springer Verlag, Berlin-Heidelberg-New York 1970

[Ka] Kato, K.: To appear

[KT] Kato, K., Trihan, F.: On the conjecture of Birch and Swinnerton-Dyer in characteristic $p > 0$. Invent. Math. 153 (2003), 537-592

[K1] Kolyvagin, V.A.: Finiteness of $E(\mathbb{Q})$ and $\text{Ш}(E, \mathbb{Q})$ for a subclass of Weil curves. Math. USSR Izvestiya Vol. 32 (1989), No. 3.

[K2] Kolyvagin, V.A.: Euler systems. In: The Grothendieck Festschrift (Vol. II), P. Cartier et al., eds., 435-483. Progress in Math. 87. Birkhäuser, Boston 1990

[K3] Kolyvagin, V.A.: On the structure of Selmer groups. Math. Annalen 291 (1991), 253-259

[K4] Kolyvagin, V.A.: On the structure of Shafarevich-Tate groups. Proceedings of the USA-USSR Symposium on Algebraic Geometry, Chicago 1989. Lecture Notes in Math. No. 1479 Springer Verlag, Berlin-Heidelberg-New York 1991

[KM] Katz, N.M., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Princeton University Press, Princeton, New Jersey 1985

[La] Lafforgue, L: Chtoucas de Drinfeld et corréspondance de Langlands. Invent. Math. 147 (2002), 1-241

[L] Lang, S.: Elliptic Curves. Diophantine Analysis. Springer Verlag, Berlin-Heidelberg-New York 1978

[M1] Milne, J.S.: On a conjecture of Artin-Tate. Ann. of Math. 102 (1975), 517-533

[M2] Milne, J.S.: Etale Cohomology. Princeton University Press, Princeton, New Jersey 1980

[M3] Milne, J.S.: Values of zeta functions of varieties over finite fields. Amer. J. Math. 108 (1986), 297-360

[M4] Milne, J.S.: Arithmetic Duality Theorems. Academic Press Inc., Boston 1986

[Mi] Milnor, J.: Introduction to Algebraic K-theory. Annals of Mathematics Studies No. 72, Princeton University Press, Princeton New Jersey, 1971

[Mo] Moret-Bailly, L.: Pinceaux de Variétés Abéliennes. Astérisque 129 (1985) Société Mathématique de France

[Mu] Murre, J.: Lectures on an Introduction to Grothendieck's Theory of the Fundamental Group. Lecture Notes. Tata Institute of Fundamental Research, Bombay 1967

[MW] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$. Invent. Math. 76 (1984), 179-330

[N] Neukirch, J.: Class Field Theory. Springer Verlag. Berlin-Heidelberg-New York-Tokyo 1986

[P] Ponrtjagin L.S.: Topological Groups. Second Edition. Gordon and Breach Inc., New York-London-Paris 1966

[PR] Perrin-Riou, B.: Travaux de Kolyvagin et Rubin. Séminaire Bourbaki 1989/90 No. 717. Astérisque 189-190 (1990), 69-106

[PT] ven der Put, M., Top J.: Analytic compactification and modular forms. pp.113-140. In: Drinfeld Modules, Modular Schemes and Applications. World Scientific, Singapore-New Jersey-London-Hong Kong 1997

[Ra] Raynaud, M.: Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes. In: Dix Exposés sur la Cohomologie des Schémas. Ed. A. Grothendieck, pp. 12-30, North-Holland Pub. Comp. Amsterdam, 1967

[R1] Rubin, K.: Euler Systems. Annals of Math. Studies No. 147. Princeton 2000

[R2] Rubin, K.: Elliptic curves with complex muliplication and the conjecture of Birch and Swinnerton-Dyer. In: Arithmetic Theory of Elliptic Curves, Cetraro 1997. Ed: C. Viola. Lecture Notes in Math. No. 1716. Springer Verlag, New York-Heidelberg-Berlin 1999 pp. 167-234

[R3] Rubin, K.: The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent. Math. 103 (1991), 25-68

[R4] Rubin, K.: The main conjecture. Appendix to: Cyclotomic Fields I and II, S. Lang. Graduate Texts in Mathematics 121. Springer Verlag, New York-Heidelberg-Berlin 1990 pp. 397-419

[S1] Serre, J-P.: Cohomologie Galoisienne. Lectures Notes in Math. No. 5. 4th Edition. Springer Verlag, Berlin-Heidelberg-New York-Tokyo 1986

[S2] Serre, J-P.: Linear Representations of Finite Groups. Graduate Texts in Mathematics No. 42. (3rd printing). Springer Verlag, New York-Heidelberg-Berlin 1986

[S3] Serre, J-P.: Lectures on the Mordell-Weil Theorem. Translated and edited by M. Brown from notes by M. Waldschmidt. Vieweg, Braunschweig-Wiesbaden 1989

[S4] Serre, J-P.: Arbres, Amalgames, SL_2. Astérisque 46. Société Mathématique de France. 3ème édition 1983

[S5] Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331

[SK] Shioda, T. Katsura, T.: On Fermat varieties. Tohoku Mathematics Journal, 31 (1979), 97-115

[Si1] Silverman, J.: The Arithmetic of Elliptic Curves. Springer Verlag, New York-Berlin-Heidelberg-Tokyo 1986

[Si2] Silverman, J.: Advanced Topics in the Arithmetic of Elliptic Curves. Springer Verlag, New York-Berlin-Heidelberg 1994

[SS] Schneider, P., Stuhler, U.: The cohomology of p-adic symmetric spaces. Invent. Math. 105 (1991), 47-122

[T1] Tate, J.: Algebraic cycles and poles of zeta functions. In: Arithmetical Algebraic Geometry. Ed. by O.F.G. Schilling. pp. 93-110. Harper and Row, New York 1965

[T2] Tate, J.: p-divisible groups. In: Proceedings of a Conference on Local Fields. Driebergen. pp. 158-183. Springer Verlag, Berlin-Heidelberg-New York 1967

[T3] Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In: Dix Exposés sur la Cohomologie des Schémas. pp. 189-214. North Holland, Amsterdam 1968

[T4] Tate, J.: Rigid analytic spaces. Invent. Math. 12 (1971), 257-289

[V] Vignéras, M.F.: Arithmétique des Algèbres de Quaternions. Lecture Notes in Math. No. 800. Springer Verlag, New York-Berlin-Heidelberg 1980

[W] Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. Math. 141 (1995), 443-551

[Z1] Zarhin, Y.: Endomorphisms of abelian varieties over fields of finite characteristic. Math. USSR Izv. 9 (1975), 255-260

[Z2] Zarhin, Y.: Abelian varieties in characteristic p. Mat. Zametki 19 (1976), 393-400 (English Translation: Mathematical Notes 19 (1976), 240-244)

[ZS] Zariski, O., Samuel, P.: Commutative Algebra. Van Nostrand Co., Princeton-London-New York-Toronto 1958

Index

Admissible family of subgroups
- definition . . . 144, 155
- of Picard groups . . . 199
- vanishing of cohomology . . . 155
Algebraic stacks . . . 81-85
Arithmetic subgroup of $\mathrm{GL}_d(\widehat{A})$ . . . 457, 469, 493, 494
Artin reciprocity map . . . 18
Artin-Tate conjecture . . . 10, 11, 359, 360, 363, 365
Atkin-Lehner operator . . . 81
Atoms and molecules . . . 150
Augmentation ideal . . . 167
Automorphic form . . . 492-495, 501-502
- cuspidal . . . 492
Automorphic representation . . . 504
- cuspidal . . . 504
- Langlands correspondence . . . 495-497
- multiplicity 1 decomposition . . . 494
- tensor product decomposition . . . 494

Birch and Swinnerton-Dyer conjecture . . . 1, 10, 11, 359, 360, 365
- for elliptic curves with complex multiplication (Rubin) . . . 363
- for Weil elliptic curves (Kolyvagin) . . . 360-362
Building map on Ω^d . . . 464-465, 466-468
- *See* Bruhat-Tits building
Bruhat-Tits building . . . 32-33
- with complex multiplication . . . 5-6, 45-56
  - classification . . . 57-62
  - complex multiplication and the standard metric . . . 33-46
  - explicit formulae for the exponent . . . 41-45
- ends of a Bruhat-Tits tree . . . 489, 453
- exponent function . . . 37, 41-45, 46-62, 64

- geometric realisation 462
- for PGL over a local field 461-464
- for SL_2 . . . . . 32-33, 45-46, 57-62, 461-464
  - apartments 33
  - building map 464-465, 466-468
- norms on a vector space over a local field 461-464
  - dialation classes of norms 462
  - imaginary norm 466
  - integral norm, rational norm 461
- standard metric 33, 46-56, 70, 465
- plane incidence geometry 33
- quotient of a Bruhat-Tits tree by an arithmetic group 471-479
- star of a vertex 49
- star map 50
- global Bruhat-Tits net with complex multiplication 65-74

Bruhat-Tits global net 65-69
- with complex multiplication 69-74
- pseudo-metric 70

Čech cohomology on an affinoid space 439
Čech galois cohomology 121-169
- admissible family of subgroups 155
- čech complex 129-130
  - cohomology of a presheaf 130-131
- comparison with derived functors 133-136
- filter 137-140, 145
- cohomology with respect to a filter 140-146
  - alternating cochains 141-144
- explicit form 144-150
- flabby sheaves 136-137
- galois covering 121

Characters of finite groups 246-250
- χ-isotypical component 250

Cohomology
- Čech galois cohomology. *See* Čech galois cohomology
- cuspidal cohomology 484
- étale cohomology of rigid spaces 440-444
- Tate cohomology groups 341
- of finite groups, definitions 174-175
  - coboundaries 174
  - coboundary formula 174
  - cochains 174
  - cocycles 174
  - cohomologically triviality 174
- harmonic cochains 481
- of the Heegner module 223-327
  - Kolyvagin elements 175-178
  - molecules and atoms 150
- cohomology of Ω^2 479-482

- of M_H^2 483-488
Compatibility of galois representations and automorphic representations 496, 500
Compatible system of λ-adic galois representations 496
Complex multiplication of Drinfeld modules 26-27
- main theorem 27
Conductor of an elliptic curve 497-499
Cuspidal automorphic form. *See* Automorphic form

Dihedral group, generalised 27-30
Drinfeld-Heegner point 75-80
- notation, conductor and class 78-79, 97
- galois action 79-80
- specialisation and generisation 77-78
Drinfeld module, definition of, ... 23, 445-446
- with complex multiplication 26-27
- singular 76
- supersingular 78, 83
- with cyclic I-structure 23-24
- with full level I-structure 24, 446
- with structure of level H 470
Drinfeld modular curve . . 23-26, 76-79, 80-103, 118, 358, 445-449, 452, 458-459
- $X_0^{\mathrm{Drin}}(I)$, $\mathbf{X}_0^{\mathrm{Drin}}(I)$, definition 23
- $Y_0^{\mathrm{Drin}}(I)$, $\mathbf{Y}_0^{\mathrm{Drin}}(I)$, definition 23-26
- M_I^d, M_I^2, M^d, definition 445-448
-action of $\mathrm{GL}(d, \mathbb{A}_f)/F^*$ on M^d 26, 447-448
-analytic description of M_I^d 25, 448-449
- compactification of M_I^2 447
- M_H^d 470
- cohomology of M_H^d 483-488, 492
- cusps 25, 453
- Drinfeld-Heegner point 75-80
- Eichler-Shimura congruence 81-85
- Hecke operators 1, 4, 6, 7, 80, 81, 86-96
- with I-cyclic structure 23-24
- with full level I-structure 24, 446

Eichler-Shimura congruence 81-85
Eisenstein series 454-456
- *See also* Rigid analytic modular forms
Elementary matrices 352
Elliptic curve 458-459
- conductor 497-499
- Eichler-Shimura congruence 81-85
- L-function 500
- sign in the functional equation 358, 388
- Igusa's theorem on galois action 339-341
- isotrivial elliptic curve 340
- Shimura-Taniyama-Weil conjecture
- analogue for $X_0^{\mathrm{Drin}}(I)$ 96-97, 458-459, 500-504

- for elliptic curves over $\mathbb{Q}$ (theorem of Wiles) 119
- associated rigid analytic modular form 458-459
- with split multiplicative reduction 499-500
Ends of a Bruhat-Tits tree 453, 489
Etale cohomology of rigid analytic spaces 440-444
Euler system 360, 361

Finite simple group $\mathrm{PSL}_2(\mathbb{Z}/l\mathbb{Z})$, $l \geq 5$, ... 346
Fricke operator 81, 93
- Hecke operators 1, 4, 6, 7, 80, 81, 86-96

Generalised Riemann hypothesis for function fields (Lafforgue) 505
Graph 475, 487
- of $\mathrm{GL}_2(A)\backslash T$ 475-479
Grothendieck fundamental group 121, 145
Group rings 144-195
- augmentation ideal 167
- Kolyvagin elements 175-178
- of Picard groups 109-110

Harmonic cochains 481
- cuspidal cohomology 484
- measures on $\mathbb{P}_1(F_\infty)$ 489
Hecke operator 1, 4, 6, 7, 80, 81, 86-96, 456-458
- Atkin-Lehner operator 81
- Fricke operator 81, 93
- Eichler-Shimura congruence 81-85
- Hecke algebra 81
Heegner module
- basic properties 195-207
- cohomology of the Heegner module 223-327
- definition 114-115
- exceptional set of prime divisors 115, 358
- explicit form 116
- faithful flatness 207-220
- galois action 115
- universal 118
- of a galois representation 117
- as a sheaf 221
Heegner sheaf 99-103, 221-222

I-cyclic structure 23-26
Igusa's theorem 339-341
Imaginary quadratic extension 14
Infinitesimal trait 246
- local parameter, valuation 246
Isogeny conjecture for abelian varieties 502
Isotypical component 250

Jacquet-Langlands L-function 496

Kolyvagin elements 175-178

Langlands correspondence, Langlands conjecture 495-497, 504-505
- Generalised Riemann hypothesis for function fields 505
- Ramanujan-Petersson conjecture 505
Lattice (*See also* Bruhat-Tits building)
- definition 32, 62, 76, 448
- associated exponential function 448
- conductor 37, 41, 63
  - local exponent of conductor 63, 41
  - local exponent and the standard metric 46-56
- equivalence 32, 66
- flag 33
  - flag complex 33, 86
- incidence 32
- index 34, 62
  - local index 62
- invariants 34
- type of lattice class 33
  - plane incidence geometry 33
  - Euclidean building (*see also* Bruhat-Tits building) 33
- $\mathfrak{p}$-incident 66
  - locally $\mathfrak{p}$-incident 67
- $\mathfrak{p}$-flag 67, 86
- $\mathfrak{p}$-lower/upper modification 65
Lattice ideal 46
Locally free sheaves 471-479
- adelic description 64, 468-470
- decomposbale 474-475
- sub-bundles 472-475
- trivialised over an open subscheme 468

Mennicke symbol on $\mathrm{SK}_1(\Lambda)$ 353
Modification, upper and lower 65
Molecules and atoms 150, 199

Norms on a vector space over a local field 461-464
- dialation classes of norms 462
- imaginary norm 466
- integral norm, rational norm 461

Orders in quadratic extensions 14-17, 63
- conductor 14

Parabolic subgroup 491
Poitou-Tate local duality 402-405
Pontrjagin duality, equivariant form 406-412
- P-character group 407

Quasi-modules, quasi-groups 330-339
- finite quasi-group 334

- quasi-constant map 334
- quasi-isomorphism 335
- trivial quasi-group 334

Ramanujan-Petersson conjecture for function fields (Lafforgue) 505
Rigid analytic modular forms 450-459
- algebraic modular forms 450
- analytic modular forms 451-452
- Eisenstein series 454-456
- Hecke operators (*see also* Hecke operators) 456-458
- with level structure 450
- q-expansions 452-454
- relation with elliptic curves 458-459
Rigid analytic spaces 440
- admissible open subset 438
- admissible covering 438
- affinoid space, affinoid algebra 437, 439
- connected 440
- étale cohomology of rigid spaces 440-444
- Grothendieck topology on a rigid space 438-440
- open affinoid subset 437
- rational subset 438
- rigid analytic morphisms 440
- rigid analytic torus 499
- Tate algebra 436-437
  - maximal spectrum 437
- the space Ω^d 25, 444-445
  - Ω^2 and tubular neighbourhoods of trees 468
  - cohomology of Ω^2 479-482
Ring class field extension 18-23
- conductor 18
- order of ring class field extension 19-22
- ramification 22

Saturated set of divisors 198
- z-maximal divisor 233
- z-saturated set of divisors 234
- z-saturation 234
Selmer group 366-367
Semi-convergent spectral sequence 339
Shimura-Taniyama-Weil conjecture
- analogue for $X_0^{\mathrm{Drin}}(I)$ 96-97, 458-459, 500-504
- for elliptic curves over $\mathbb{Q}$ (theorem of Wiles) 119
Sieves 169
Special galois representation $\mathrm{sp}_{\mathrm{Gal}}$ 486-487, 500
- elliptic curves with split multiplicative reduction 458-459, 499-500
Special representation of $\mathrm{GL}_2(F_\infty)$ 490
Split multiplicative reduction of elliptic curves 499-500, 501
- special galois representation 500

Stukas of Drinfeld 497, 504
Sufficiently large multiplicative set 406

Tate conjecture 2-3, 8-10, 329, 359, 363, 365
Tate-Shafarevich group 8, 361-366

Universal
- universal exact sequences 161
- universal submodule 160
- universal Heegner module 118
- universally cohomologically trivial module 174

Weil group 495
Weil pairing 402
Weil parametrisation 96

Zeta function 2