University of Utah

Algebraic Number Theory

Dick Gross

Notes by Sean Sather-Wagstaff

Introduction

These notes are based on a semester-long course in algebraic number theory given at the University of Utah during the Spring of 1999. The author learned the subject from John Tate and has used many of Tate's unpublished ideas here.

Throughout these notes, we shall employ the following notations. For a ring A, we let $A^\times$ denote the multiplicative group of units in A. If A is a subgroup (resp. subfield) of B, we let $(B : A)$ denote the index (resp. degree) of A in B. For a finite extension of fields $k \subseteq K$, we let Tr and $\mathbb{N}$ denote the trace and norm maps, respectively.

Lecture 1

One of our first goals is to discuss the properties of the ring of integers in a number field. To accomplish this, we shall first consider general lattices in a rational vector space.

Definition. Let V be a finite dimensional vector space of dimension n over the rational numbers $\mathbb{Q}$. A *lattice* in V is a free abelian subgroup $L \subset V$ of rank n.

Assume that L is a lattice in V with $v_1, \dots, v_n \in V$ such that $L = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_n$. Then the set $\{v_1, \dots, v_n\}$ forms a basis for V. It suffices to show that the v_i are linearly independent over $\mathbb{Q}$. Suppose that $\sum_i a_i v_i = 0$ for some $a_1, \dots, a_n \in \mathbb{Q}$. Choose a nonzero integer N so that Na_i is an integer for each i. Then $0 = N\sum_i a_i v_i = \sum_i Na_i v_i$ which is a sum of elements in L. Thus, each $Na_i = 0$ which implies that each $a_i = 0$.

We recall that the set of bases of V (over $\mathbb{Q}$) is in bijection with $GL(V)$ and the set of bases of L (over $\mathbb{Z}$) is in bijection with $\mathrm{Aut}(L) = GL_n(\mathbb{Z})$. It follows from the previous comments that the set of lattices in V is in bijection with $GL(V)/\mathrm{Aut}(L) \cong GL_n(\mathbb{Q})/GL_n(\mathbb{Z})$.

If M is a subgroup of L of finite index, then M is also a lattice in V. This follows from the fact that the quotient L/M is a finitely generated, *torsion* abelian group, and is therefore of the form $\mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \mathbb{Z}/a_n\mathbb{Z}$ for some integers $a_i \geq 1$. It follows that there is a basis $v_1, \dots, v_n$ of L such that $a_1v_1, \dots, a_nv_n$ is a basis of M.

For any $\alpha \in GL(V)$, the image $\alpha(L)$ is another lattice in V. In particular, if $\alpha \in \mathbb{Q}^\times = \mathbb{Q} \smallsetminus \{0\}$ then αL is another lattice in V, with basis $\{\alpha v_1, \dots, \alpha v_n\}$.

If M and L are lattices in V, then there exists $\alpha, \beta \in \mathbb{Q}^\times$ such that $\alpha L \subseteq M \subseteq \beta L$ where each subgroup has finite index. It should be noted that this fact does not hold in a real vector space.

Definition. Assume that $\langle\, , \rangle : V \otimes V \to \mathbb{Q}$ is a nondegenerate bilinear form. Then there is an isomorphism $V \to \mathrm{Hom}(V, \mathbb{Q})$ which is given by $v \to \langle v, \, \rangle$. Assume that L is a lattice in V and define the *dual lattice* L^* of L to be $L^* = \{v \in V : \langle v, L\rangle \subseteq \mathbb{Z}\}$. The dual lattice is, in fact, a lattice: if $\{v_1, \dots, v_n\}$ is a basis of L, then L^* has the dual basis (over $\mathbb{Z}$) $\{v_1^*, \dots, v_n^*\}$ where v_i^* is given by $\langle v_i, v_j^*\rangle = \delta_{i,j}$ where $\delta_{i,j}$ is the Kronecker delta function.

Definition. Under these assumptions let E denote the "inner product matrix" $E = (\langle v_i, v_j\rangle)$. We define the *discriminant* of L as $\mathrm{disc}(L) = \det(E) \in \mathbb{Q}^\times$. This is independent of the basis chosen. To see this, fix a change-of-basis matrix $A \in GL_n(\mathbb{Z})$. After changing basis, the new inner product matrix is $E' = AEA^t$ whose determinant is $\det(E') = \det(A)^2 \det(E) = \det(E)$.

Definition. By multiplying our bilinear form by a nonzero integer, we may assume that $\langle L, L\rangle \subseteq \mathbb{Z}$. We note that this condition is equivalent to the condition $L \subseteq L^*$. A lattice satisfying these equivalent conditions is called *integral.* By definition, if L is an integral lattice, then $\mathrm{disc}(L) \in \mathbb{Z}$. Furthermore, we have the following proposition.

Proposition 1. *The index $(L^* : L) = \pm disc(L)$.*

Proof. Since L is a subgroup of L^*, and both groups are free abelian of rank n, the additivity of rank on short exact sequences shows that the rank of the quotient L^*/L is zero. Since the quotient is finitely generated, the classification of finitely generated abelian groups shows that the quotient is a finite group. Thus, the index $(L^* : L)$ is finite. From the observations above, it follows that there is a basis $\{v_1^*, \dots, v_n^*\}$ of L^* and nonzero integers $a_1, \dots, a_n$ such that the set $\{a_1v_1^*, \dots, a_nv_n^*\}$ forms a basis of L. Furthermore, $L^*/L \cong \oplus_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$, so that $(L^* : L) = |\prod_{i=1}^n a_i|$. Let $\{v_1, \dots, v_n\}$ denote the dual basis of L. Let E and E' denote the inner product matrices $E = (\langle v_i, v_j\rangle)$ and $E' = (\langle v_i, a_jv_j\rangle)$. By definition, E' is the diagonal matrix

$$E' = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

There is a matrix $A \in GL_n(\mathbb{Z})$ such that $E' = EA$, and it follows that

$$\mathrm{disc}(L) = \det(E) = \pm \det(E') = \pm a_1 \cdots a_n.$$

Thus, $(L^* : L) = |\prod_{i=1}^n a_i| = \pm \mathrm{disc}(L)$. ∎

Definition. A lattice L is *unimodular* if $L = L^*$. By the proposition, we see that this is equivalent to the condition that $\mathrm{disc}(L) = \pm 1$.

In the general (i.e., not necessarily unimodular) case, the inner product on V induces a pairing $\langle\, , \rangle : L^*/L \otimes L^*/L \to \mathbb{Q}/\mathbb{Z}$ which is a duality of finite abelian groups. It follows that the set of unimodular lattices M which lie between L and L^* is in bijection with the subgroups A of L^*/L such that $A = A^\perp$ under $\langle\, , \rangle$.

Example. Consider the lattice $\mathbb{Z}^n \subset \mathbb{Q}^n$ with $\langle \mathbf{x}, \mathbf{y}\rangle = \sum_i x_iy_i$. Then $\mathbb{Z}^n$ is a self-dual lattice and $e_i^* = e_i$.

Definition. An integral lattice L is *even* if, for all $v \in L$, $\langle v, v\rangle \in 2\mathbb{Z}$. Note that the previous example is not even.

Example. With $\mathbb{Z}^n$ as in the previous example, let $L = \{\sum_i a_i e_i : \sum_i a_i \in 2\mathbb{Z}\}$. Then $L \subset \mathbb{Z}^n$ is a sublattice of index 2. Furthermore, L is even since $\sum_i a_i^2 \equiv \sum_i a_i \pmod 2$.

Lemma 2. *Assume that M and L are lattices in $(V, \langle\ ,\ \rangle)$ such that M is a sublattice of L of index N. Then $disc(M) = N^2 disc(L)$.*

Example. If $L \subseteq \mathbb{Z}^n$ is the even sublattice of the previous example, then the lemma implies that $\mathrm{disc}(L) = 4$.

Proof. It is straight-forward to check that we have the following containments: $M \subseteq L \subseteq L^* \subseteq M^*$. We claim that the index $(M^*, L^*) = N$. Since $\langle\ ,\ \rangle : M^*/L^* \otimes L/M \to \mathbb{Q}/\mathbb{Z}$ is a duality of finite abelian groups and L/M has order N, it follows that M^*/L^* also has order N by the theory of finite abelian groups. By Proposition 1, we see that

$$\mathrm{disc}(M) = \pm(M^* : M) = \pm(L : M)(L^* : L)(M^* : L^*) = \pm N^2 (L^* : L) = \pm N^2 \mathrm{disc}(L).$$

Finally, $\mathrm{disc}(L)$ and $\mathrm{disc}(M)$ have the same sign. To see this, choose a basis $v_1, \dots, v_n$ of L such that there are nonzero integers $a_1, \dots, a_n$ such that $a_1 v_1, \dots, a_n v_n$ is a basis of M. Then

$$\mathrm{disc}(M) = \det(\langle a_i v_i, a_j v_j\rangle) = \det(a_i a_j \langle v_i, v_j\rangle) = \Big(\prod_i a_i^2\Big) \det(\langle v_i, v_j\rangle) = \Big(\prod_i a_i^2\Big)\mathrm{disc}(L)$$

as desired. $\square$

Example. Let $L \subset \mathbb{Z}^n$ be the even sublattice from the previous example. Then $L \subset \mathbb{Z}^n \subset L^*$. Since $\mathbb{Z}^n$ is unimodular, the proof of Lemma 2 shows that $(\mathbb{Z}^n : L) = 2 = (L^* : \mathbb{Z}^n)$. One can verify directly that the element $\eta = \frac{1}{2}(e_1 + \cdots e_2)$ is contained in L^*, but not in $\mathbb{Z}^n$. If n is odd, then $2\eta \notin L$ and $4\eta \in L$, and it follows that $L^*/L \cong \mathbb{Z}/4\mathbb{Z}$. If n is even, then every element of L^*/L is annihilated by 2, so that $L^*/L \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The inner product induces a pairing $\langle\ ,\ \rangle : L^*/L \times L^*/L \to (\frac{1}{2}\mathbb{Z})/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. We claim that for $v \in L^*/L$, $\langle v, v\rangle = 0$ in $\mathbb{Q}/\mathbb{Z}$ if and only if $n \equiv 0 \pmod 4$. If $n \not\equiv 0 \pmod 4$ then $\langle \eta, \eta\rangle = \frac{1}{4}n \notin \mathbb{Z}$. Assume that $n \equiv 0 \pmod 4$. It is always the case that for $v \in \mathbb{Z}^n$, $\langle v, v\rangle \in \mathbb{Z}$, so we need only check η: $\langle \eta, \eta\rangle = \frac{1}{4}n \in \mathbb{Z}$ since n is divisible by 4.

In the case when $L^*/L \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, there are exactly three distinct nontrivial subgroups of L^*/L. Thus, there are exactly three lattices in k which live between L and L^*. $\mathbb{Z}^n$ is one of these lattices, and we call the others M and M'. We claim that $n \equiv 0 \pmod 4$ if and only if M and M' are integral and unimodular. (Of course, by checking indexes, we see that M and M' are always unimodular, so the second condition is equivalent to M and M' being integral.) This follows from the fact that there are elements $v \in M$ and $v' \in M'$ such that $M = L + \mathbb{Z}v$ and $M' = L + \mathbb{Z}v'$. Then $\langle v, v\rangle$ and $\langle v', v'\rangle$ are integers if and only if for every $v'' \in L^*$, $\langle v'', v''\rangle$ is an integer.

Finally, if $n \equiv 0 \pmod 8$, then M and M' are both even. (This is the best of all worlds.) The point here is that $\langle \eta, \eta\rangle = \frac{1}{4}n \in 2\mathbb{Z}$ since n is divisible by 8. For more discussion and interesting applications, the interested reader is encouraged to consult *Sphere Packing, Lattices and Groups* by Conway and Sloan.

In order to define algebraic numbers and algebraic integers, we need the following propositions.

Proposition 3. *For any complex number α the following conditions are equivalent:*

1. *α satisfies a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with rational coefficients.*
2. *The smallest subfield $\mathbb{Q}(\alpha)$ of $\mathbb{C}$ containing $\mathbb{Q}$ and α is of finite degree over $\mathbb{Q}$.*
3. *There is a field k of finite degree over $\mathbb{Q}$ which contains α.*

Definition. We say that a complex number α is *algebraic* if one of these equivalent conditions holds.

Proof. "2.$\Rightarrow$ 3." clear

"1.$\Rightarrow$ 2." Since α satisfies a monic polynomial with rational coefficients, there exists unique such (monic) polynomial $g_\alpha(x) \in \mathbb{Q}[x]$ with minimal degree. Then $g_\alpha(x)$ is the generator of the nonzero ideal $I \subset \mathbb{Q}[x]$ of polynomials satisfied by α. I is a maximal ideal and the map $\mathbb{Q}[x]/I \to \mathbb{Q}(\alpha)$ given by $x + I \mapsto \alpha$ is an isomorphism. This implies that the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is finite.

"3.$\Rightarrow$ 1." The map $\alpha : k \to k$ given by multiplication by α is $\mathbb{Q}$-linear. The monic polynomial

$$f(x) = \det(xI - \alpha) = x^n - \mathrm{Tr}\,(\alpha)x^{n-1} + \cdots \pm \det(\alpha)$$

is clearly satisfied by α. $\square$

Corollary 4. *The set $\overline{\mathbb{Q}}$ of algebraic numbers forms a subfield of $\mathbb{C}$.*

Proof. Assume that $\alpha, \beta \neq 0$ are algebraic. It suffices to show that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic as well. Let $k = \mathbb{Q}(\alpha, \beta)$ denote the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}, \alpha, \beta$. Then the degree $(k : \mathbb{Q}(\alpha)) = (\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)) \leq (\mathbb{Q}(\beta) : \mathbb{Q})$ is finite since β is algebraic. Thus, $(k : \mathbb{Q}) = (\mathbb{Q}(\alpha) : \mathbb{Q})(k : \mathbb{Q}(\alpha))$ is finite. Since the desired elements are all contained in k, they are all algebraic as desired. $\square$

Proposition 5. *For any complex number α the following conditions are equivalent:*

1. *α satisfies a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with integer coefficients.*
2. *$\mathbb{Z}[\alpha]$ is a $\mathbb{Z}$-module of finite rank.*
3. *There is a subring $M \subset \mathbb{C}$ containing α which has finite rank as a $\mathbb{Z}$-module.*

Definition. We say that a complex number α is an *algebraic integer* if one of these equivalent conditions holds.

Proof. "1.$\Rightarrow$ 2." $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$.

"2.$\Rightarrow$ 3." clear

"3.$\Rightarrow$ 1." The argument from Proposition 3 applies. The map $\alpha : M \to M$ is an endomorphism of a free $\mathbb{Z}$-module. Therefore, the coefficients of the polynomial

$$f(x) = \det(xI - \alpha) = x^n - \mathrm{Tr}\,(\alpha)x^{n-1} + \cdots \pm \det(\alpha)$$

are integers. $\square$

Corollary 6. *The set $\overline{\mathbb{Z}}$ of algebraic integers forms a subring of $\overline{\mathbb{Q}}$.*

Proof. As before, given algebraic integers α, β, let $M = \mathbb{Z}[\alpha, \beta]$. This ring has finite rank as a $\mathbb{Z}$-module and contains $\alpha \pm \beta, \alpha\beta$. $\square$

Lemma 7. *With notation as above:*

1. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.
2. $\overline{\mathbb{Q}}/\overline{\mathbb{Z}}$ *is a torsion group (like $\mathbb{Q}/\mathbb{Z}$).*

Proof. 1. For $a \in \mathbb{Z}$, a satisfies the monic polynomial $x - a \in \mathbb{Z}[x]$. This gives the containment "$\supseteq$". For the other containment, fix $\alpha = a/b \in \overline{\mathbb{Z}} \cap \mathbb{Q}$ and suppose that $\alpha \notin \mathbb{Z}$. Without loss of generality, we assume that a and b are relatively prime. Since $\alpha \notin \mathbb{Z}$, it follows that $b \neq \pm 1$. If α satisfies the monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, then

$$a^n/b^n + a_{n-1}a^{n-1}/b^{n-1} + \cdots + a_0 = 0.$$

Multiplication by b^n yields the equation

$$a^n + \underbrace{ba^{n-1}a_{n-1} + \cdots + b^n a_0}_{\text{divisible by } b} = 0$$

which implies that a^n is divisible by b. However, since b is not a unit and $(a, b) = 1$, we see that this is a contradiction.

2. Assume that α satisfies the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$. For a positive integer N, let $\beta = N\alpha$. Then

$$0 = N^n((\beta/N)^n + a_{n-1}(\beta/N)^{n-1} + \cdots + a_0) = \beta^n + Na_{n-1}\beta^{n-1} + \cdots + N^n a_0$$

which implies that if we choose N such that $N^i a_{n-i} \in \mathbb{Z}$, then $\beta = N\alpha \in \overline{\mathbb{Z}}$. Thus, $\overline{\mathbb{Q}}/\overline{\mathbb{Z}}$ is a torsion group. $\square$

Lecture 2

Let $k \supseteq \mathbb{Q}$ be a number field. It follows from the definition that every element of k is algebraic. Let A denote the subring of algebraic integers in k, that is, $A = k \cap \overline{\mathbb{Z}}$. It follows that $A \cap \mathbb{Q} = \mathbb{Z}$.

Theorem 8. *A is a lattice in the rational vector space k.*

Proof. First, we claim that A contains a lattice L in k. To see this, fix a basis $v_1, \ldots, v_n$ of k over $\mathbb{Q}$. Since $\overline{\mathbb{Q}}/\overline{\mathbb{Z}}$ is a torsion group, there exists nonzero integer N such that $Nv_1, \ldots, Nv_n \in A$. Let $L = Nv_1\mathbb{Z} + \cdots + Nv_n\mathbb{Z}$, which is a lattice in k contained in A.

Now, consider the linear and bilinear forms on k defined by

$$\begin{aligned} k &\to \mathbb{Q} & \qquad\qquad k \times k &\to \mathbb{Q} \\ \alpha &\mapsto \mathrm{Tr}\,(\alpha) & (\alpha, \beta) &\mapsto \langle \alpha, \beta \rangle = \mathrm{Tr}\,(\alpha\beta) \end{aligned}$$

respectively. Recall that the trace is given by considering multiplication by α as a $\mathbb{Q}$-linear map $k \to K$ and using the formula

$$\det(xI - \alpha) = x^n - \mathrm{Tr}\,(\alpha)x^{n-1} + \cdots + (-1)^n \mathbb{N}(\alpha).$$

The fact that $\mathrm{Tr}\,(\alpha + \beta) = \mathrm{Tr}\,(\alpha) + \mathrm{Tr}\,(\beta)$ implies that $\langle\, , \rangle$ is a symmetric, bilinear form on k. Furthermore, it is nondegenerate since $\langle \alpha, \alpha^{-1} \rangle = \mathrm{Tr}\,(1) = \deg(k) \neq 0$. We need the following.

Lemma 9. *The image of A under the trace map is contained in $\mathbb{Z}$.*

Before we prove the lemma, we use it to complete the proof of the theorem. Consider the dual lattice of L with respect to this bilinear form: $L^* = \{\alpha \in k : \mathrm{Tr}\,(\alpha L) \subseteq \mathbb{Z}\}$. For every $\alpha \in A$, the fact that $L \subseteq A$ implies that $\alpha L \subseteq \alpha A \subseteq A$. Therefore, the lemma implies that $\alpha \in L^*$. Thus, $L \subseteq A \subseteq L^*$. Since the index $(L^* : L)$ is finite, we see that the index $(L^* : A)$ is also finite, which implies that A is a free abelian group of rank equal to the rank of L^*. That is, A is a lattice. ☐

Proof of Lemma 9. It suffices to show that all the coefficients of the polynomial $f_\alpha(x) = \det(xI - \alpha)$ are integers when $\alpha \in A \subseteq \overline{\mathbb{Z}}$. To see this, let $m = (\mathbb{Q}(\alpha) : \mathbb{Q})$ and let $\ell = (k : \mathbb{Q}(\alpha))$, so that $n = m\ell$. Then a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is exactly $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$. Let $g_\alpha(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ denote the minimal polynomial of α over $\mathbb{Q}$.

Let $\beta_1, \dots, \beta_\ell$ be a basis for k over $\mathbb{Q}(\alpha)$. Then $\{\alpha^i \beta_j : 1 \leq j \leq \ell, 0 \leq i \leq m-1\}$ forms a basis for k over $\mathbb{Q}$. We wish to find the matrix representing left multiplication by α with respect to this basis. Let T be the following $m \times m$ matrix:

$$T = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{m-1} \end{pmatrix}$$

The matrix for $xI - \alpha$ is then given in block form:

$$\begin{pmatrix} xI - T & 0 & \cdots & 0 \\ 0 & xI - T & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & \cdots & xI - T \end{pmatrix}$$

It follows that $f_\alpha(x) = (g_\alpha(x))^\ell$. Thus, it suffices to show that for $\alpha \in A$, the coefficients of the minimal polynomial of α are in $\mathbb{Z}$.

Over $\mathbb{C}$, we may factor $g_\alpha(x)$ as $g_\alpha(x) = \prod_{i=1}^{m}(x - \alpha_i)$. We then have a commuting diagram of $\mathbb{Q}$-isomorphisms of fields:

$$\begin{tikzcd}
\mathbb{Q}(\alpha) \arrow[ddd, "\cong"'] & & & \mathbb{Q}[x]/(g_\alpha(x)) \arrow[lll, "\cong"'] \arrow[ddd, "="] \\
& \alpha \arrow[d, mapsto] & x \arrow[l, mapsto] \arrow[d, mapsto] & \\
& \alpha_i & x \arrow[l, mapsto] & \\
\mathbb{Q}(\alpha_i) & & & \mathbb{Q}[x]/(g_\alpha(x)) \arrow[lll, "\cong"']
\end{tikzcd}$$

Since $\mathbb{Q}(\alpha_i) \cong \mathbb{Q}(\alpha)$ and these are finite extensions of $\mathbb{Q}$, Proposition 5 implies that the α_i are algebraic integers. Corollary 6 implies that the symmetric functions in the α_i are algebraic integers. Since these are the coefficients of $g_\alpha(x)$, they are also in $\mathbb{Q}$, and it follows that they are in $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. $\square$

Definition. We define the *discriminant* of k to be the discriminant of the lattice A in k with respect to the bilinear form $\langle \alpha, \beta \rangle = \mathrm{Tr}\,(\alpha\beta)$. That is, if $\alpha_1, \ldots, \alpha_n$ forms a basis of A over $\mathbb{Z}$, then $\mathrm{disc}(k) = \mathrm{disc}(A) = \det(\mathrm{Tr}\,(\alpha_i\alpha_j))$. Since $\mathrm{Tr}\,(A) \subseteq \mathbb{Z}$, this matrix has integer entries and $\mathrm{disc}(k) \in \mathbb{Z}$.

Example. If $k = \mathbb{Q}$, then $A = \mathbb{Z} = A^*$ and $\mathrm{disc}(\mathbb{Q}) = 1$. Next lecture, we shall prove the following theorem, due to Minkowski. The proof involves the "geometry of numbers".

Theorem. If $\mathrm{disc}(A) = \pm 1$, then $k = \mathbb{Q}$.

Proposition 10. *Let $k \supseteq \mathbb{Q}$ be a number field with ring of algebraic integers A, and let $d = disc(A)$. Then $d \equiv 0, 1 \pmod 4$. Equivalently, $d \equiv a^2 \pmod 4$ for some integer a.*

Proof. Since the extension $\mathbb{Q} \subseteq k$ is finite and separable, there are $n = (k : \mathbb{Q})$ distinct $\mathbb{Q}$-embeddings $\sigma_1, \ldots, \sigma_n$ of k into $\mathbb{C}$. Then $\mathrm{Tr}\,(\alpha) = \sum_{\ell=1}^{n} \sigma_\ell(\alpha)$ for all $\alpha \in k$. Let $\alpha_1, \ldots, \alpha_n \in A$ form a basis of A over $\mathbb{Z}$. It follows that $\mathrm{Tr}\,(\alpha_i\alpha_j) = \sum_{\ell=1}^{n} \sigma_\ell(\alpha_i\alpha_j) = \sum_{\ell=1}^{n} \sigma_\ell(\alpha_i)\sigma_\ell(\alpha_j)$. Let $B = (\sigma_\ell(\alpha_i))$, which is an $n \times n$ matrix with entries in $\overline{\mathbb{Z}}$. In particular, $\det(B) \in \overline{\mathbb{Z}}$. Then $d = \det(\mathrm{Tr}\,(\alpha_i\alpha_j)) = \det(B^tB) = \det(B)^2$. Expanding $\det(B)$ using the formula for $\mathrm{Tr}\,(\alpha_i)$ we have

$$\det(B) = \sum_{\pi \in S_n} \mathrm{sign}(\pi) \prod_{\ell=1}^{n} \sigma_\ell(\alpha_{\pi(\ell)}) = \sum_{\pi \in A_n} \prod_{\ell=1}^{n} \sigma_\ell(\alpha_{\pi(\ell)}) - \sum_{\pi \notin A_n} \prod_{\ell=1}^{n} \sigma_\ell(\alpha_{\pi(\ell)}) = x - y$$

where $x = \sum_{\pi \in A_n} \prod_{\ell=1}^{n} \sigma_\ell(\alpha_{\pi(\ell)})$ and $y = \sum_{\pi \notin A_n} \prod_{\ell=1}^{n} \sigma_\ell(\alpha_{\pi(\ell)})$. Since each α_i is an algebraic integer, it follows that each $\sigma_\ell(\alpha_{\pi(\ell)})$ satisfies the same monic polynomial as $\alpha_{\pi(\ell)}$ and is therefore an algebraic integer. Thus, x and y are both algebraic integers, as are the elements $x + y$ and xy. For any $\mathbb{Q}$-automorphism τ of $\mathbb{C}$, τ permutes the zeroes of any given polynomial with integer coefficients. In particular, for any fixed $\pi \in S_n$, τ permutes the set $\{\sigma_\ell(\alpha_{\pi(\ell)})\}_{\ell=1}^{n}$. It follows that τ simply rearranges the terms and factors of $x + y$ and xy, so that $\tau(x + y) = x + y$ and $\tau(xy) = xy$. By taking a finite Galois extension K of $\mathbb{Q}$ in $\mathbb{C}$ which contains $x + y$ and xy, we see that these elements are in the fixed field of the Galois group of K over $\mathbb{Q}$. That is, $x + y, xy \in \mathbb{Q}$. Since these elements are also in $\overline{\mathbb{Z}}$, we see that they are integers. Finally, this shows that

$$d = (\det(B))^2 = (x - y)^2 = (x + y)^2 - 4xy$$

which is of the form $d = (\text{integer})^2 - 4(\text{integer})$. Thus, $d \equiv a^2 \pmod 4$ for some integer a, as desired. $\square$

Example. We apply the proposition to the case of quadratic fields. Let k be an extension of $\mathbb{Q}$ of degree 2. The Theorem of the Primitive Element implies that $k = \mathbb{Q}(\alpha)$ for some $\alpha \in k$. Let $x^2 - bx + c$ be the minimal polynomial of α, and let $\beta = \alpha - \frac{b}{2}$. Then $\beta \in k \setminus \mathbb{Q}$ implies that $k = \mathbb{Q}(\beta)$. Furthermore, $\beta^2 = (\alpha - \frac{b}{2})^2 = \alpha^2 - b\alpha + \frac{b^2}{4} = \frac{b^2}{4} - c$. That is, β satisfies a polynomial of the form $x^2 - D$. By replacing β by a rational multiple of β (after replacing α by β) we may assume that the minimal polynomial of α is $x^2 - D$ where D is a square-free integer. It follows that $k \cong \mathbb{Q}[x]/(x^2 - D)$. Let A denote the ring of algebraic integers in k and let L denote the lattice $L = \mathbb{Z} + \mathbb{Z}\alpha$. Since $\alpha \in A$, it follows that $L \subseteq A$, and since these are both lattices in k, the index $N = (A : L)$ is finite. By Lemma 2, $d = \operatorname{disc}(A) = \operatorname{disc}(L)/N^2$. To compute $\operatorname{disc}(L)$, we let $\alpha_1 = 1$ and $\alpha_2 = \alpha$, and compute: $\operatorname{Tr}(1) = (k : \mathbb{Q}) = 2$; $\operatorname{Tr}(\alpha) = 0$ since the trace is the coefficient of x in the minimal polynomial $x^2 - D$ of α; and $\operatorname{Tr}(\alpha^2)$ is the sum of the two conjugates of $\alpha^2 = D$ which is $2D$ since $D \in \mathbb{Z}$. Thus,

$$\operatorname{disc}(L) = \det(\operatorname{Tr}(\alpha_i\alpha_j)) = \det\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D$$

and $d = 4D/N^2$, which is an integer.

There are two possibilities since D is square-free and $4D$ is divisible by N^2. (1) If $N = 1$ then $L = A$, which implies that $d = 4D \equiv 0 \pmod 4$. (2) If $N = 2$ then L has index 2 in A and $d = 4D/N^2 = 4D/4 = D$ and the following argument shows that $D \equiv 1 \pmod 4$. We write $\alpha = \sqrt{D}$ and note that since A/L has order 2, $2A \subseteq L$ which implies that $A \subseteq \frac{1}{2}L = \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{1}{2}\sqrt{D}$. We wish to know exactly when an element of $\frac{1}{2}L$ is in $A \setminus L$. Let $\beta = \frac{1}{2}(a + b\sqrt{D})$ be such an element. Then a and b are not both even. Since $\beta \in A$, the proof of Lemma 9 shows that $\mathbb{N}(\beta) \in \mathbb{Z}$. Direct computation shows that $\mathbb{N}(\beta) = \frac{1}{4}(a^2 - b^2D) \in \mathbb{Z}$, which implies that $a^2 - b^2D \in 4\mathbb{Z}$. That is, $a^2 \equiv b^2D \pmod 4$. If b were even, then this would imply that a is also even, a contradiction. Thus, b is odd, and $b^2 \equiv 1 \pmod 4$. It follows that $a^2 \equiv D \pmod 4$, so that if a were even, then D would be divisible by 4, contradicting the fact that D is square-free. Thus, $a^2 \equiv 1 \pmod 4$, which implies that $D \equiv 1 \pmod 4$. It also follows that $A = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{d}}{2}) = \mathbb{Z} + \mathbb{Z}(\frac{d+\sqrt{d}}{2})$.

Thus, we have proved the following.

Theorem 11. *The discriminants of quadratic fields are exactly the integers $d \equiv 0, 1 \pmod 4$, $d \neq 1$ which are as square free as possible. That is, the only square factor of d permitted is 4, and this occurs if and only if $\frac{d}{4} \not\equiv 0, 1 \pmod 4$.*

It follows that the possible values for d are

$$\begin{array}{ll} d > 0 & d = 5,\ 8, 12, 13,\ 17,\ 20,\ 21,\ \ldots \\ d < 0 & d = \text{-}3, \text{-}4,\ \text{-}7,\ \text{-}8, \text{-}11, \text{-}15, \text{-}17,\ \ldots \end{array}$$

The first list corresponds to real quadratic fields since $k = \mathbb{Q}(\sqrt{D})$ and $D = d > 0$ or $D = d/4 > 0$. The second list corresponds to imaginary quadratic fields.

Now we are in the position to completely describe the ring of integers for a quadratic field. If $d \equiv 0 \pmod 4$, then $A = L = \mathbb{Z} + \mathbb{Z}\sqrt{D}$. In this case, $D = d/4$ so that $A = \mathbb{Z} + \mathbb{Z}\frac{\sqrt{d}}{2} =$

$\mathbb{Z}+\mathbb{Z}(\frac{d+\sqrt{d}}{2})$. If $d \equiv 1 \pmod 4$, then $A = \mathbb{Z}+\mathbb{Z}(\frac{d+\sqrt{d}}{2})$, from the above work. Therefore, we have proved the following.

Theorem 12. *The ring of algebraic integers of a quadratic field k is always*

$$A = \mathbb{Z}+\mathbb{Z}\Big(\frac{d+\sqrt{d}}{2}\Big)$$

where $d = disc(k)$.

Lecture 3

Example. We continue with the example of quadratic fields. If $d = -4$, then with the previous notation, $D = -1$, and the ring of algebraic integers is the ring of Gaussian integers $A = \mathbb{Z}+\mathbb{Z}i \subset \mathbb{C} = \mathbb{R}+\mathbb{R}i$. Furthermore, $A^\times = \{i^n\}$ which is cyclic of order 4.

If $d = -3$, then $A = \mathbb{Z}+\mathbb{Z}(\frac{1+\sqrt{-3}}{2})$ is the ring of Eisenstein integers. If we let $\zeta = \frac{1+\sqrt{-3}}{2}$, then

$$\mathrm{Tr}\,(\zeta) = \frac{1+\sqrt{-3}}{2} + \frac{1-\sqrt{-3}}{2} = 1$$

and

$$\mathbb{N}(\zeta) = \Big(\frac{1+\sqrt{-3}}{2}\Big)\Big(\frac{1-\sqrt{-3}}{2}\Big) = \frac{1+3}{4} = 1.$$

It follows that $\zeta^2 - \zeta + 1 = 0$. Furthermore,

$$\zeta^3 = \frac{1+3\sqrt{-3}-9+(-3\sqrt{-3})}{8} = -1$$

so that ζ is a primitive sixth root of unity. Since $\zeta^2 = \frac{-1+\sqrt{-3}}{2}$, we see that $A = \mathbb{Z}+\mathbb{Z}\zeta = \mathbb{Z}+\mathbb{Z}\zeta^2$, and $A^\times = \{\zeta^n\}$ is cyclic of order 6. One point of interest here is that the point $(\zeta, \zeta^{-1}) \in \mathbb{C}^2$ is in the intersection of each Fermat curve $x^p + y^p = 1$ for primes $p > 3$.

If $d = 5$, then $A = \mathbb{Z}+\mathbb{Z}\epsilon$, where $\epsilon = \frac{1+\sqrt{5}}{2}$. Let $\epsilon' = \frac{1-\sqrt{5}}{2}$. Then $\epsilon\epsilon' = -1$ so that $\epsilon^{-1} = -\epsilon' \in A$. It follows that $A^\times = \{\pm 1\} \times \{\epsilon^{\mathbb{Z}}\}$.

Definition. If k is a number field, then an *order* in k is a subring $B \subseteq k$ of rank $n = (k : \mathbb{Q})$ as a free $\mathbb{Z}$-module.

An order B in k is always contained in the ring of algebraic integers with finite index. Since B is a lattice, it suffices to show that $B \subseteq A$. For $b \in B$, the fact that B is a ring implies that the $\mathbb{Z}$-linear map given by multiplication by b maps $B \to B$. Fixing a basis for B over $\mathbb{Z}$, this map is given by an $n \times n$ matrix with integer entries which we also denote b. Then b satisfies the polynomial $f_b(x) = \det(xI - b)$ which is monic with integer coefficients. Thus, $b \in A$. If $f = (A : B)$, then Lemma 2 implies that $\mathrm{disc}(B) = f^2\mathrm{disc}(A)$.

Proposition 13. *Assume that k is a quadratic field and f is a positive integer. Then there is a unique order $B = \mathbb{Z}+fA$ of index f in A, the ring of integers.*

Proof. It is clear that $B = \mathbb{Z} + fA$ is a ring. Furthermore, if $d = \mathrm{disc}(A)$, then $B = \mathbb{Z} + fA = \mathbb{Z} + f\mathbb{Z}(\frac{d+\sqrt{d}}{2})$ is a lattice. Thus, B is an order, and this formulation shows that B has index f in A. Let B' be any order in k with index f in A. Then f annihilates A/B' so that $fA \subseteq B' \subseteq A$. Since B' is a ring, $\mathbb{Z} \subseteq B'$ so that $B \subseteq B' \subseteq A$. Since B and B' both have index f in A, they must be equal. $\square$

If $d = \mathrm{disc}(A)$ and $d_B = \mathrm{disc}(B)$, then $d_B = f^2 d \equiv 0, 1 \pmod 4$. It follows that

$$B = \mathbb{Z} + f\mathbb{Z}\Big(\frac{d+\sqrt{d}}{2}\Big) = \mathbb{Z} + \mathbb{Z}\Big(\frac{f^2 d + f\sqrt{d}}{2}\Big) = \mathbb{Z} + \mathbb{Z}\Big(\frac{d_B + \sqrt{d_B}}{2}\Big).$$

Example. If $d = -3$, then $A = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-3}}{2})$. The unique order given by $f = 2$ is $B = \mathbb{Z} + 2A = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$, and $B^\times = \{\pm 1\}$.

If $d = -4$, then $A = \mathbb{Z} + \mathbb{Z}i$. In this case ,the order of index 2 is $B = \mathbb{Z} + \mathbb{Z}2i$. Again $B^\times = \{\pm 1\}$.

We note that there is a correspondence between orders B in a quadratic field k and binary quadratic forms. If $q(x,y) = ax^2 + bxy + cy^2$ for integers a, b, c then the discriminant of q is $\mathrm{disc}(q) = b^2 - 4ac$. If M is a free $\mathbb{Z}$-module of rank 2, then choosing a basis e_1, e_2 of M induces a map $q : M \to \mathbb{Z}$ given by $q(xe_1 + ye_2) = q(x,y)$. We can use q to induce a symmetric bilinear form $[\,,\,] : M \times M \to \mathbb{Z}$ by defining $[m,n] = q(m+n) - q(m) - q(n)$. It is straightforward to verify that this operation is symmetric and bilinear. What we notice, however, is that this form is even since $[m,m] = q(2m) - 2q(m) = 4q(m) - 2q(m) = 2q(m)$. If we compare this to the bilinear form $\langle \alpha, \beta \rangle = \mathrm{Tr}\,(\alpha\beta)$ on $B \subseteq k$, we see that it is not always even, even when $d \equiv 1 \pmod 4$. For example, when $d = 5$, we have $\epsilon = \frac{1+\sqrt{5}}{2}$ and $\langle \epsilon, \epsilon \rangle = \mathrm{Tr}\,(\epsilon^2) = \mathrm{Tr}\,(\frac{3+\sqrt{5}}{2}) = 3$. From this we see that we should devise an alternate bilinear form on k.

From our notes before, we know that there is a square-free integer D such that $k \cong \mathbb{Q}(\sqrt{D})$. Quadratic extensions are always Galois, and the nontrivial $\mathbb{Q}$-automorphism of k is given by $\sigma(\sqrt{D}) = -\sqrt{D}$. We define a new bilinear form $\{\,,\,\}$ on k by the formula $\{x,y\} = \mathrm{Tr}\,(x\sigma(y))$. Since $\mathrm{Tr}\,(x) = x + \sigma(x)$, it is straightforward to verify that this form is symmetric and bilinear. If we restrict to $B \times B$, the form takes its values in $\mathbb{Z}$ since $B \subseteq A$ and $\sigma(A) = A$. Furthermore, for $x \in B$, $\{x,x\} = \mathrm{Tr}\,(x\sigma(x)) = 2\mathbb{N}(x) \in 2\mathbb{Z}$. B is a free $\mathbb{Z}$-module of rank 2, and we define $q : B \to \mathbb{Z}$ by $x \mapsto \frac{1}{2}\{x,x\}$. With the correct basis, this is a binary quadratic form. Let $d_B = \mathrm{disc}(B)$ and $\alpha = \frac{d_B + \sqrt{d_B}}{2}$, so that $1, \alpha$ forms a basis of B over $\mathbb{Z}$. Then

$$\begin{aligned} q(x,y) &= \tfrac{1}{2}\{x + y\alpha, x + y\alpha\} = \mathbb{N}(x + y\alpha) \\ &= \Big(x + y\Big(\frac{d_B + \sqrt{d_b}}{2}\Big)\Big)\Big(x + y\Big(\frac{d_B - \sqrt{d_b}}{2}\Big)\Big) \\ &= x^2 + d_B xy + \frac{d_B^2 - d_B}{4} y^2 \end{aligned}$$

The coefficients 1 and d_B are clearly integers, and since $d_B \cong 0, 1 \pmod 4$ we see that $\frac{d_B^2 - d_B}{4}$ is also an integer. Furthermore, $\mathrm{disc}(q) = d_B^2 - (d_B^2 - d_B) = d_B = \mathrm{disc}(B)$. It is important to note that frequently there are many quadratic forms of discriminant d_B other than the ones coming from this construction.

Example. Let $d = -15$ and consider the quadratic forms $q_1(x, y) = x^2 - 15xy + 60y^2$ and $q_2(x, y) = 2x^2 + xy + 2y^2$, which both have discriminant -15. These forms are not equivalent under any change of basis. To see this we notice that the first form comes from our construction. If these were equivalent, then A would have an element of norm 2 since $\mathbb{N}(e_1) = q_2(1, 0) = 2$. This is impossible, though, since if $2 = \mathbb{N}(\frac{a+b\sqrt{-15}}{2}) = \frac{a^2+15b^2}{4}$ then $a^2 + 15b^2 = 8$ which is impossible for integers a and b. It turns out that there is an ideal $I \subset A$ of index 2 which leads to q_2.

Now, we discuss the "geometry of numbers" which will help us find estimates of d from the degree n of k. It will also give an elegant proof of the theorem of Minkowski from last lecture. We have a chain of containments $A \subset k \subset k \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^n$ so we may view A as a discrete, co-compact subspace of Euclidean space. Let $k = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f_\alpha(x)$ where f_α is the minimal polynomial of α over $\mathbb{Q}$. By definition, f_α is irreducible over $\mathbb{Q}$, but over $\mathbb{R}$ it splits into a product $f_\alpha(x) = \prod_i g_i(x)$ of distinct irreducible factors of degree 1 or 2. (The factors are distinct by separability.) If r_1 is the numbers of real zeroes of f_α and r_2 is the number of conjugate pairs of complex zeroes, then $r_1 + 2r_2 = n$ and the Chinese Remainder Theorem implies that

$$k \otimes \mathbb{R} = \mathbb{R}[x]/f_\alpha(x) = \mathbb{R}[x]/\prod_i g_i(x) = \prod_i \mathbb{R}[x]/g_i(x) = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

As a side note, another method for obtaining r_1 and r_2 is to consider the nondegenerate bilinear form $\langle x, y\rangle = \mathrm{Tr}\,(xy)$ on $k \otimes \mathbb{R}$ and to observe that this form has signature $(r_1 + r_2, r_2)$.

Example. For the quadratic fields $k = \mathbb{Q}(\sqrt{D})$ where D is square-free, we see that

$$k \otimes \mathbb{R} = \begin{cases} \mathbb{R} \times \mathbb{R} & \text{if } D > 0 \\ \mathbb{C} & \text{if } D < 0 \end{cases}$$

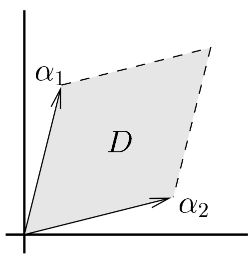
because if $D > 0$ then $f_\alpha(x) = x^2 - D$, and if $D < 0$ then $f_\alpha(x) = x^2 + D$. This is a specific case of the general fact that r_1 is the number of distinct real embeddings of a general number field k, and r_2 is the number of distinct conjugate pairs of complex embeddings.

We also observe that $k \otimes \mathbb{C} \cong \mathbb{C}^n$. Let $\sigma_1, \ldots, \sigma_n$ be the distinct n embeddings of k into $\mathbb{C}$. Then the isomorphism $k \otimes \mathbb{C} \to \mathbb{C}^n$ is given by $\alpha \otimes 1 \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$.

Let $L \subset k$ be any lattice in k. The fundamental domain for L acting on $\mathbb{R}^n$ is

$$D = \Big\{\sum_{i=1}^{n} x_i\alpha_i : 0 \le x_i < 1\Big\}$$

as in the figure.



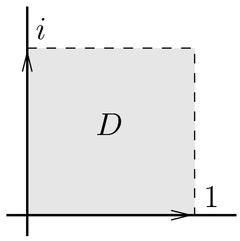
Proposition 14. *$disc(L) = (-4)^{r_2}(vol(D))^2$.*

Corollary 15. *The sign of $disc(L)$ is $(-1)^{r_2}$.*

Proof. If $r_2 = 0$, then all of the embeddings $\sigma_1, \ldots, \sigma_n$ of k are real. Let $\alpha_1, \ldots, \alpha_n$ be a basis of L. The coordinates of α_i in the standard orthonormal basis of $\mathbb{R}^n$ are $(\sigma_1(\alpha_i), \ldots, \sigma_n(\alpha_i))$ and $\mathrm{vol}(D) = |\det(\sigma_i(\alpha_j))|$. If $B = (\sigma_i(\alpha_j))$ then we already observed that $\mathrm{disc}(L) = \det(B^t B) = (\det(B))^2 = (\mathrm{vol}(D))^2$, as desired.

If $r_2 \neq 0$, then each conjugate pair of complex embeddings contributes a factor of $dz \wedge d\overline{z} = -2i dx \wedge dy$. Thus, each such pair contributes a factor of $(-2i)^2 = -4$, for a total contribution of $(-4)^{r_2}$. For more details, the interested reader should consult the book *Théorie algébrique des nombres* by Samuel. □

Example. Consider the Gaussian integers $A = \mathbb{Z}[i] \subset k \otimes \mathbb{R} = \mathbb{C} = \mathbb{R} + \mathbb{R}i$. The fundamental domain of A



has volume 1, and $\mathrm{disc}(A) = -4$.

Definition. A subset P of Euclidean space is *centrally symmetric* if for each point x of P, $-x$ is also a point of P.

Theorem 16. *Suppose that L is a lattice in $\mathbb{R}^n$ with fundamental domain D, P is a closed, bounded, convex, centrally symmetric subset of $\mathbb{R}^n$ and $vol(P) \geq 2^n vol(D)$. Then P contains a nonzero point of L.*

Proof. We will prove the theorem in the case $\mathrm{vol}(P) > 2^n \mathrm{vol}(D)$. A simple limiting argument gives the general case since P is closed and L is discrete.

If we let $\frac{1}{2}P = \{\frac{1}{2}x : x \in P\}$ then the condition $\mathrm{vol}(P) > 2^n \mathrm{vol}(D)$ is equivalent to the condition $\mathrm{vol}(\frac{1}{2}P) > \mathrm{vol}(D)$. We claim that there are distinct points $x, y \in \frac{1}{2}P$ such that $x - y \in L$. This will establish the theorem since it follows that $x = \frac{1}{2}p$ and $y = -\frac{1}{2}q$ for some points $p, q \in P$ (by central symmetry). Then $0 \neq x - y = \frac{1}{2}p + \frac{1}{2}q \in P$ by convexity, and $x - y$ is the desired point.

We give an intuitive argument to see that such x and y exist. The interested reader can find the details in Samuel. We can translate pieces of $\frac{1}{2}P$ mod L to fill up D, like cutting up a round carpet to cover the floor of a square room. Since $\mathrm{vol}(P) > 2^n \mathrm{vol}(D)$, it follows that some point of D is double-covered in this process. That is, there are distinct points x, y of $\frac{1}{2}P$ whose images via some translation by a vector of L are the same., So, $x \equiv y \pmod{L}$, as desired. □

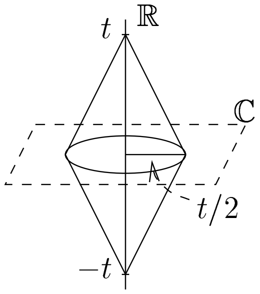
Theorem 17. *If L is any lattice in k, then there exists a nonzero element α of L such that*

$$|\mathbb{N}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |disc(L)|^{1/2}.$$

Proof. For $t > 0$, let P_t be the following region in $\mathbb{R}^n \cong k \otimes \mathbb{R}$:

$$P_t = \left\{\alpha \in k \otimes \mathbb{R} : \sum_{i=1}^{n} |\sigma_i(\alpha)| \leq t\right\}$$

As the sketch suggests



the volume of P_t is

$$\mathrm{vol}(P_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} \tag{1}$$

which can be verified directly by integration. Choose t so that $\mathrm{vol}(P_t) = 2^n\mathrm{vol}(D)$. By Proposition 14,

$$\mathrm{vol}(P_t) = 2^n\mathrm{vol}(D) = \frac{2^{(r_1+2r_2)}|\mathrm{disc}(L)|^{1/2}}{2^{r_2}} = 2^{(r_1+r_2)}|\mathrm{disc}(L)|^{1/2} \tag{2}$$

Then P_t satisfies the hypotheses of Theorem 16, and we may fix $\alpha \in (L \setminus \{0\}) \cap P_t$. Then

$$|\mathbb{N}(\alpha)|^{1/n} = \underbrace{\left(\prod_{i=1}^{n} |\sigma_i(\alpha)|\right)^{1/n}}_{\text{geometric mean}} \leq \underbrace{\frac{1}{n}\sum_{i=1}^{n} |\sigma_i(\alpha)|}_{\text{arithmetic mean}} \leq \frac{t}{n} \tag{3}$$

which implies that $|\mathbb{N}(\alpha)| \leq \frac{t^n}{n^n}$. From equations (1), (2) and (3) it follows that

$$|\mathbb{N}(\alpha)| \leq \frac{t^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\mathrm{disc}(L)|^{1/2}$$

as desired. $\square$

Corollary 18. *If A is the ring of algebraic integers in a number field k, then*

$$|disc(A)|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}.$$

Proof. Every $\alpha \in A \setminus \{0\}$ has $|\mathbb{N}(\alpha)| \geq 1$, so the theorem implies that for some such α,

$$1 \leq |\mathbb{N}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\mathrm{disc}(A)|^{1/2}$$

from which the result is immediate. $\square$

Corollary 19. *(Minkowski) If disc$(A) = \pm 1$, then $A = \mathbb{Z}$ and $k = \mathbb{Q}$.*

Proof. The function of n:

$$\frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2n} \leq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2r_2} \leq |\mathrm{disc}(A)| = 1$$

is monotone increasing, and for $n = 2$

$$\frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2n} > 1.$$

It follows that $n = 1$. $\square$

Lecture 4

Let k be a number field with ring of algebraic integers A, and let $d = \mathrm{disc}(A)$. We now use the geometry of numbers to give a bound on d in terms of $n = (\mathbb{Q} : k)$. By Corollary 18

$$|d|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}.$$

By Stirling's formula, $n! = \Gamma(n+1)$, so there exists θ in the interval $(0,1)$ such that

$$n! = \sqrt{2\pi n}\, n^n e^{(-n+\frac{\theta}{12n})}$$

and it follows that

$$|d|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2} = \frac{e^{(n-\frac{\theta}{12n})}}{\sqrt{2\pi n}}\left(\frac{\pi}{4}\right)^{r_2}.$$

Raising both sides to the $2/n$ power, we find that

$$|d|^{1/n} \geq e^2\left(\frac{\pi}{4}\right)^{2r_2/n}\left(\frac{e^{(-\frac{\theta}{6n^2})}}{\sqrt[n]{2\pi n}}\right).$$

We can write $e^2 = (e^2)^{n/n} = (e^2)^{(\frac{r_1}{n}+\frac{2r_2}{n})}$ so that

$$|d|^{1/n} \geq (e^2)^{r_1/n}\left(e^2\frac{\pi}{4}\right)^{2r_2/n}\left(\frac{e^{(-\frac{\theta}{6n^2})}}{\sqrt[n]{2\pi n}}\right).$$

The factor $\left(\frac{e^{(-\frac{\theta}{6n^2})}}{\sqrt[n]{2\pi n}}\right) \to 1$ as $n \to \infty$ so that

$$|d|^{1/n} \gtrapprox_{n\to\infty} (7.3)^{r_1/n}(5.8)^{2r_2/n}$$

Example. If $n = 2r_2$ (the case when k is totally complex) then asymptotically $|d|^{1/n} \geq 5.8$ so that $|d| \geq (5.8)^n$. This inequality actually holds for $n \geq 10^8$.

Stark-Odlyzko have given the following improvement on the bound. Assuming the Riemann Hypothesis for the zeta function of k:

$$|d|^{1/n} \geq (215)^{r_1/n}(44)^{2r_2/n}.$$

In the totally complex case $n = 2r_2$, this gives the bound $|d| \geq (44)^n$.

Now we consider the arithmetic properties of the ring of integers A of a number field k. It is a fact that A is a Dedekind domain, i.e., a smooth ring of dimension 1. In particular, every ideal I in A is a product of prime ideals. However, if we take an arbitrary order B in k, then B will generally not be a Dedekind domain. Among other things, we want to know what keeps B from being a Dedekind domain.

We note that there are standard methods of constructing new Dedekind domains from old ones. If A_0 is a Dedekind domain, with field of quotients $k_0 \supset A_0$ and k is a finite separable extension of k_0, then we let A be the integral closure of A_0 in k. It follows that A is a Dedekind domain, as well.

Given two lattices L and M in k, we have ways of combining L and M to get other lattices in k. (We will apply these constructions mostly to ideals of an order B, but they are valid in this more general context.) The intersection $L \cap M$ is a lattice in k since there is a nonzero rational number α such that $\alpha L \subseteq M$. This implies that there are nonzero integers a, b such that $aL \subseteq bM$, and it follows that for all $x \in L$, $ax \in aL \cap bM \subseteq L \cap M$. That is, $L/(L \cap M)$ is torsion and finitely generated, so that $L \cap M$ has finite index in L. The sum $L + M$ is also a lattice because the same argument as above shows that $a(L + M) \subseteq M$ so that $(L + M)/M$ is also finitely generated and torsion. The product

$$L \cdot M = \left\{ \sum_i \ell_i m_i : \ell_i \in L, m_i \in M \right\}$$

is a lattice because if $m_1, \ldots, m_n$ is a basis for M then $L \cdot M = Lm_1 + \cdots + Lm_n$ is a finite sum of lattices. The quotient

$$L/M = \{\alpha \in k : \alpha M \subseteq L\} = \cap_{i=1}^n Lm_i^{-1}$$

is a finite intersection of lattices and therefore a lattice. The quotient lattice should not be confused with the quotient of a group by a subgroup since M is not necessarily contained in L. We call this lattice the quotient and use the fraction notation because the definition implies that $(L/M) \cdot M \subseteq L$, so that in some sense L/M (almost) behaves like an object which we might call $L \cdot M^{-1}$. It is important to note that strict containment may occur here, so this justification is, at best, imprecise. We also note that $L \cdot M = L \otimes_{\mathbb{Z}} M$ and $L/M = \hom_{\mathbb{Z}}(M, L)$. Finally, $L/L = \{\alpha \in k : \alpha L \subseteq L\} = \mathrm{End}(L)$ is a ring, and therefore an order in k. If we let $B = L/L$, then L is a left B-module in k.

Fix an order B in k and let I be a nonzero ideal of B. Then I is a lattice in k since for a nonzero element $\alpha \in I$, $\alpha B \subseteq I \subseteq B$. αB is a lattice, so it follows that I has finite index in B. Furthermore, by definition, $B \subseteq I/I$.

Lemma 20. *The index* $(B : \alpha B) = |\mathbb{N}(\alpha)|$.

Proof. $(B : \alpha B) = |\det(\alpha : B \to B)| = |\mathbb{N}(\alpha)|$ by definition. $\square$

Definition. If I is a nonzero ideal in an order B, then we define the *norm* of I to be the index $\mathbb{N}(I) = (B : I)$.

Definition. If L is any lattice in k (not necessarily contained in B) with $\mathrm{End}(L) \supseteq B$, then we say that L is a *fractional ideal* of B. The condition $\mathrm{End}(L) \supseteq B$ is equivalent to the condition $BL \subseteq L$.

Proposition 21. *An order B in k is a domain of dimension 1, i.e., every nonzero prime ideal $P \subset B$ is maximal.*

Proof. B is a domain since it is a subring of a field. Since P has finite index in B, the ring $k_P = B/P$ is a finite integral domain. For a nonzero element α of k_P the multiplication map $\alpha : k_P \to k_P$ is therefore injective, and since k_P is finite, the map is also surjective. This implies that k_P is a field since this homomorphism maps onto the identity. Thus, P is maximal. $\square$

Definition. An ideal I of B is called *principal* if $I = \alpha B$ for some $\alpha \in B$. We notice that a principal ideal $I = \alpha B$ satisfies the condition $\mathrm{End}(I) = B$:

$$\mathrm{End}(I) = \{\beta \in k : \beta\alpha B \subseteq \alpha B\} = \{\beta \in k : \beta B \subseteq B\} = B$$

The last equality follows from two facts: (1) every element of B maps $B \to B$ since B is a ring, so "$\supseteq$"; and (2) if $\beta \in k$ amps $B \to B$, then $\beta = \beta(1) \in \beta B \subseteq B$, so "$\subseteq$".

We claim that non-maximal orders are not principal ideal domains (even though they are all domains of dimension 1). To see this, let $B \subset A$ be an order with index $f = (A : B) > 1$. Then the ideal fA is principal in A and is contained in B (and is an ideal in B since $fA \subset B \subset A$). However, fA is not a principal ideal of B since, if it were, then the above notes would show that $\mathrm{End}(fA) = B$. But $\mathrm{End}(fA) = A \neq B$ so this is not possible.

Example. Here is a case where the ring of integers $A \subset k$ is not a principal ideal domain. Let p be a positive prime in $\mathbb{Z}$ such that $p \equiv 1 \pmod 4$ and let $k = \mathbb{Q}(\sqrt{-p})$. Then by our work in Lecture 2, $A = \mathbb{Z} + \mathbb{Z}(\sqrt{-p})$ since the discriminant is $d = -4p$ and

$$A = \mathbb{Z} + \mathbb{Z}\Big(\frac{-4p + \sqrt{-4p}}{2}\Big) = \mathbb{Z} + \mathbb{Z}(-2p + \sqrt{-p}) = \mathbb{Z} + \mathbb{Z}\sqrt{-p}$$

Let $I = \{a + b\sqrt{-p} : a \equiv b \pmod 2\} \subset A$. I is an ideal of A, as follows. Clearly, I is closed under addition. Take $a + b\sqrt{-p} \in I$ and $\alpha + \beta\sqrt{-p} \in A$. Then

$$(a + b\sqrt{-p})(\alpha + \beta\sqrt{-p}) = (a\alpha - b\beta p) + \sqrt{-p}(a\beta + b\alpha)$$

The relation between a and b says that a and b are either both odd or both even. If a and b are both even, then the product is in $2A \subseteq I$. If they are both odd, then since p is odd, $a\alpha - b\beta p \equiv \alpha + \beta \pmod 2$ and $a\beta + b\alpha \equiv \alpha + \beta \pmod 2$, so mod 2 the coefficients of the product are the same and the product is in I. It is straightforward to check (by the definition of I) that the containments $A \subset I$ and $I \subset 2A$ each have index 2. Now, suppose that I were principal, say $I = \alpha A$. Then $\mathbb{N}(\alpha) = (A : \alpha A) = (A : I) = 2$. However, if $\alpha = a + b\sqrt{-p}$, then $2 = \mathbb{N}(\alpha) = a^2 + pb^2$, which can never occur since $p \geq 5$. Thus, I is not principal. Note that this example encompasses the classical example which states that $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ is not a principal ideal domain.

Next, we want to show that if $P \subset A$ is a nonzero prime ideal, then $P \cdot (A/P) = A$. That is, A/P is a fractional ideal which "inverts P".

Proposition 22. *Let B be an order in k and P a nonzero prime in B. Then exactly one of the following holds.*

1. *$P \cdot (B/P) = B$, or*
2. *$P/P = End(P) \supsetneq B$.*

This proposition follows from the following theorem.

Theorem 23. *Let B be an order in k and P a nonzero prime in B. Then $B/P \supsetneq B$.*

Example. If p is a prime in $\mathbb{Z}$, then $\mathbb{Z}/p\mathbb{Z} = \frac{1}{p}\mathbb{Z} \supsetneq \mathbb{Z}$.

Proof of Proposition 22. We have the following containments in general:

$$P = B \cdot P \subseteq (B/P) \cdot P \subseteq B.$$

If $(B/P) \cdot P = B$, then 1. holds. Otherwise, $(B/P) \cdot P = \subsetneq B$. It is straightforward to show that $(B/P) \cdot P$ is an ideal in B. The maximality of P implies that $P = (B/P) \cdot P$, and the theorem implies that there exists $\gamma \in (B/P) \smallsetminus B$. Then $\gamma P \subseteq (B/P) \cdot P = P$ which implies that $\gamma \in (P/P) \smallsetminus B$, which implies 2. □

We need a bit more machinery before we can prove the theorem. Let M be a nonzero, simple, finite B-module. Then M is cyclic, say $M = Be$. Let P be the annihilator of M, $P = \mathrm{Ann}(e) \subset B$. Then the map $B/P \to M$ given by $b \mapsto be$ is an isomorphism of one-dimensional vector spaces over the residue field B/P.

Proposition 24. *Any nonzero ideal I in an order B of k contains a product of prime ideals $P_1, \ldots, P_t$. The primes which occur in this product are exactly the primes which contain I.*

Proof. Since I has finite index in B, we can find a chain of ideals $I = I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_t = B$ such that each quotient I_m/I_{m-1} is a simple B-module. By the previous remark, there are prime ideals $P_1, \ldots, P_t$ such that $I_m/I_{m-1} \cong B/P_m$. It follows that $P_m I_m \subseteq I_{m-1}$, and therefore, $P_1 \cdots P_t \subseteq I_0 = I$.

To prove the second claim, let $P \supseteq I \subseteq P_1 \cdots P_t$. By maximality, it suffices to show that some $P_i \subseteq P$. Suppose that no P_i is contained in P. Then there are elements $\alpha_i \in P_i \smallsetminus P$, and the product of these elements is in $P_1 \cdots P_t \subseteq I \subseteq P$. However, the product is not in P since P is prime and no factor is in P, yielding a contradiction. □

We note, in addition, that the norm $\mathbb{N}(I) = \prod_{i=1}^{t} \mathbb{N}(P_i)$. The chain of ideals $I = I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_t = B$ shows us that

$$\mathbb{N}(I) = (B : I) = (I_t : I_{t-1}) \cdots (I_1 : I_0) = (B : P_t) \cdots (B : P_1) = \mathbb{N}(P_t) \cdots \mathbb{N}(P_1)$$

as claimed.

Example. In the notation of the proposition, I may not equal $P_1 \cdots P_t$. Let k be a quadratic field with ring of integers A. By Proposition 13, for a fixed prime p there is a unique order $B = \mathbb{Z} + pA \subset A$ with index $(A : B) = p$. By our notes above, the ideal of A $P = pA \subset B$ is also an ideal in B which is prime and not principal in B. Furthermore, $I = pB \subset pA$. P is the unique prime of B containing I and $P \supsetneq I \supset P^2 = p^2 A$, but $I \neq P^2$ since $p \in I \setminus P^2$.

Proof of Theorem 23. It is clear from the definition that $B \subseteq B/P$. To see that equality does not hold, fix a nonzero element α of P and let $I = \alpha B \subseteq P \subset B$. By Proposition 24, there are primes $P_1, \ldots, P_t$ such that $I \supseteq PP_1 \cdots P_t$. If $I \supseteq P_1 \cdots P_t$, then $P = P_i$ for some i. Cancel off as many "factors" of P as possible so that we may assume that $P_1 \cdots P_u \not\subseteq I$ and $PP_1 \cdots P_u \subseteq I$. Fix $\beta \in (P_1 \cdots P_u) \setminus I$. Then in k, $\gamma = \beta/\alpha \notin B$ and $\gamma P \subseteq B$ so that $\gamma \in B/P$. ☐

Corollary 25. *If P is a prime ideal in the ring of integers A, then $P \cdot (A/P) = A$.*

Proof. By Proposition 22, if $P \cdot (A/P) \neq A$, then $\mathrm{End}(P)$ is a ring in k which properly contains A. But every order in k is contained in A, so this is a contradiction. ☐

Theorem 26. *(Dedekind) Let A be the ring of integers in a number field k.*

1. *Every nonzero prime ideal is invertible, in the sense that there is a fractional ideal $P^{-1} \subset k$ such that $PP^{-1} = A$.*
2. *Every ideal is uniquely the product of prime ideals $I = P_1 \cdots P_t$.*
3. *The set Ideal of fractional ideals forms an abelian group, freely generated by the prime ideals of A. The identity element is A, and for any fractional ideal I, $I^{-1} = A/I$. If $I = \prod_P P^{ord_P(I)}$, then the isomorphism Ideal $\to \oplus_P \mathbb{Z}$ is given by $I \mapsto (\ldots, ord_P(I), \ldots)$.*

Proof. 1. follows from Corollary 25 since A/P is a fractional ideal. We shall prove 3. in the following lecture.

2. As in the proof of Proposition 24, we have ideals I_j and prime ideals P_j such that

$$P_1 \cdots P_t \subseteq I = I_0 \subset I_1 \subset \cdots \subset I_t = B$$

If $t = 1$, then the only prime containing I is P_1 and $P_1 \subseteq I \subseteq P_1$ which implies that $I = P_1$. So, we proceed by induction. The chain $I_1 \subset I_2 \subset \cdots \subset I_t = B$ satisfies the induction hypothesis, so

$$P_2 \cdots P_t = I_1 \supseteq I \supseteq P_1 \cdots P_t = P_1 I_1$$

Multiplying by $P_2^{-1} \cdots P_t^{-1}$ yields

$$A \supseteq IP_2^{-1} \cdots P_t^{-1} \supseteq P_1$$

If $A = IP_2^{-1} \cdots P_t^{-1}$, then multiplying by $P_2 \cdots P_t$ implies that $I = P_2 \cdots P_t$. This implies that A/I has a Jordan-Holder series with $t - 1$ links, a contradiction. Thus,

$A \neq IP_2^{-1} \cdots P_t^{-1}$, and the maximality of P_1 implies that $IP_2^{-1} \cdots P_t^{-1} = P_1$ so that multiplying by $P_1 \cdots P_t$ implies that $I = P_1 \cdots P_t$.

For uniqueness, we write $I = P_1 \cdots P_t = P_1' \cdots P_u'$. Then $P_1 \supseteq P_1' \cdots P_u'$ which implies that $P_1 = P_i'$ for some i as in the proof of Proposition 24. Multiply by P_1^{-1} and apply induction. □

Lecture 5

Proof of Theorem 26, Part 3. We already have unique factorization for integral ideals. To factor and invert an arbitrary fractional ideal, we use the following lemma to reduce to the case of integral ideals.

Lemma 27. *If L is any fractional ideal of A, there exist integral ideals I, J such that $I \cdot L = J$.*

Proof. Let $J = L \cap I \subseteq A$, which is an integral ideal. Our result follows from the following sublemma. □

Lemma 28. *If J and L are fractional ideals such that $J \subseteq L$, then there exists an integral ideal I such that $I \cdot L = J$.*

Proof. By our notes in Lecture 1, since A and L are both lattices, there exists nonzero rational number α such that $\alpha L \subseteq A$. It follows that $\alpha J \subseteq \alpha L \subseteq A$. Since αJ and αL are therefore integral ideals in A, there are prime ideals $P_1, \ldots, P_m$ and $Q_1, \ldots, Q_n$ such that $\alpha J = P_1 \cdots P_m$ and $\alpha L = Q_1 \cdots Q_n$. The containment $\alpha J \subseteq \alpha L$ and the proof of Proposition 24, show that (after rearranging the P_i) $Q_1 = P_1$. Thus, we multiply by P_i^{-1} and get $\alpha J' \subseteq \alpha L' = Q_2 \cdots Q_n \subseteq A$. Continuing this process, we see that

$$\alpha J = P_1 \cdots P_m = Q_1 \cdots Q_n P_{n+1} \cdots P_m = \alpha L P_{n+1} \cdots P_m$$

which implies that $J = L \cdot I$ where $I = P_{n+1} \cdots P_m$. □

The rest of the theorem now follows. We notice that $I \subseteq J$ if and only if $\mathrm{ord}_P(I) \geq \mathrm{ord}_P(J)$ for all prime ideals P. □

Definition. The set $\mathbf{P}$ of principal fractional ideals $\mathbf{P} = \{\alpha A : \alpha \in k^\times\}$ is a subgroup of the group $\mathbf{I}$ of all fractional ideals, since $(\alpha A)(\beta A) = (\alpha\beta)A$ and $(\alpha A)^{-1} = \alpha^{-1}A$. We define the *ideal class group* of A (or k) as the quotient $C = \mathbf{I}/\mathbf{P}$.

Proposition 29. *If k is a number field with ring of integers A, and Ideal and C are as above, then we have a long exact sequence*

$$1 \to A^\times \xrightarrow{\iota} k^\times \xrightarrow{\epsilon} \mathbf{I} \xrightarrow{\rho} C \to 1$$

where ι is the natural inclusion, ρ is the natural projection and ϵ is given by $\alpha \mapsto \alpha A$.

Proof. It is straightforward to check exactness at each point, except maybe at $k^\times$. An element $\alpha \in k^\times$ is in $\ker(\epsilon)$ if and only if $\alpha A = A$. This occurs if and only if α and α^{-1} are in A, since $1 \in A$, and this occurs if and only if $\alpha \in A^\times$. $\square$

We note, for the people who know some K-theory, that this comes from the long exact sequence in K-theory.

$$\begin{tikzcd} K_1(A) \arrow[r] \arrow[d, equal] & K_1(k) \arrow[r] \arrow[d, equal] & \oplus_P \overbrace{K_0(A/P)}^{=\mathbb{Z}} \arrow[r] \arrow[d, equal] & K_0(A) \arrow[r] \arrow[d, equal] & K_0(k) \arrow[r] \arrow[d, equal] & 0 \\ A^\times \arrow[r] & k^\times \arrow[r] & \mathbf{I} \arrow[r] & \mathbb{Z}+C \arrow[r] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

which continues to the left as

$$\begin{tikzcd} K_2(A) \arrow[r] & K_2(k) \arrow[r, "\beta"] \arrow[d, equal] & \oplus_P K_1(A/P) \arrow[r] \arrow[d, equal] & {} \\ & (k^\times \otimes k^\times)/S \arrow[r] & \oplus_P (A/P)^\times \arrow[r] & {} \end{tikzcd}$$

where S is the subgroup generated by the Steinberg relations and β is the tame symbol.

Theorem 30. *If k is a number field with ring of integers A, and $\mathbf{I}$ and C are as above, then C is finite and $A^\times$ is finitely generated.*

Example. It is a very special property of number fields that C is finite and $A^\times$ is finitely generated. We give an example to show that this is not true in general. Let $\Lambda \subset \mathbb{C}$ be a lattice, that is, a discrete, co-compact, additive subgroup. Fix nonzero complex numbers w_1, w_2 such that $w_1/w_2 \notin \mathbb{R}$ and $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Let $E = \mathbb{C}/\Lambda$ and let A denote the ring of meromorphic functions $E \to \mathbb{P}^1(\mathbb{C})$ whose only poles lie in Λ. Then

$$A = H^0(E \smallsetminus \{0\}, \mathcal{O}_E) = \mathbb{C}[p, p']/((p')^2 = 4p^3 - g_2 p - g_3)$$

For any $z \in E \smallsetminus \{0\}$, let

$$P_z = \{f \in A : f(z) = 0\} \subset A.$$

Each P_z is a maximal ideal in A with $A/P_z \overset{\cong}{\to} \mathbb{C}$ given by $f \mapsto f(z)$. When is $\prod_z P_z^{m(z)}$ principal, given by gA? If $g : E \to \mathbb{P}^1(\mathbb{C})$ has a pole at 0 and zeroes of order $m(z)$ at $z \in E \smallsetminus \{0\}$, then the divisor of g is

$$\operatorname{div}(g) = \sum_{z \in E \smallsetminus 0} m(z)z - \sum_{z \in E \smallsetminus 0} m(z)(0).$$

Abel's Theorem says that $\operatorname{div}(g) = \sum_{P \in E} m_P P$ satisfies the relations

$$\sum_P m_P = 0 \qquad \text{and} \qquad \sum_z m_z z \equiv 0 \pmod{\Lambda}.$$

Thus, $\prod_z P_z^{m(z)} = gA$ if and only if $\sum_z m_z z \in \Lambda$. The exact sequence from Proposition 29 is then

$$1 \to \mathbb{C}^\times \to \mathbb{C}(p, p') \to \bigoplus_{z \in E \smallsetminus 0} \mathbb{Z} \to E \to 0$$

$\mathbb{C}^\times = A^\times$ is not finitely generated and $E = C$ is not finite.

Proof of Theorem 30. The fact that $A^\times$ is finitely generated is the Unit Theorem, which we shall prove in Lecture 8. For now we prove that the ideal class group is finite.

The norm which we defined on integral ideals $\mathbb{N}(I) = (A : I)$ extends to the set of all fractional ideals in a well-defined manner. If I is a fractional ideal with prime factorization $I = \prod_i P_i^{a_i}$, then we define $\mathbb{N}(I) = \prod \mathbb{N}(P_i)^{a_i}$. This agrees with the original definition for integral ideals, by a composition series argument as in the proof of Proposition 24. Furthermore, we note that since A/P_i is a finite field, say with $q_i = p_i^{b_i}$ elements, $\mathbb{N}(P_i) = (A : P_i) = q_i$. As we observed previously, the norm of an element of k^* is not necessarily the same as the norm of the principal ideal it generates. However, $\mathbb{N}(\alpha A) = |\mathbb{N}(\alpha)|$. For an integral ideal I, we compute the discriminant, as a lattice: $\operatorname{disc}(\alpha A) = \operatorname{disc}(A)(\mathbb{N}(\alpha A))^2$. Finally, it is clear that the norm map, as defined, extends to a homomorphism of abelian groups $\mathbb{N} : \mathbf{I} \to \mathbb{Q}_+^\times$. Our result will follow from the following theorem.

Theorem 31. *Every ideal class $c \in C$ is represented by an integral ideal I such that $\mathbb{N}(I) \leq e(k)$ where*

$$e(k) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |d|^{1/2}$$

and $d = disc(A)$.

Before we prove Theorem 31, we see that it implies Theorem 30, as follows. The cardinality of C is at most the cardinality of the set of integral ideals I such that $(A : I) = \mathbb{N}(I) \leq e(k)$. In turn, this is at most the cardinality of the set of lattices in $A \cong \mathbb{Z}^n$ of index at most $e(k)$. By the theory of finitely generated abelian groups, this cardinality is finite, so C is finite. ☐

Proof of Theorem 31. Let J be a fractional ideal in the class c, and consider the lattice J^{-1}. By Theorem 17, there exists a nonzero element α of the lattice J^{-1} such that

$$|\mathbb{N}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\operatorname{disc}(J^{-1})|^{1/2} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} \frac{|d|^{1/2}}{\mathbb{N}(J)}$$

Since $\alpha \in J^{-1}$, $\alpha A \subseteq J^{-1}$ and $I = \alpha J \subseteq A$. Thus, I and J are in the same class of C, since they differ by the principal fractional ideal αA. And

$$\mathbb{N}(I) = |\mathbb{N}(\alpha)| \cdot \mathbb{N}(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} \frac{|d|^{1/2}}{\mathbb{N}(J)} \cdot \mathbb{N}(J) = e(k)$$

as desired. ☐

Definition. The *class number* of a number field k is denoted $h = h(k)$ and is defined to be the cardinality of the ideal class group C of k.

Example. If $n = 1$ (so that $k = \mathbb{Q}$) then $r_1 + 2r_2 = n = 1 \Rightarrow r_2 = 0$ and $|d| = 1$ so that $e(k) = 1$. Since every element of C is represented by an integral ideal of norm at most 1, it follows that $C = (1)$.

If $n = 2$ then k is a quadratic extension. If $d < 0$ then $D < 0$ so that k is not a real field. That is, $r_2 = 1$. Then $e(k) = \frac{2}{\pi}|d|^{1/2}$ which is strictly less than 2 for the allowable discriminants $d = -3, -4, -7, -8$. In this case, $C = (1)$ again, and this implies that every fractional ideal is principal. In particular, each such $A = \mathbb{Z} + \mathbb{Z}(\frac{d+\sqrt{d}}{2})$ is a principal ideal domain. If $d > 0$, then $r_2 = 0$ and $e(k) < 2$ for $d = 5, 8, 12, 13$, and the rings of integers in these cases are also principal ideal domains.

If $e(k) < 3$, then every nontrivial class in C is represented by an integral ideal I such that $\mathbb{N}(I) = 2$. Since this index is prime, there are no lattices strictly between I and A. In particular, $I = P$ is prime and A/P is the field of two elements. When $n = 2$ and $d < 0$ we see that $2 \le e(k) < 3$ when $d = -11, -15, -19, -20$. In these cases

$$A = \mathbb{Z} + \mathbb{Z}\Big(\frac{d+\sqrt{d}}{2}\Big) = \mathbb{Z}[x]/(x^2 - dx + \tfrac{d^2-d}{4})$$

We wish to know when, under these assumptions, there is a prime ideal P with $\mathbb{N}(P) = 2$. This occurs if and only if there is a surjection $A \to \mathbb{Z}/2\mathbb{Z}$. To find such a surjection, it is equivalent to find a solution of the congruence $x^2 - dx + \frac{d^2-d}{4} \equiv 0 \pmod 2$, so that we know where to send x, since the image of $\mathbb{Z}$ is already determined. Furthermore, the number of distinct solutions (mod 2) is exactly the number of such maps, and therefore the number of such prime ideals. We check this by cases.

(a) If $d \equiv 0 \pmod 4$, then the congruence is $x^2 + \frac{d}{4} \equiv 0 \pmod 2$, which has exactly one solution. Otherwise, $d \equiv 1 \pmod 4$.
(b) If $d \equiv 1 \pmod 8$, then the congruence is $x^2 - x \equiv 0 \pmod 2$, which has exactly two solutions.
(c) If $d \equiv 5 \pmod 8$, then the congruence is $x^2 - x + 1 \equiv 0 \pmod 2$, which has no solutions.

We correlate this with our possibilities for d.

(a) If $d = -20$, then there is exactly one prime ideal with norm 2.
(b) If $d = -15$, then there are exactly two prime ideals with norm 2.
(c) If $d = -11, -19$, then there are no prime ideals with norm 2.

Thus, for $d = -3, -4, -7, -8, -11, -19$ the class number is $h = 1$. For the cases $d = -20, -15$, we have more work to do.

For $d = -20$, $h = 2$. The generator of the class group in this case is a prime P of norm 2. In this case, $A = \mathbb{Z} + \mathbb{Z}(\sqrt{-5})$ and it follows that P is not principal. If P were principal, say $P = (a + b\sqrt{-5})A$, then $2 = \mathbb{N}(P) = a^2 + 5b^2$ which is impossible since a and b are integers. Since C has order 2, the class of P has order 2, so that P^2 is principal. The congruence we solve to find P in this case is $x^2 - 5 \equiv x^2 + 1 \equiv 0 \pmod 2$. It follows that $x \mapsto \overline{1} \in \mathbb{Z}/2\mathbb{Z}$ and the kernel is $P = \langle 2, x-1 \rangle$. It is straightforward to verify that $P^2 = 2A$ which has index 4 in A since $\mathbb{N}(2) = 4$.

For $d = -15$, we know that $h \le 3$. In this case $A = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$, and the prime ideals of index 2 are $P = \langle 2, x \rangle$ and $P' = \langle 2, x-1 \rangle$. Every class in C is represented by A, P or P', and the same check of norms as above shows that neither prime ideal is principal. Thus, $h = 2$ or 3. Even though we have two distinct prime ideals of index 2 in A, it turns out that they represent the same nontrivial class in C and $h = 2$. Let $\alpha = 2$, $\beta = \frac{1+\sqrt{-15}}{2}$ and $\gamma = \frac{1-\sqrt{-15}}{2}$ in A. Each element has norm 4, and the ideals generated by these elements are all distinct, since none of the pairwise quotients are in A. It ends up that

$$PP' = \alpha A \qquad P^2 = \beta A \qquad (P')^2 = \gamma A$$

so that in the class group $[P][P'] = [P][P]$ which implies that $[P'] = [P]$. Another way to see the fact that C has order 2 is to observe that if it had order 3, then each nontrivial element would have order 3, which does not hold in this case.

We should observe that for quadratic fields with negative discriminants, it has been proven that the only examples with trivial class group are those with

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

However, for positive discriminant the list seems infinite. Whether or not the list is actually infinite is still an open question.

The case $d = -163$ is particularly interesting. If $\alpha = \frac{1+\sqrt{-163}}{2}$, then $A = \mathbb{Z} + \mathbb{Z}\alpha$. The minimal polynomial of α is $f_\alpha(x) = x^2 + x + 41$. The interesting fact here is that the values $f_\alpha(0), f_\alpha(1), \ldots, f_\alpha(40)$ are all prime numbers. Of course, $f(41) = 41(41+1+1)$ is not prime, but people considered functions of this type when trying to find prime-generating functions.

Definition. We are interested in finding the prime ideals of an order B. We define the *characteristic* of a prime ideal P to be the characteristic of its residue field B/P.

Lecture 6

Let k be a number field with ring of integers A, and let B be any order in k. The prime ideals P of B with characteristic p are exactly the maximal ideals containing pB, as $\mathrm{char}(P) = p$ if and only if, under the natural projection $B \to B/P$, the number $p \mapsto 0$, which occurs if and only if $p \in P$ or equivalently that $pB \subseteq P$.

Since the elements which occur in the Jordan-Hölder series for $pB \subset B$ are exactly the prime ideals which contain pB, the above remarks show that the prime ideals in B of characteristic p are exactly the primes which occur in the product $P_1 \cdots P_t \subseteq pB$ from Proposition 24. In particular, there are only finitely many primes in B having a prescribed characteristic. Let $P_1, \cdots, P_u$ be the prime ideals of characteristic p. Then there are positive integers $e_1, \ldots, e_u$ such that $P_1^{e_1} \cdots P_u^{e_u} \subseteq pB$. ($e_i$ is the multiplicity with which P_i occurs as a Jordan-Hölder factor in B/pB.) Since each P_i has characteristic p, the field B/P_i has order p^{f_i} for some positive integer f_i. Since B is a lattice of rank n, pB has index p^n in B, so

$$p^n = (B : pB) = \prod_{i=1}^{u} \mathbb{N}(P_i)^{e_i} = \prod_{i=1}^{u} (p^{f_i})^{e_i} = p^{(\sum_i e_i f_i)}$$

from which it follows that $n = \sum_{i=1}^{u} f_i e_i \geq u$. That is, there are at most n prime ideals of characteristic p in B.

We consider these ideas in the simplest of cases. Assume that α is an algebraic integer with minimal polynomial $f(x)$ of degree n. Then $B = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \cdots + \mathbb{Z}\alpha^{n-1}$ is an order in $k = \mathbb{Q}(\alpha)$. For example, if $n = 2$, then every order B is of this form with $\alpha = \frac{d_B + \sqrt{d_B}}{2}$ where $d_B = \mathrm{disc}(B)$. Then $B \cong \mathbb{Z}[x]/(f(x))$ and

$$B/pB = \mathbb{Z}[x]/(p, f(x)) = (\mathbb{Z}/p\mathbb{Z}[k])/(\tilde{f}(x)) = \prod_i (\mathbb{Z}/p\mathbb{Z}[k])/(g_i(x)^{e_i})$$

where $\tilde{f}(x)$ is the reduction of $f(x)$ modulo p and $\tilde{f}(x) = \prod_i g_i(x)^{e_i}$ is the prime factorization of $\tilde{f}(x)$. It follows that the set of maximal ideals P_i of characteristic p with multiplicity e_i in the Jordan-Hölder decomposition are exactly the ideals $\langle p, \hat{g}_i(x) \rangle$ where $\hat{g}_i(x) \in \mathbb{Z}[x]$ is a lift of $g_i(x)$, and that under this correspondence (with the previous notation) $f_i = \deg(g_i(x))$. Thus, we have all the machinery to prove the following.

Corollary 32. *If $k = \mathbb{Q}(\alpha)$ where α is an algebraic integer, and p is a prime whose square does not divide disc$(\alpha) =$ disc$(\mathbb{Z}[\alpha]) \in \mathbb{Z} \smallsetminus \{0\}$, then $pA = \prod P_i^{e_i}$ mirrors the factorization of $f_\alpha(x)$ modulo p. More precisely, if $\deg(P_i) = f_i$ where $\#(A/P_i) = p^{f_i}$, then $\deg(P_i) = \deg(\hat{g}_i(x))$ and the number of times that P_i occurs as a factor in the Jordan-Hölder series for A/pA is exactly e_i, the multiplicity of the factor $g_i(x)$ in $\tilde{f}(x)$. Moreover, if p does not divide disc(α), then all the $e_i = 1$.*

Definition. In this notation, we call e_i the *ramification index* of P_i over p, and we call f_i the *residue degree.* If $e_i \geq 2$, then we say that P_i is *ramified* over p.

Proof. We claim that the index N of $\mathbb{Z}[\alpha]$ in A is prime to p. The formula $N^2\mathrm{disc}(A) = \mathrm{disc}(\mathbb{Z}[\alpha]) = \mathrm{disc}(\alpha)$ shows that if p divides N then p^2 divides $\mathrm{disc}(\alpha)$, a contradiction. Fixing integers r, s such that $1 = pr + Ns$, it is straightforward to check that the map $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to A/pA$ is an isomorphism. The previous discussion and the results on prime factorization in A imply the result. $\square$

Example. Assume that k is a cubic extension of $\mathbb{Q}$ with ring of integers A such that $2A$ is a product of three distinct primes $2A = P_1P_2P_3$. For any $\alpha \in A \smallsetminus \mathbb{Z}$, $k = \mathbb{Q}(\alpha)$ since the degree is prime. However, $\mathbb{Z}[\alpha] \subsetneq A$, because if they were equal, then the factorization of $f_\alpha(x)$ with coefficients reduced modulo 2 would have three distinct linear factors. This is a contradiction since there are only two distinct linear polynomials in $\mathbb{Z}/2\mathbb{Z}[x]$. An example where this occurs is when k is the unique cubic extension of $\mathbb{Q}$ contained in the cyclotomic field $\mathbb{Q}(\zeta_{31})$, where ζ_{31} is a primitive 31st root of unity. The essential reason why $2A$ factors as claimed is in the congruence $2 \equiv 7^3 \pmod{31}$. We shall discuss this example in more detail in the future.

Next, we want to investigate the relation between $d = d_A = \mathrm{disc}(A)$ and the e_i. We recall that the dual lattice of A is defined to be $A^* = \{\beta \in k : \mathrm{Tr}\,(\beta A) \subseteq \mathbb{Z}\}$. By Proposition 1, $|d|$ is the index $(A^* : A)$.

Definition. We define the *different* of A to be the integral ideal $\mathcal{D} = (A^*)^{-1} \subseteq A^{-1} = A$. By Lemma 2, $\mathbb{N}(\mathcal{D}) = (A : \mathcal{D}) = |d|$. We adopt the following notation. Let P have characteristic p and let e_P denote the number of times P occurs as a factor in the Jordan-Hölder series for A/pA.

Proposition 33. *$\mathcal{D} = \prod_P P^{m_P}$ for nonnegative integers m_P, and $m_P \geq e_P - 1$ with equality if and only if char$(P) \nmid e_P$.*

Definition. If $m_P > e_P - 1$, then we say that P is *wildly ramified.* Otherwise, we say that P is *tamely ramified.*

Before we prove the proposition, we list some consequences.

Corollary 34. *If k is quadratic, then the only primes p which have a ramified factor P in A are the primes dividing d.*

Proof. We assume that $k = \mathbb{Q}(\sqrt{D})$ where D is square-free, and recall from Theorem 11 that $d \equiv 0, 1 \pmod 4$ is as square-free as possible. Also, if $d \equiv 1 \pmod 4$ then $d = D = \pm \prod_{\mathrm{odd}} p_i$, and if $d \equiv 0 \pmod 4$ then $d = 4D = \pm 2^a \prod_{\mathrm{odd}} p_i$ where a is 2 or 3. If $\eta = \frac{d+\sqrt{d}}{2}$, then $A = \mathbb{Z} + \mathbb{Z}\eta$.

We claim that $\mathcal{D} = \sqrt{d}A \subset A$ and that the index is $\mathbb{N}(\mathcal{D}) = (A : \mathcal{D}) = |d|$. The first claim follows from the fact that $A^* = \frac{1}{\sqrt{d}}A$, which the interested reader is invited to check. The second claim follows from Proposition 1, since $\mathbb{N}(\mathcal{D}) = (\mathcal{D} : A) = (A^* : A) = |d|$.

As before, $pA = \prod_i P_1^{e_i}$ where $\sum_i e_i f_i = n = 2$. Then P is a ramified factor of p if and only if $P = P_1$ and $e_1 = 2$. This implies that $m_P \geq e_P - 1 = 1$ so that P occurs in the factorization of $\mathcal{D}$. Thus, $d = \mathbb{N}(\mathcal{D})$ is divisible by $\mathbb{N}(P)$, which is a power of p. $\square$

By the proof, if k is quadratic, then $\mathcal{D}$ is principal so that its class in the class group C is zero. In general, this is not the case. However, we have the following theorem, which we shall not prove (c.f. André Weil *Basic Number Theory*, Theorem XIII.12.13).

Theorem. If k is a number field, then the class of the different $\mathcal{D}$ in the class group C is contained in $2C$.

We shall use the following proposition to prove Proposition 33.

Proposition 35. *Let B be an order in a number field with dual module B^*, p a prime number, and P_i the Jordan-Hölder factors of pA with multiplicities e_i. Then $\cap_i P_i \subseteq pB^*$, and $\cap_{i \neq i_0} P_i \subseteq pB^*$ if and only if $p | e_{i_0}$.*

Proof. Let $I = \cap_i P_i$. We have the following chain of equivalences: $I \subseteq pB^*$ iff $\frac{1}{p}I \subseteq B^*$ iff $\mathrm{Tr}\,(\frac{1}{p}I) \subseteq \mathbb{Z}$ iff $\mathrm{Tr}\,(I) \subseteq p\mathbb{Z}$ iff for every $\alpha \in I$, $\mathrm{Tr}\,(\alpha) \equiv 0 \pmod p$ iff for every $\alpha \in I$, the multiplication map $\tilde{\alpha} : B/pB \to B/pB$ has trace zero. The map $\tilde{\alpha}$ is a linear endomorphism of the n-dimensional vector space B/pB over $\mathbb{Z}/p\mathbb{Z}$. Using the Jordan-Hölder decomposition of B/pB, we can write a matrix for $\tilde{\alpha}$ consisting of diagonal blocks each of which gives the action on the corresponding B/P_i. Thus,

$$\mathrm{Tr}\,(\tilde{\alpha} : B/pB \to B/pB) = \sum_i e_i \mathrm{Tr}\,(\tilde{\alpha}_i : B/P_i \to B/P_i)$$

and $I \subseteq pB^*$ iff the sum $\sum_i e_i \mathrm{Tr}\,(\tilde{\alpha}_i : B/P_i \to B/P_i) = 0$. Thus, if $\alpha \in I$ then each $\tilde{\alpha}_i = 0$ so that $\mathrm{Tr}\,(\tilde{\alpha}_i) \equiv 0$ and $I \subseteq pB^*$.

Let $I_0 = \cap_{i \neq i_0} P_i$ and fix $\alpha \in I_0$. If $\alpha \in I$, then each $\mathrm{Tr}\,(\tilde{\alpha}_i) \equiv 0$, so assume that $\alpha \notin I$. Then every such α is in pB^* iff the i_0 term in the sum $\sum_i e_i \mathrm{Tr}\,(\tilde{\alpha}_i)$ is zero. It suffices to show that there is some such α with $\mathrm{Tr}\,(\tilde{\alpha}_{i_0}) \not\equiv 0$ so that the previous condition is equivalent to $e_i \equiv 0 \pmod p$, as desired.

For $i \neq i_0$, $P_i + P_{i_0} = B$ by maximality, so the Chinese Remainder Theorem implies that $I_0 + P_{i_0} = B$. It follows that the projection map $I_0 \to B/P_{i_0}$ is surjective, and it suffices to find an element $\beta \in B/P_{i_0}$ such that $\mathrm{Tr}\,(\beta : B/P_{i_0} \to B/P_{i_0}) \not\equiv 0$. Since B/P_{i_0} is a field, we just choose β to be a primitive element over $\mathbb{Z}/p\mathbb{Z}$ so that the corresponding trace is 1. $\square$

Proof of Proposition 33. Let $B = A$ in Proposition 35 so that $pA = \prod_i P_i^{e_i}$. Then since the P_i are maximal, $\cap_i P_i = \prod_i P_i \subseteq pA^* = \prod_i P_i^{e_i}\mathcal{D}^{-1}$. This implies that $\mathcal{D} \subseteq \prod_i P_i^{e_i - 1}$ with equality if and only if no e_i is divisible by p. $\square$

Example. We consider the factorization of the ideals pA in a quadratic field k. In particular, we prove the converse of Corollary 34. If $\alpha = \frac{d+\sqrt{d}}{2}$, then the minimal polynomial of α is $f_\alpha(x) = x^2 - dx + \frac{d^2-d}{4}$ and the ring of integers of k is $A = \mathbb{Z} + \mathbb{Z}\alpha$. We apply Corollary 32 in two cases.

Case 1: $p = 2$. If $d \equiv 0 \pmod 4$, then $f_\alpha(x)$ reduces to $x^2 - \frac{d}{4}$ which factors to x^2 or $(x+1)^2$ depending on whether $\frac{d}{4}$ is even or odd. Thus, $2A = P^2$. Also, $\mathrm{ord}_2(\mathcal{D}) = 2$ or 3 since this is the exponent for the power of 2 dividing $d = (A : \mathcal{D})$. If $d \equiv 1 \pmod 4$, then the reduction of $f_\alpha(x)$ modulo 2 is

$$\tilde{f}_\alpha(x) = \begin{cases} x^2 - x & \text{if } d \equiv 1 \pmod 8, \\ x^2 - x + 1 & \text{if } d \equiv 5 \pmod 8) \end{cases}$$

If $d \equiv 1 \pmod 8$, then $\tilde{f}_\alpha(x)$ has two distinct factors and $2A = P_1P_2$ is a product of distinct primes. (In this case, we say that p is *split*.) If $d \equiv 5 \pmod 8$, then $\tilde{f}_\alpha(x)$ is irreducible and $2A$ is prime. (In this case we say that p is inert.) Notice that since $2 \nmid d$, $\mathrm{ord}_2(\mathcal{D}) = 0$.

Case 2: $p > 2$. If $p|d$, then modulo p, $\tilde{f}_\alpha(x) = x^2$ so that $pA = P^2$ and $\mathrm{ord}_p(\mathcal{D}) = 1$ since d is as square-free as possible. If $p \nmid d$, then we notice that in $\mathbb{Z}/p\mathbb{Z}$ the roots of $\tilde{f}_\alpha(x)$ are $\frac{d \pm \sqrt{d}}{2}$, which makes sense if d is a square modulo p, since 2 is a unit in $\mathbb{F}_p$. Thus, if d is a square modulo p, then since $d \not\equiv 0$ and $p > 2$ we see that the zeros of $\tilde{f}_\alpha(x)$ are distinct and so p splits: $pA = P_1P_2$. If d is not a square modulo p, then $\tilde{f}_\alpha(x)$ is irreducible and p is inert: $pA = P$.

We should note that we can use the Legendre symbol $(\frac{d}{p})$ to summarize. Recall that if p is a prime which does not divide an integer a, then

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p, \\ -1 & \text{if } a \text{ is a square modulo } p \end{cases}$$

Thus, for any prime p

$$pA = \begin{cases} P^2 & \text{if } p|d, \\ P_1P_2 & \text{if } p = 2 \text{ and } d \equiv 1 \pmod 8, \text{ or if } p > 2 \text{ and } (\frac{d}{p}) = 1, \\ P & \text{if } p = 2 \text{ and } d \equiv 5 \pmod 8, \text{ or if } p > 2 \text{ and } (\frac{d}{p}) = -1, \end{cases}$$

The basic properties of the Legendre symbol may be found in almost any basic text on number theory. Probably the most fundamental result is the Law of Quadratic Reciprocity.

Theorem. (Gauss) If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

from which it follows that

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -(\frac{q}{p}) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Furthermore,

$$\left(\frac{2}{p}\right) = (-1)^{(\frac{p^2-1}{8})}$$

It is unexpected but true that all cases of quadratic reciprocity are roughly equivalent to the fact that the factorization of p in A depends only on the residue class of p modulo d.

For example, if ℓ is an odd prime such that $\ell \equiv 1 \pmod 4$ and $k = \mathbb{Q}(\sqrt{\ell})$, then the discriminant is $d = \ell$ and we have the following factorizations:

$$2A = \begin{cases} P_1 P_2 & \text{if } \ell \equiv 1 \pmod 8 \text{ iff } (\frac{2}{\ell}) = 1 \text{ by quadratic reciprocity} \\ P & \text{if } \ell \equiv 5 \pmod 8 \text{ iff } (\frac{2}{\ell}) = -1 \text{ by quadratic reciprocity} \end{cases}$$

and if p is an odd prime distinct from ℓ

$$pA = \begin{cases} P_1 P_2 & \text{if } (\frac{\ell}{p}) = 1 \text{ iff } (\frac{p}{\ell}) = 1 \text{ by quadratic reciprocity} \\ P & \text{if } (\frac{\ell}{p}) = -1 \text{ iff } (\frac{p}{\ell}) = -1 \text{ by quadratic reciprocity} \end{cases}$$

which shows that the factorization of pA (whether pA is split or inert) depends only on p modulo $\ell = d$.

If ℓ is an odd prime such that $\ell \equiv 3 \pmod 4$ and $k = \mathbb{Q}(\sqrt{-\ell})$, then the discriminant is $d = -\ell \equiv 1 \pmod 4$ and we have the following factorizations:

$$pA = \begin{cases} P_1 P_2 & \text{if } (\frac{-\ell}{p}) = 1 = (\frac{p}{\ell}) \\ P & \text{if } (\frac{-\ell}{p}) = -1 = (\frac{p}{\ell}) \end{cases}$$

which is the same behavior as the previous example.

Assume that $d = -4$, so that $k = \mathbb{Q}(i)$ and $A = \mathbb{Z}[i]$. Then for an odd prime p, pA is split iff $p \equiv 1 \pmod 4$ and is inert iff $p \equiv 3 \pmod 4$. The ideal $2A$ is ramified and $\mathcal{D} = 2A = P^2$.

In fact, for any quadratic field k, there exists a group homomorphism $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ such that pA splits iff $\chi(p) = 1$, and pA is inert iff $\chi(p) = -1$. In the cases $\mathbb{Q}(\sqrt{\pm\ell})$ above, we see that $\chi(p) = (\frac{p}{\ell}) : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \{\pm 1\}$. χ is necessarily unique, by the given property.

For any number field k, let T denote the set of nonzero prime ideals of A. Let U denote the prime numbers, and consider the following function of s:

$$\prod_{P \in T} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \prod_{p \in U} \underbrace{\left(\prod_{P \supseteq pA} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1}\right)}_{\text{at most } n \text{ factors}}$$

For example, if $n = 1$ so that $k = \mathbb{Q}$ and $A = \mathbb{Z}$, then this function is

$$\prod_{p \in U} \left(1 - \frac{1}{p^s}\right)^{-1}$$

If $n = 2$, then there are three options for the factor corresponding to the prime number p:

$$
\begin{aligned}
pA &= P^2 && \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1} && (4)\\
pA &= P && \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \left(1 - \frac{1}{p^{2s}}\right)^{-1} \\
&&& \qquad\qquad\qquad = \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 + \frac{1}{p^s}\right)^{-1} \\
&&& \qquad\qquad\qquad = \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \\
pA &= P_1P_2 && \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{1}{p^s}\right)^{-1} \\
&&& \qquad\qquad\qquad = \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}
\end{aligned}
$$

Thus, in each unramified case, the factor corresponding to p is

$$\left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Example. We consider the factorization of the ideals pA in a cyclotomic field. Let ℓ be an odd prime number, $\zeta = \zeta_\ell$ a primitive ℓth root of unity, and $k = \mathbb{Q}(\zeta)$. Let $\phi(x) = x^{\ell-1} + x^{\ell-2} + \cdots + 1$ so that ζ satisfies the polynomial $x^\ell - 1 = (x-1)\phi(x)$. We claim that $\phi(x)$ is irreducible over $\mathbb{Q}$. To see this, let $\pi = \zeta - 1$, which satisfies the polynomial

$$\phi(1+y) = \frac{(1+y)^\ell - 1}{(1+y) - 1} = \frac{y^\ell + \binom{\ell}{1}y^{\ell-1} + \cdots + \ell y + 1 - 1}{y} = y^{\ell-1} + \binom{\ell}{1}y^{\ell-2} + \cdots + \ell$$

This polynomial is monic, ℓ divides all the non-leading coefficients and ℓ^2 does not divide the constant term. Therefore, by Eisenstein's criterion, $\phi(1+y)$ is irreducible over $\mathbb{Q}$, and the same is true for $\phi(x)$. Since $\phi(1+y)$ is the minimal polynomial of π and ℓ is odd, $\mathbb{N}(\pi) = \ell$ the constant term of $\phi(1+y)$. Similarly, $\mathbb{N}(\zeta) = 1$.

We note, for historical interest, that Kummer studied cyclotomic fields extensively. He discovered that the ring of integers in this case is not a principal ideal domain (although, not in those terms) and developed the theory of ideals as a result.

Lecture 7

We continue with the notation from the previous lecture. Let $\sigma_1, \ldots, \sigma_{\ell-1}$ be the distinct $\mathbb{Q}$-embeddings of k into $\mathbb{C}$. If we assume that $\zeta \in \mathbb{C}$, then we may assume that $\sigma_i(\zeta) = \zeta^i$. Since $\ell = \mathbb{N}(\pi) = \prod_{i=1}^{\ell-1}\sigma_i(\pi) = \pi(\zeta^2 - 1)\cdots(\zeta^{\ell-1} - 1)$, we see that π divides ℓ in A. In particular, $\ell A \subseteq \pi A \subseteq A$.

Proposition 36. *The ring of integers in k is $A = \mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$.*

Proof. The second equality is clear. Let $B = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{\ell-2}$. Then $d_B = \operatorname{disc}(B) = \det(\sigma_i(\zeta^j))^2$ as we noted in the proof of Proposition 10. This is exactly

$$d_B = \det \begin{pmatrix} 1 & \zeta & \zeta^2 & \cdots & \zeta^{\ell-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(\ell-1)} \\ 1 & \zeta^3 & \zeta^6 & \cdots & \zeta^{3(\ell-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{\ell-1} & \zeta^{2(\ell-1)} & \cdots & \zeta^{(\ell-1)(\ell-1)} \end{pmatrix}^2 = \prod_{i<j}(\zeta^i - \zeta^j)^2$$

since this is the Vandermonde determinant. Using the fact that $\zeta^i - \zeta^j = \zeta^i(1 - \zeta^{j-i}) = -\sigma_i(\zeta)\sigma_{j-i}(\pi)$ and some bookkeeping, we see that

$$d_B = \prod_{i<j}(\zeta^i - \zeta^j)^2 = \pm(\mathbb{N}(\zeta))^{\ell-2}(\mathbb{N}(\pi))^{\ell-2} = \pm\ell^{\ell-2}$$

Since $\ell > 2$ is prime, all the embeddings of k are complex. Thus, $r_2 = \frac{\ell-1}{2}$ and Corollary 15 implies that $d_B = (-1)^{(\frac{\ell-1}{2})}\ell^{\ell-2}$. By Proposition 1,

$$\ell^{\ell-2} = |d_B| = (B^* : B) = (B^* : A^*)(A^* : A)(A : B) \geq (A^* : A).$$

The following proposition will help us complete the proof.

Proposition 37. $\frac{\pi}{\ell}A \subseteq A^*$.

Before we prove Proposition 37, we complete the proof of Proposition 36. By Lemma 20, $(A : \pi A) = |\mathbb{N}(\pi)| = \ell$, and since A is a lattice of rank $\ell - 1$, $(A : \ell A) = \ell^{\ell-1}$. The inclusions $\ell A \subseteq \pi A \subseteq A$ imply that $(\pi A : \ell A) = \ell^{\ell-2}$. Dividing the inclusion $\ell A \subseteq \pi A$ by ℓ gives $A \subseteq \frac{\pi}{\ell}A \subseteq A^*$ so that

$$\ell^{\ell-2} \geq (A^* : A) \geq (\frac{\pi}{\ell}A : A) = (\pi A : \ell A) = \ell^{\ell-2}$$

which implies equality. It follows that $A = B$ and $A^* = \frac{\pi}{\ell}A$. $\square$

Proof of Proposition 37. It suffices to show that $\operatorname{Tr}(\frac{\pi}{\ell}A) \subseteq \mathbb{Z}$. This occurs if and only if $\operatorname{Tr}(\pi A) \subseteq \ell\mathbb{Z}$. For $\alpha \in A$,

$$\begin{aligned} \operatorname{Tr}(\pi\alpha) = \operatorname{Tr}((\zeta - 1)\alpha) &= \sum_{i=1}^{\ell-1}\sigma_i(\zeta - 1)\sigma_i(\alpha) \\ &= \sum_{i=1}^{\ell-1}(\zeta^i - 1)\sigma_i(\alpha) = \sum_{i=1}^{\ell-1}(\zeta - 1)(\zeta^{i-1} + \cdots + 1)\sigma_i(\alpha) \\ &\in \pi A \cap \mathbb{Z} \end{aligned}$$

so it suffices to show that $\pi A \cap \mathbb{Z} = \ell\mathbb{Z}$. Since $\pi A \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ and $\ell\mathbb{Z} \subseteq \pi A \cap \mathbb{Z}$ and $\ell\mathbb{Z}$ is maximal, either $\pi A \cap \mathbb{Z} = \mathbb{Z}$ or $\pi A \cap \mathbb{Z} = \ell\mathbb{Z}$. If $\pi A \cap \mathbb{Z} = \mathbb{Z}$ then π is a unit in A so that $\pi A = A$. But we have already seen that $(A : \pi A) = \ell > 2$, a contradiction. $\square$

It follows from the proof that $\mathcal{D} = (\frac{\ell}{\pi})A$.

We now return to the task of factoring the ideals pA. First, the ideal ℓA is completely ramified, in the sense that $\ell A = P^{\ell-1}$ where P has residue degree $f = 1$ and ramification index $e = \ell - 1 = n$, and $\mathbb{N}(P) = \ell$. Let $P = \pi A$, which is prime since $A/P = \mathbb{Z}[\pi]/(\pi) = \mathbb{F}_\ell$. Suppose that $\ell A = P^e \prod_i P_i^{e_i}$ with $e_i \geq 1$. Since $P \supseteq \ell A$, we know that $e \geq 1$. Furthermore, since P and each P_i has characteristic ℓ

$$\ell^{\ell-1} = \mathbb{N}(\ell) = \mathbb{N}(P^e \prod_i P_i^{e_i}) = \mathbb{N}(P)^e \prod_i \mathbb{N}(P_i)^{e_i} \geq \ell^{(e+\sum_i e_i)}$$

so that $e, e_i < \ell$. In particular, e and the e_i are not divisible by ℓ. By Proposition 33, we see that the factorization of $\mathcal{D}$ contains P^{e-1} and $P_i^{e_i-1}$ so that

$$P^{e-1} \prod_i P_i^{e_i} = \frac{\ell}{\pi} A = \mathcal{D} \subseteq P^{e-1} \prod_i P_i^{e_i-1}$$

so that each $e_i \geq e_i - 1$, a contradiction. Thus, $\ell A = P^e$ and $\ell^{\ell-1} = \mathbb{N}(\ell) = \mathbb{N}(P)^e = \ell^e$ so that $e = \ell - 1$, as claimed.

If $p \neq \ell$, then by our computation in Proposition 37, $|d| = \ell^{\ell-2}$ so that $p \nmid d$. By Corollary 32, the ideal pA completely splits as $pA = \prod_i P_i$ and the factorization of pA mirrors the factorization of $\phi(x)$ modulo p. When does $\phi(x)$ have a linear factor modulo p? This occurs iff there is an ℓth root of unity in $\mathbb{F}_p^\times$. Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, such an element exists iff $\mathbb{F}_p^\times$ contains a subgroup of order ℓ iff $\ell | p-1$ iff $p \equiv 1 \pmod{\ell}$. In this case, though, $\mathbb{F}_p^\times$ has $\ell - 1$ distinct elements of order ℓ and so $\phi(x)$ splits into distinct linear factors modulo p and $pA = P_1 \cdots P_{\ell-1}$.

In general, let f be the smallest integer such that $\ell | (p^f - 1)$, that is, f is the order of p in $\mathbb{F}_\ell^\times$. Then $pA = P_1 \cdots P_g$ for distinct P_i such that $\mathbb{N}(P_i) = p^f$ and $g = \frac{\ell-1}{f}$. The same reasoning as above shows that $\phi(x)$ splits completely over $\mathbb{F}_{p^f}$. Each zero of $\phi(x)$ in $\mathbb{F}_{p^f}$ has f distinct conjugates, and the coefficients of the factors of $\phi(x)$ modulo p will be the symmetric polynomials in these conjugates. It follows that, modulo p, $\phi(x)$ factors into g distinct factors, each of degree f.

Example. If $\ell = 3$, then $\zeta = \frac{-1+\sqrt{-3}}{2}$ so that $k = \mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. By our work above, we know that $3A = P^2$. If $p \equiv 1 \pmod 3$, then $pA = P_1 P_2$. If $p \equiv -1 \pmod 3$, then $f = 2$ and $g = 1$ so that $pA = P$.

Example. If $\ell = 5$, then $\mathbb{F}_5^\times \cong \mathbb{Z}/4\mathbb{Z}$. As before, $5A = P^4$. If $p \equiv 1 \pmod 5$, then pA splits completely as $pA = P_1 P_2 P_3 P_4$. If $p \equiv -1 \pmod 5$, then $f = 2$ and $g = 2$ so that $pA = P_1 P_2$. If $p \equiv 2, 3 \pmod 5$, then $f = 4$ and $g = 1$ so that $pA = P$.

We observe that a cyclotomic field k is always Galois over $\mathbb{Q}$. The extension is separable because $\mathrm{char}(\mathbb{Q}) = 0$, and it is normal since the conjugates of ζ are simply $\zeta^i \in k$. Furthermore, the Galois group $G = \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{F}_\ell)^\times$. The homomorphism $\psi : G \to (\mathbb{F}_\ell)^\times$ is given by $\sigma \mapsto a \pmod{\ell}$ where $\sigma(\zeta) = \zeta^a$. The map ψ is always an injection, and the irreducibility of $\phi(x)$ implies that ψ is also a surjection.

Back in the case $\ell = 5$, $G = \mathbb{Z}/4\mathbb{Z}$ has a unique subgroup of index 2. The Galois correspondence implies that there is a unique quadratic subfield L of k. If $\alpha = \zeta + \zeta^{-1}$, then $\mathbb{Q}(\alpha) \subsetneq k$ since α is real and $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha)$ since α is irrational. Thus, $\mathbb{Q}(\alpha)$ must be the unique quadratic subfield of k. It will follow from the following theorem that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

Theorem 38. *(Gauss) Assume that ℓ is a prime number, $\ell > 2$, and $\zeta = \zeta_\ell \in \mathbb{C}$ is a primitive ℓth root of unity. Let $k = \mathbb{Q}(\zeta)$. Then there is a unique quadratic subfield L of k, and $L = \mathbb{Q}(\sqrt{(-1)^{(\frac{\ell-1}{2})}\ell})$.*

Compare this to the theorem which states that every quadratic field is contained in a cyclotomic field (cf. Lang, *Algebra*, Theorem VI.3.3).

Proof. As we noted before, k is Galois over $\mathbb{Q}$ with Galois group $G = \mathbb{F}_\ell^\times = \mathbb{Z}/(\ell-1)\mathbb{Z}$. Since ℓ is odd, G has a unique subgroup of index 2, which implies that k has a unique quadratic subfield. Let

$$D = (-1)^{(\frac{\ell-1}{2})}\ell \qquad \text{and} \qquad g = \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right)\zeta^a$$

It is not difficult to show that $g^2 = D$ (cf. Lang, *Algebra*, Theorem VI.3.3). Thus, $L = \mathbb{Q}(g) = \mathbb{Q}(\sqrt{D})$ is the desired subfield. $\square$

Of course, the fields we have studied in depth thus far have all been Galois and cyclic over $\mathbb{Q}$. This has made our computations relatively easy. The following example involves an extension with Galois group S_3, and we omit proofs of many of the facts.

Example. Let $f(x) = x^3 - x - 1$ and $\alpha \in \mathbb{C}$ a zero of $f(x)$. Any rational zero of $f(x)$ would necessarily be ± 1, so $f(x)$ is irreducible. Let $k = \mathbb{Q}(\alpha)$ and let K be a splitting field of $f(x)$ over $\mathbb{Q}$. The discriminant of $f(x)$ is -23 and therefore not a square, so that k is not Galois over $\mathbb{Q}$ and the Galois group of $f(x)$ is $G = \mathrm{Gal}(K/\mathbb{Q}) = S_3$. The ring of algebraic integers in k is $A = \mathbb{Z}[\alpha]$ and $d = \mathrm{disc}(A) = -23$. Modulo 23, $f(x)$ factors as $(x-3)(x-10)^2$. Thus, by Corollary 32, $23A = P_1P_2^2$ where the residue degrees are $f_1 = f_2 = 1$. In fact, $P_2 = \mathcal{D}$ has index 23 in A. If $p \neq 23$ then there is no ramification. When $(\frac{p}{23}) = -1$, i.e. p is not a square modulo 23, $pA = P_1P_2$ where $f_1 = 1$ and $f_2 = 2$. When $(\frac{p}{23}) = 1$, either $pA = P_1P_2P_3$ with the $f_i = 1$ or $pA = P$ with $f = 3$. These different possibilities mirror the different quadratic forms $x^2 + xy + 6y^2$ and $2x^2 + xy + 3y^2$ with discriminant -23 as in Lecture 3: pA splits completely when $p = x^2 + xy + 6y^2$ for integers x, y, and pA is inert when $p = 2x^2 + xy + 3y^2$ for integers x, y.

We note that prime factorization is known explicitly in relatively few cases. For example, if k has degree 5 over $\mathbb{Q}$ and has nonsolvable Galois closure, then a simple recipe for prime factorization is not known.

Now, we are ready to build the machinery to finish the proof of Theorem 30. We state the result in more generality, as a separate theorem.

Theorem 39. *(Unit Theorem) Assume that k is a number field and that B is an order in k. Then the group of units $B^\times$ is a finitely generated abelian group. Furthermore, the torsion subgroup of $B^\times$ is cyclic of finite order, and the rank of $B^\times$ is $r = r_1 + r_2 - 1$. Finally, if $r_1 \neq 0$, then $B^\times_{tor} = \{\pm 1\}$.*

It should be noted that the torsion subgroup of $B^\times$ is exactly the set of roots of unity in B, since an element $\alpha \in B$ is torsion iff $\alpha^s = 1$ for some integer s.

Example. If $k = \mathbb{Q}$, then $r_1 = 1$ and $r_2 = 0$ so that $A^\times = \{\pm 1\}$, not that this is a surprise.

If $k = \mathbb{Q}(\sqrt{-D})$ for a positive, square-free integer D, then $r_1 = 0$ and $r_2 = 1$. Thus, $A^\times$ is torsion. If $D = 1$, then $A^\times$ is cyclic of order 4, generated by $\sqrt{-1}$. If $D = 3$, then $A^\times$ is cyclic of order 3, generated by $\frac{-1+\sqrt{-3}}{2}$. In all other cases, $A^\times = \{\pm 1\}$.

If $k = \mathbb{Q}(\sqrt{D})$ for a positive, square-free integer D, then $r_1 = 2$ and $r_2 = 0$. Thus, $A^\times$ has rank 1, and since $k \subset \mathbb{R}$, the torsion subgroup is $\{\pm 1\}$. If $B = \mathbb{Z}[\sqrt{D}]$ and $\epsilon = a + b\sqrt{D}$ is a unit in B, then $a^2 - Db^2 = \mathbb{N}(\epsilon) = \pm 1$. The equation $a^2 - Db^2 = \pm 1$ is Pell's equation, which was studied in depth by Fermat, Wallis and Brounker, using continued fractions to find $\sqrt{D}$.

Lemma 40. *Assume that k is a number field and that B is an order in k. Then $\epsilon \in B$ is a unit in B iff $\mathbb{N}(\epsilon) = \pm 1$.*

Proof. If ϵ is a unit, then $1 = \mathbb{N}(1) = \mathbb{N}(\epsilon)\mathbb{N}(\epsilon^{-1})$, and since $\mathbb{N}(\epsilon)$ and $\mathbb{N}(\epsilon^{-1})$ are integers, $\mathbb{N}(\epsilon) = \pm 1$. Conversely, assume that $\mathbb{N}(\epsilon) = \pm 1$. The minimal polynomial of ϵ over $\mathbb{Q}$ is $x^m - \mathrm{Tr}\,(\epsilon)x^{m-1} + \cdots + \pm\mathbb{N}(\epsilon)$. Thus, $\epsilon(\epsilon^{m-1} - \mathrm{Tr}\,(\epsilon)\epsilon^{m-2} + \cdots) = \pm\mathbb{N}(\epsilon) = \pm 1$. Since the element $\epsilon^{m-1} - \mathrm{Tr}\,(\epsilon)\epsilon^{m-2} + \cdots$ is in B, we see that ϵ is a unit in B. ☐

Given a number field k, there are r_1 distinct embeddings of k in $\mathbb{R}$, and there are $2r_2$ distinct embeddings of k in $\mathbb{C}$ whose images are not contained in $\mathbb{R}$. We construct $r_1 + r_2$ valuations $v : k^\times \to \mathbb{R}^\times$ corresponding to the embeddings. Recall that a valuation on k is a homomorphism of multiplicative groups $|\,| : k^\times \to \mathbb{R}^\times$ such that $|\alpha + \beta| \leq |\alpha| + |\beta|$. We shall use the notation $|\alpha|_v$ in place of $v(\alpha)$ to remind us that v is a valuation. If $\sigma : k \to \mathbb{R}$, then define $|\alpha|_v = |\sigma(\alpha)|$ where $|\,|$ represents the usual absolute value on $\mathbb{R}$. If $\sigma : k \to \mathbb{C}$ is a strictly complex embedding, then let $|\alpha|_v = |\sigma(\alpha)|^2$ where $|\,|$ is the usual absolute value on $\mathbb{C}$. If $\overline{\sigma} : k \to \mathbb{C}$ is the conjugate embedding, then it follows that $|\alpha|_v = \sigma(\alpha)\overline{\sigma}(\alpha)$, so this does not depend on the choice of representative of conjugacy class. We refer to the valuations constructed in this manner as the *infinite* valuations, and we say that the valuation *divides* ∞. Also, an *infinite place* is one of the following: a real embedding of k or a conjugate pair of complex embeddings.

Claim: For any nonzero $\alpha \in A$, $\prod_{r_1+r_2} |\alpha|_v = |\mathbb{N}(\alpha)| \in \mathbb{Q}_+^\times$, where the product is taken over the distinct infinite valuations of k. To see this, we compute

$$|\mathbb{N}(\alpha)| = \prod_{i=1}^{n} |\sigma(\alpha)| = \prod_{\mathbb{R}\text{ plc.}} |\sigma(\alpha)| \cdot \prod_{\mathbb{C}\text{ plc.}} \sigma(\alpha)\overline{\sigma}(\alpha) = \prod_{r_1+r_2} |\alpha|_v$$

as claimed.

Corollary 41. *A nonzero element $\alpha \in A$ is a unit iff $\prod_{r_1+r_2} |\alpha|_v = 1$.*

Example. If $k = \mathbb{Q}(\sqrt{D})$ for a positive, square-free integer D, then $r_1 = 2$ and $r_2 = 0$. If $\epsilon = a + b\sqrt{D} \neq \pm 1$ is a unit in A, then $|\epsilon|_1 > 1$ and $|\epsilon|_2 < 1$ so that either $|a + b\sqrt{D}| > 1$ and $|a - b\sqrt{D}| < 1$ or vice versa. We shall generalize this example in the next lecture.

We can also find valuations corresponding to nonzero prime ideals P of A. For $\alpha \in k^\times$, let $\mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\alpha A)$ as in Lecture 4, and define $|\alpha|_P = \mathbb{N}(P)^{-\mathrm{ord}_P(\alpha)} = q^{\mathrm{ord}_P(\alpha)}$ where $q = \mathbb{N}(P) = p^f$. The image of $|\,|_P$ in $\mathbb{R}_+^\times \cong \mathbb{R}$ is exactly $q^{\mathbb{Z}}$. In this case, we have $|\alpha+\beta|_P \leq \max\{|\alpha|, |\beta|\}$. A valuation which satisfies this property is called *non-archimedean*. The valuations constructed in this manner are the *finite* valuations on k.

Theorem 42. *(Product Formula) If $\alpha \in k^\times$, then $|\alpha|_v = 1$ for almost all valuations defined thus far, and $\prod_{all\ v} |\alpha|_v = 1$.*

Proof. For any such α there exist an integer N and nonzero $\beta \in A$ such that $\alpha = \frac{\beta}{N}$, so we may assume without loss of generality that $\alpha \in A$. Then $\alpha A = \prod_i P_i^{m_1}$, so the only possible valuations v with $|\alpha|_v \neq 1$ are the infinite valuations (a finite number) and those from the product with $m_i \geq 1$. Furthermore,

$$\prod_{\text{all } v} |\alpha|_v = \prod_{v|\infty} |\alpha|_v \cdot \prod_P |\alpha|_P = |\mathbb{N}(\alpha)| \cdot \prod_i \mathbb{N}(P_i)^{-m_1}$$
$$= |\mathbb{N}(\alpha)| \cdot (A : \alpha A)^{-1} = |\mathbb{N}(\alpha)| \cdot |\mathbb{N}(\alpha)|^{\cdot -1} = 1$$

as claimed. □

It follows from the proof that $\alpha \in A$ iff $|\alpha|_P \leq 1$ for all prime ideals P, and $\alpha \in A^\times$ iff $|\alpha|_P = 1$ for all prime ideals P.

Corollary 43. *For all $\alpha \in A^\times$, $\prod_{v|\infty} |\alpha|_v = 1$.*

Lecture 8

We continue with the notation from last lecture.

Proposition 44. *Assume that $r_1 + r_2 \geq 2$, and fix an infinite valuation v. Let B be an order in k. Then there exists a unit $\epsilon \in B^\times$ such that $|\epsilon|_v < 1$ and for all infinite valuations $w \neq v$, $|\epsilon|_w < 1$.*

Proof. For any $t = (t_1, \ldots, t_{r_1+r_2}) \in \mathbb{R}_+^{r_1+r_2}$ let $P_t \subset k \otimes \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the region

$$P_t = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |x|_v < t_v \text{ for all } v\}$$

The numbers $t_1, \ldots, t_{r_1}$ are radii of intervals. The $t_{r_1+1}, \ldots, t_{r_1+r_2}$ are square roots of radii of circles, as $z\overline{z} < t_v \Rightarrow |z| < \sqrt{t_v}$, which implies that the area of the circle is πt_v. Then $\overline{P}_t$ is a closed, bounded, convex, centrally symmetric subset of Euclidean space. Also, $\mathrm{Vol}(P_t) = 2^{r_1}\pi^{r_2} \prod_{r_1+r_2} t_v$. Let $M = \prod_{r_1+r_2} t_v$ and choose t and t' so that $\overline{P}_{t'} \subset P_t$ and $M' = (\frac{2}{\pi})^{r_2}|d_B|^{1/2} = M + 1$. Then $\mathrm{Vol}(P_{t'}) = 2^{r_1+r_2}|d_B|^{1/2} = 2^n \mathrm{Vol}(D)$ where D is the fundamental domain of B acting on $k \otimes \mathbb{R}$. It follows from Theorem 16 that $\overline{P}_{t'}$ contains a nonzero element α of B, and by our choices $\alpha \in P_t \cap B$. Since α is an algebraic integer, $|\mathbb{N}(\alpha)| \geq 1$. By construction $|\mathbb{N}(\alpha)| < M + 1$. So, α is an element of small norm. There is no reason *a priori* why we should expect α to satisfy the properties we desire from ϵ. However, we apply the following strategy to generate ϵ. (We say "generate" instead of "construct" because this method is *not* an efficient way to calculate ϵ in practice.) We shall construct elements α_i of B with small norm, and it will follow that $\alpha_i B = \alpha_j B$ for some $i \neq j$. Then $\alpha_i = \alpha_j \epsilon$ for some unit ϵ.

For $\delta > 0$, let $t_w = \delta$ for $w \neq v$ and $t_v = M/\delta^{(r_1+r_2-1)}$, and let $P(\delta)$ denote the corresponding P_t. (Here, we are taking "small" values of δ.) These choices for t give us a nonzero

$\alpha \in P(\delta) \cap B$. By construction, if $w \neq v$, then $0 < |\alpha|_w < \delta$. We claim that $|\alpha|_w \geq \frac{\delta}{M}$, so that these values are bounded away from zero. Fix some $w_0 \neq v$, and suppose that $|\alpha|_{w_0} < \frac{\delta}{M}$. Then

$$1 \leq |\mathbb{N}(\alpha)| = |\alpha|_{w_0} \cdot |\alpha|_v \cdot \prod_{w \neq v, w_0} |\alpha|_w < \frac{\delta}{M} \Big(\frac{M}{\delta^{(r_1+r_2-1)}} \Big) \delta^{(r_1+r_2-2)} = 1$$

a contradiction.

Let c be the number of ideals I of B such that $\mathbb{N}(I) \leq M+1$. (As noted before, c is finite.) For $i = 0, 1, 2, \dots, c$ fix nonzero $\alpha_i \in P(\frac{\delta}{M^i}) \cap B$. Since the set $\{\alpha_i B\}$ consists of $c+1$ ideals of norm $\mathbb{N}(\alpha_i B) = |\mathbb{N}(\alpha)| < M+1$, it follows that some $\alpha_i B = \alpha_j B$ for $0 \leq i < j \leq c$. Let $\epsilon = \alpha_i / \alpha_j$, which is an element of $B^\times$. Then, for $w \neq v$, $|\alpha_i|_w \geq \frac{\delta}{M^{i+1}}$ and $|\alpha_j|_w < \frac{\delta}{M^j}$, which implies that

$$|\epsilon|_w = \frac{|\alpha_i|_w}{|\alpha_j|_w} > \frac{(\delta / M^{i+1})}{(\delta / M^j} = \frac{M^j}{M^{i+1}} \geq 1$$

Furthermore, by Corollary 43, $1 = |\alpha|_v \cdot \prod_{w \neq v} |\alpha|_w < |\alpha|_v$, as desired. □

If B is an order in a number field k, define a group homomorphism

$$\lambda : B^\times \to \oplus_{v|\infty} \mathbb{R}v = \mathbb{R}^{(r_1+r_2)} \qquad \text{as} \qquad \lambda(\epsilon) = \sum_v \log |\epsilon|_v \cdot v.$$

Since $\mathbb{R}^{(r_1+r_2)}$ is torsion-free, it is clear that the torsion subgroup of $B^\times$ is in the kernel of λ. Also, the fact that $\prod_{v|\infty} |\epsilon|_v = 1$ implies that the image of λ is contained in the hyperplane $H = \{\sum_v a_v v : \sum_v a_v = 0\}$, since $\sum_v \log |\epsilon|_v = 0$. We can now formulate the Unit Theorem in terms of λ.

Theorem 45. *(Unit Theorem) Assume that k is a number field and that B is an order in k. Then the group of units $B^\times$ is a finitely generated abelian group. In fact,*

1. *The torsion subgroup of $B^\times$ is cyclic of finite order and equal to* $\ker(\lambda)$.
2. *The image of λ is a lattice in H, that is, a discrete, co-compact subgroup. Therefore, the rank of $B^\times$ is $r = r_1 + r_2 - 1$.*
3. *If $r_1 \neq 0$, then $B^\times_{tor} = \{\pm 1\}$.*

Proof. First, we note that, if we can prove that $B^\times_{\text{tor}}$ is finite, then the fact that it consists exactly of the roots of unity in B implies that it is cyclic. Second, if $r_1 \neq 0$, then there is a real embedding of k. Since roots of unity map to roots of unity, this implies that the only roots of unity in k are ± 1.

Let S be a compact subset of H. Then $\lambda^{-1}(S)$ is contained in the intersection of B with a bounded subset of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = k \otimes \mathbb{R}$. Since B is discrete in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, it follows that $\lambda^{-1}(S)$ is finite. Let $S = \{0\}$ to see that $\ker(\lambda) \supseteq B^\times_{\text{tor}}$ is finite. The fact that $\ker(\lambda)$ is finite implies that it is torsion, so that it is contained in (and therefore equal to) the set of roots of unity in B. This implies 1.

The argument of the preceding paragraph implies that $\mathrm{Im}(\lambda)$ is discrete in H. To show that $\mathrm{Im}(\lambda)$ is co-compact in H, we must show that the $\mathbb{R}$-span of $\mathrm{Im}(\lambda)$ is H. It suffices to show that if a linear form $\ell = \sum_v a_v x_v$ vanishes on $\mathrm{Im}(\lambda)$, then it vanishes on H, i.e., all a_v are equal since $H = \{(x_v) : \sum_v x_v = 0\}$. If $r_1 + r_2 < 2$ then there are two cases. Case 1: $r_1 = 1$ and $r_2 = 0$. In this case $k = \mathbb{Q}$ and the result is trivial. Case 2: $r_1 = 0$ and $r_2 = 1$. In this case, k is a purely imaginary quadratic field, which we checked explicitly in the previous lecture. Thus, we assume without loss of generality that k has at least two places.

If the form ℓ vanishes on $\mathrm{Im}(\lambda)$, then $\sum_v a_v \log|\epsilon|_v = 0$ for all $\epsilon \in B^\times$. Let v_0 be a place such that $a_{v_0} \leq a_v$ for all v, and let $\ell' = \ell - a_{v_0}\sum_v x_v$. Then all the coefficients of ℓ' are nonnegative, and the coefficient of x_{v_0} is 0. Furthermore, ℓ' vanishes on $\mathrm{Im}(\lambda)$ because ℓ vanishes on $\mathrm{Im}(\lambda)$ and $a_{v_0}\sum_v x_v$ vanishes on H. It suffices to show that $\ell' = 0$. By Proposition 44, there is an element $\epsilon \in B^\times$ such that $|\epsilon|_{v_0} < 1$ and for $w \neq v_0$, $|\epsilon|_w > 1$. If some $a'_w > 0$, then

$$0 = \ell'(\lambda(\epsilon)) = \sum_v a'_v \log|\epsilon|_v = \sum_{w\neq v_0} a'_w \log|\epsilon|_w > 0$$

a contradiction. $\square$

We sketch a generalization of the ideas behind the Unit Theorem. Recall that

$$A = \{\alpha \in k : |\alpha|_P \leq 1 \text{ for all } P\}$$

and

$$A^\times = \{\alpha \in k : |\alpha|_P = 1 \text{ for all } P\} = \{\alpha \in k : |\alpha|_v = 1 \text{ for all finite valuations } v\}.$$

Let S be a finite set of valuations of k which contains the infinite valuations. That is, S consists of all $r_1 + r_2$ infinite valuations and a finite number of the finite valuations. Let A_S denote the set $A_S = \{\alpha \in k : |\alpha|_v \leq 1 \text{ for all } v \notin S\}$. In other words, A_S consists of the elements α of k such that the the only primes with negative ramification index in the prime decomposition of αA must be in S. A_S is a ring containing A, and we sometimes denote A_S by $A[1/P]_{P\in S}$. The Generalized Unit Theorem states that the group of units of A_S is exactly $A^\times = \{\alpha \in k : |\alpha|_v = 1 \text{ for all } v \notin S\}$. The proof is similar to that of the Unit Theorem. The main tool is the homomorphism of groups

$$\lambda_S : A_S^\times \to \oplus_{v\in S}\mathbb{R}v \qquad \text{given by} \qquad \lambda_S(\epsilon) = \sum_{v\in S} \log|\epsilon|_v v.$$

The kernel of λ_S is $(A_S^\times)_{\mathrm{tor}}$, which is finite and consists of roots of unity. The image of λ_S is a lattice in the hyperplane $H_S = \{(x_v)_{v\in S} : \sum_{v\in S} x_v = 0\}$ and therefore the rank of $A_S^\times$ is $\dim(H) = \#(S) - 1$. The details are left to the interested reader. We will, however, consider a few examples.

Example. Let $k = \mathbb{Q}$ so that $A = \mathbb{Z}$, and let $S = \{\infty, p\}$ for some prime number p. (By saying that $\infty \in S$, we mean that the unique (real) embedding of $\mathbb{Q}$ is in S.) Then $A_S = \mathbb{Z}[1/p] = \{\frac{a}{p^r} : r \in \mathbb{Z}\}$. A contains the units ± 1 as well as the new unit p. It follows that $A_S^\times = \{\pm 1\} \times p^{\mathbb{Z}}$.

Example. Assume that A is the ring of algebraic integers in an arbitrary number field k, and S consists of the infinite valuations and a single finite valuation, say at the prime ideal P. Fix an element $\epsilon \in A_S^\times \smallsetminus A^\times$. Then for $Q \neq P$, $\mathrm{ord}_Q(\epsilon) = 0$ and $\mathrm{ord}_P(\epsilon) < 0$. It follows from the finiteness of the class group of A that $P^n = \epsilon A$ for some $n \geq 1$.

Lecture 9

We continue our discussion of the units in the ring of integers A of a number field k.

Corollary 46. *(Kronecker) If ϵ is an algebraic integer such that $|\epsilon|_v = 1$ for all infinite valuations v, then ϵ is a root of unity.*

Proof. Since $|\mathbb{N}(\epsilon)| = \prod_{v|\infty} |\epsilon|_v = 1$, Corollary 41 implies that ϵ is a unit in A. Letting $\lambda : A^\times \to \oplus_{v|\infty}\mathbb{R}v$ be given by $\alpha \mapsto \sum_v \log|\alpha|_v v$ as in the previous lecture, it follows that ϵ is in the kernel of λ, which is exactly the set μ of roots of unity in A. $\square$

Definition. A unit ϵ of A is called a *Lehmer unit* if all but two of its conjugates lie on the unit circle in $\mathbb{C}$. More precisely, if $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of k in $\mathbb{C}$ and $|\,|$ is the standard absolute value on $\mathbb{C}$, then for some $i \neq j$, $|\sigma_i(\epsilon)|, |\sigma_j(\epsilon)| \neq 1$ and for $l \neq i, j$, $|\sigma_l(\epsilon)| = 1$.

If ϵ is a Lehmer unit, then the fact that $1 = \prod_{v|\infty} |\epsilon|_v = \sigma_i(\epsilon)\sigma_j(\epsilon)$ implies that $\sigma_j(\epsilon) = \sigma_i(\epsilon)^{-1} = \sigma_i(\epsilon^{-1})$. For example, if k is a real quadratic field, and α is a unit in the interval $(0,1)$, then for the nontrivial embedding σ, $\sigma(\alpha) = 1/\alpha$ is in the interval $(1,\infty)$ and α is a Lehmer unit. In fact, if ϵ is a Lehmer unit and σ and τ are the embeddings such that $|\sigma(\epsilon)|, |\tau(\epsilon)| \neq 1$, then $\sigma(\epsilon)$ and $\tau(\epsilon)$ must be real. If not, say $\sigma(\epsilon)$ is not real, then $\overline{\sigma(\epsilon)}$ is another conjugate of ϵ. Since $|\overline{\sigma(\epsilon)}| = |\sigma(\epsilon)| \neq 1$, it follows that $\overline{\sigma(\epsilon)} = \tau(\epsilon)$. However, the fact that

$$|\tau(\epsilon)| = \frac{1}{|\sigma(\epsilon)|} = \frac{1}{|\overline{\sigma(\epsilon)}|} \neq 1$$

implies that $|\tau(\epsilon)| \neq |\overline{\sigma(\epsilon)}|$. It is natural to ask whether or not there are Lehmer units which are not roots of unity and whose real conjugates get arbitrarily close to 1. Lehmer conjectured that this could not occur.

Example. Let ℓ be a prime number $\ell \geq 3$, ζ a primitive ℓth root of unity, and $k = \mathbb{Q}(\zeta)$. By Proposition 36, the ring of integers of k is $A = \mathbb{Z}[\zeta]$. k is Galois over $\mathbb{Q}$ with Galois group G which is cyclic of order $n = \ell - 1 = 2r_2$ since k has no real embeddings. Then $r_1 = 0$ and $r_2 = \frac{\ell-1}{2}$, and by the Unit Theorem, $A^\times$ has rank $r_1 + r_2 - 1 = \frac{\ell-3}{2}$. Since G is cyclic of even order, it has a unique subgroup of order 2 whose nontrivial element is given by complex conjugation. Under the Galois Correspondence, the fixed field k^+ of this subgroup is the unique intermediate field of degree $\frac{\ell-1}{2}$ over $\mathbb{Q}$. Let A^+ denote the ring of algebraic integers in k^+. Clearly, $\mathbb{Z}[\zeta + \zeta^{-1}] \subseteq A^+$, and a discriminant computation shows equality. (One must verify directly that $\mathrm{disc}(A^+) = \ell^{(\frac{\ell-3}{2})}$.) Since k^+ is the fixed field of complex conjugation, k^+ is a real field. It follows from a little Galois theory that, $r_1^+ = n^+ = \frac{\ell-1}{2}$ and $r_2^+ = 0$. We verify this in more generality below. Again by the Unit Theorem, the rank of $(A^+)^\times$ is $\frac{\ell-3}{2}$. Since $(A^+)^\times \subseteq A^\times$ and these finitely generated groups have the same rank, the index $(A^\times : (A^+)^\times)$ is finite.

More generally, let k be a number field which is totally complex (i.e., $r_1 = 0$) which therefore has degree $n = 2r_2$ over $\mathbb{Q}$. Furthermore, assume that k is a quadratic extension of a totally real field k^+. (k is called a *CM field* in this event.) Assuming that $k \subset \mathbb{C}$, we let $\tau : k \to \mathbb{C}$ denote the embedding of k corresponding to complex conjugation. That is, if σ is a fixed embedding of k, then $\tau = \overline{\sigma}$. We let k^+ denote the fixed field of τ, or equivalently, $k^+ = k \cap \mathbb{R}$. Note that if σ is any embedding of k in $\mathbb{C}$, then $\overline{\sigma} = \sigma \circ \tau$ is the embedding of k conjugate to σ and $\{\sigma, \overline{\sigma}\}$ are the same real embedding of k^+. That is, there is a 1–1 correspondence between real embeddings of k^+ and conjugate pairs of embeddings of k. Furthermore, $(A^+)^\times$ has finite index in $A^\times$, as both groups have rank $r_2 - 1$.

Let u be a unit in A, and let $\epsilon = u/\tau(u)$. Then for any infinite place v of k,

$$|\epsilon|_v = \frac{|\sigma(u)|}{|\overline{\sigma(u)}|} = 1$$

so that ϵ is a root of unity by Corollary 46. It follows that $\tau(u) = \epsilon u$ for a root of unity ϵ. If β is another root of unity in k, then $\tau(\beta u) = \beta^{-1}\epsilon u = \frac{\epsilon}{\beta^2}(\beta u)$. Of course, $\frac{\epsilon}{\beta^2}$ is another root of unity. It follows that if we let $\epsilon = \beta^2$ and $u' = \beta u$, then u' is in the fixed field of τ, that is, $u' \in k^+$. Since u' is an algebraic integer, $u' \in A^+$. Also, u' is a unit in A^+, as is shown by Lemma 40 and the correspondence between real embeddings of k^+ and conjugate pairs of embeddings of k.

Let μ denote the set of roots of unity in k, and consider the map $\phi : A^\times \to \mu/\mu^2$ given by $u \mapsto u/\tau(u)$. The previous paragraph shows ϕ is well-defined and has kernel exactly $(A^+)^\times \cdot \mu$. Since μ is finite cyclic, it follows that $\mu/\mu^2 \cong \mathbb{Z}/2\mathbb{Z}$. Thus, the index of $(A^+)^\times \cdot \mu$ in $A^\times$ is 1 or 2, depending on whether ϕ is trivial or not. For example, if $k = \mathbb{Q}(\zeta)$ is the cyclotomic field from above, then $(A^+)^\times \cdot \mu = A^\times$. Since $(A^+)^\times \cap \mu = \{\pm 1\}$, this is not a direct product, but if μ' denotes the set of ℓth roots of unity, then $(A^+)^\times \times \mu' = A^\times$, as ℓ is odd by assumption.

Recall the notation from Lectures 6 and 7. If ζ is a primitive ℓth root of unity, let $\pi = \zeta - 1$. For integers a such that $2a \not\equiv 0 \pmod{\ell}$, let $\alpha(a) = \zeta^a - \zeta^{-a} = (\zeta^{2a} - 1)(\zeta^{-a})$. We claim that $\alpha(a)$ has norm ℓ. From our earlier computations, $\mathbb{N}(\zeta) = 1$ and $\mathbb{N}(\pi) = \ell$. Since $\zeta^{2a} - 1$ is a conjugate of π and ζ^{-a} is a conjugate of ζ we see that $\mathbb{N}(\alpha(a)) = \mathbb{N}(\pi)\mathbb{N}(\zeta) = \ell$. Also, it is straightforward to check that $\tau(\alpha(a)) = -\alpha(a)$. Let

$$u_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}} = \frac{\alpha(a)}{\alpha(1)}$$

(We call u_a a *circular unit* because if $\zeta = e^{2\pi i/\ell}$ then

$$u_a = \frac{e^{2\pi a i/\ell} - e^{-2\pi a i/\ell}}{e^{2\pi i/\ell} - e^{-2\pi i/\ell}} = \frac{\sin(2\pi a/\ell)}{\sin(2\pi/\ell)}$$

which is an expression in terms of the circular function sin.) We claim that u_a is a unit in A^+. To see this, it suffices to show that u_a is a unit in A which is fixed by τ, since then u_a is in A^+ and $\tau(u_a^{-1}) = \tau(u_a)^{-1} = u_a^{-1}$ so that $u_a^{-1} \in A^+$. Since $\mathbb{N}(\alpha(a)) = \ell$, we see that $\mathbb{N}(u_a) = \ell/\ell = 1$. Furthermore, u_a can be expressed as a polynomial in the algebraic integers ζ, ζ^{-1} so that u_a is an algebraic integer. Thus, u_a is a unit in A. Finally, since $\tau(\alpha(a)) = -\alpha(a)$, it follows that $\tau(u_a) = u_a$. To get distinct $\alpha(a)$ up to sign, we can allow a to run from 1 to $\frac{\ell-1}{2}$. The choice $a = 1$ gives $u_a = 1$, so we have $\frac{\ell-3}{2}$ reasonable choices for a. In fact, we have the following theorem.

Theorem 47. *(Kummer) Let U be the subgroup of $(A^+)^\times$ generated by the u_a. Then U is a free abelian group of rank $\frac{\ell-3}{2}$ and the index of U in $(A^+)^\times$ is finite and divisible by 2. Furthermore, if h^+ is the class number of A^+, then the index is exactly $2h^+$.*

The proof of this theorem involves the theory of L-functions, so we omit it here (cf. Borevich and Shafarevich *Number Theory*, Chapter 5). However, we check an example.

Example. Let $\ell = 5$. Then $u_2 = \frac{\zeta^2-\zeta^{-2}}{\zeta-\zeta^{-1}} = \zeta + \zeta^{-1}$. Since k has degree 4 over $\mathbb{Q}$, the field k^+ is real quadratic, so $k^+ = \mathbb{Q}(\sqrt{D})$ for some square free positive integer D. The nontrivial element of $\mathrm{Gal}(k^+/\mathbb{Q}) = \mathrm{Gal}(k/\mathbb{Q})/\mathrm{Gal}(k/k^+)$ is given by sending $\zeta \mapsto \zeta^2$. Thus,

$$\mathrm{Tr}\,(u_2) = (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$$

by examining the minimal polynomial of ζ, and

$$\mathbb{N}(u_2) = (\zeta + \zeta^{-1})(\zeta^2 + \zeta^{-2}) = \zeta^3 + \zeta^{-1} + \zeta + \zeta^{-3} = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$$

so that the minimal polynomial of u_2 is $x^2 + x - 1$. The quadratic formula tells us that $u = \frac{-1\pm\sqrt{5}}{2}$ and by fixing an embedding, we may assume that $u = \frac{-1+\sqrt{5}}{2}$. It follows that $k^+ = \mathbb{Q}(\sqrt{5})$, and a computation from Lecture 5 shows that $h^+ = 1$.

Next, we will discuss the tools developed by Chevalley, Artin, and Weil: completions of fields, the Adèles and the Idèles. These tools will give us a succinct reinterpretation of the finiteness of the ideal class group and the Unit Theorem. In much of the following discussion, only sketches of proofs will be given. The interested reader is invited to supply the missing details.

Recall that we construct infinite valuations on a number field from its embeddings in $\mathbb{C}$. These valuations satisfy the Archimedean property: for all $x, y \in k^\times$ there exists an integer n such that $|nx|_v > |y|_v$. This follows from the fact that the absolute values on $\mathbb{C}$ and $\mathbb{R}$ are Archimedean. The finite valuations are those induced by nonzero prime ideals P in A by the formula $|x|_P = \mathbb{N}(P)^{-\mathrm{ord}_P(x)}$. It follows that $|\alpha+\beta|_P \le \max\{|\alpha|_P, |\beta|_P\} \le |\alpha|_P + |\beta|_P$. Another way to express the first inequality is to say that all triangles are isosceles, since equality holds in the first inequality exactly when $|\alpha|_P \ne |\beta|_P$. However, the finite valuations do not satisfy the Archimedean property: since $\mathbb{Z} \subseteq A$, any integer n has $|n|_P \le 1$ so that $|nx|_P = |n|_P|x|_P \le |x|_P$.

We recall the construction of the real numbers from the rationals. With the standard absolute value on $\mathbb{Q}$

$$|x| = \begin{cases} x & \text{if } x > 0 \\ -x & \text{if } x < 0 \end{cases}$$

we say that a sequence $\{a_n\}$ is *Cauchy* if, for every $\epsilon > 0$ there exists N such that $n, m \ge N \Rightarrow |a_m - a_n| < \epsilon$. The problem with $\mathbb{Q}$ is that there exist (lots of) Cauchy sequences in $\mathbb{Q}$ which do not converge to elements of $\mathbb{Q}$. Basically, $\mathbb{R}$ is constructed by adjoining all the limits of Cauchy sequences in $\mathbb{Q}$ to $\mathbb{Q}$. We will be more specific below.

Definition. A *valued field* is a field k with valuation $|\,| : k^\times \to \mathbb{R}_+^\times$. A valued field k is *complete* if every Cauchy sequence in k converges to an element of k. A *completion* of a valued field k is an extension field K satisfying the following properties: (1) K is a valued field which is complete and whose valuation extends the valuation on k; and (2) K contains k as a dense subfield. We require property (2) for uniqueness purposes: without it, $\mathbb{C}$ would be a completion of $\mathbb{Q}$.

Theorem 48. *For a valued field k with valuation $|\,|_v$, a completion k_v exists and is unique up to unique continuous isomorphism. More precisely, if k_v and k'_v are completions of k, then there exists a unique continuous isomorphism $k_v \to k'_v$ making the following diagram commute.*

$$\begin{tikzcd} k_v \arrow[rr] & & k'_v \\ & k \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Sketch of proof. Let R be the ring of all Cauchy sequences $\{a_n\}$ with $a_n \in k$. Let $\mathfrak{m}$ denote the (maximal) ideal of R consisting of all null sequences, that is, sequences $\{a_n\}$ such that $\lim_{n\to\infty} |a_n|_v = 0$. We define k_v to be the quotient $k_v = R/\mathfrak{m}$, which is the field of limits of Cauchy sequences in k. We claim that this is a completion of k. We first extend the valuation from k to k_v in the natural way

$$|\,|_v : k_v^\times \to \mathbb{R}_+^\times \qquad \text{as} \qquad |\{a_n\}|_v = \lim_{n\to\infty} |a_n|_v \in \mathbb{R}$$

We embed k in k_v as the constant sequences

$$k \to k_v \qquad \text{as} \qquad a \mapsto \{a, a, a, \dots\}$$

since the constant sequences are trivially Cauchy.

Under this embedding, k is dense in k_v. Fix any $\alpha = \{a_n\} \in k_v$, and define a Cauchy sequence $\alpha_1, \alpha_2, \dots$ of elements in the image of k in k_v as $\alpha_i = \{a_i, a_i, \dots\}$. Then $\alpha = \lim_{n\to\infty} \alpha_i$. Finally, k_v is complete. Fix a Cauchy sequence in k_v, $\alpha^i = \{\alpha_n^i\} = \{\alpha_1^i, \alpha_2^i, \dots\}$. We want to show that this sequence converges to an element of k_v. Let β denote the "diagonal" sequence $\beta = \{\alpha_1^1, \alpha_2^2, \dots\}$. It is straightforward to show that $\beta = \lim_{n\to\infty} \alpha^n$. The uniqueness result is left as an easy exercise. □

Example. Let $k = \mathbb{Q}$ and $P = p\mathbb{Z}$ for a prime number p. The completion of $\mathbb{Q}$ with respect to the valuation $|\,|_P$ is denoted $\mathbb{Q}_p$ and called the *p-adic numbers*. It will follow from more general work that the ring of integers in $\mathbb{Q}_p$ is exactly $\mathbb{Z}_p = \lim_{\leftarrow}(\mathbb{Z}/p^n\mathbb{Z})$.

More generally, if k is a number field and P is a nonzero prime ideal in A of characteristic p, then the completion of k with respect to the valuation $|\,|_P$ is denoted k_P. We shall see that k_P is a finite extension of $\mathbb{Q}_p$ of degree $e_P f_P$, where e_P is the ramification index of P and f_P is the residue degree.

Lecture 10

We continue with the notation from the previous lecture. Given a nonzero prime ideal P in A, let $q = \mathbb{N}(P)$. Then the valuation $|\,|_P$ on k takes its values in $q^{\mathbb{Z}}$. Since the valuation is non-Archimedean, if the sequence $\{a_n\}$ is Cauchy with respect to $|\,|_P$, then the sequence $\{|a_n|_P\}$ in $q^{\mathbb{Z}} \subset \mathbb{Q}$ must stabilize. It follows that the valuation on k_P also takes its values in $q^{\mathbb{Z}}$. It also follows that the extended valuation is non-Archimedean. Define

$$A_P = \{\alpha \in k_P : |\alpha|_P \leq 1\}$$

and

$$P_P = \{\alpha \in k_P : |\alpha|_P < 1\} = \{\alpha \in k_P : |\alpha|_P \leq \tfrac{1}{q}\}$$

The fact that the valuation is non-Archimedean implies that A_P is a subring of k_P and that P_P is an ideal in A_P. Furthermore, restricting the embedding $k \hookrightarrow k_P$ to A and P induces a commuting diagram

$$\begin{tikzcd}
P_P \arrow[r, phantom, "\subset"] & A_P \arrow[r, phantom, "\subset"] & k_P \\
P \arrow[u, hook] \arrow[r, phantom, "\subset"] & A \arrow[u, hook] \arrow[r, phantom, "\subset"] & k \arrow[u, hook]
\end{tikzcd}$$

Proposition 49. *A_P is a discrete valuation ring with maximal ideal P_P.*

Proof. Since $P \neq 0$, we know that $P^2 \subsetneq P$. Fix an element $\pi \in P \setminus P^2$, that is, such that $|\pi|_P = \frac{1}{q}$. The fact that $P_P = \pi A_P$ will follow immediately from the following theorem.

Theorem 50. *Let I be any nonzero ideal of A_P and suppose that*

$$\max\{|\alpha|_P : 0 \neq \alpha \in I\} = q^{-m}$$

for some $m \geq 0$. Then $I = \beta A_P$ for some $\beta \in I$ such that $|\beta|_P = q^{-m}$.

Proof. First, we note that $\max\{|\alpha|_P : 0 \neq \alpha \in I\}$ is always of the form q^{-m}. This follows from the fact that $\{\mathrm{ord}_P(\alpha) : 0 \neq \alpha \in I\}$ is a nonempty set of natural numbers. Furthermore, there is an element β of I with $|\beta|_P = q^{-m}$ and we fix such an element. Clearly, $I \supseteq \beta A_P$. Conversely, if $\alpha \in I$, then $|\alpha/\beta|_P \leq 1$ so that $\gamma = \alpha/\beta \in A_P$ which implies that $\alpha = \gamma\beta \in \beta A_P$. $\square$

From the proof of the theorem, we see that $P_P = \pi A_P$. Furthermore, if P_P were not maximal, then there would be some proper ideal I of A_P such that $P_P \subsetneq I$. By the theorem, $I = \beta A_P$ for some $\beta \in I$. If β were in P_P, then $I = P_P$, so that $\beta \notin P_P$. It follows that $1 \geq |\beta|_P \geq 1$ so that $|\beta|_P = 1$. This implies that $|\beta^{-1}|_P = |\beta|_P^{-1} = 1$ so that $\beta^{-1} \in A_P$ which implies that $I = A_P$. It follows exactly from this logic that the units of A_P are exactly those elements α of k_P such that $|\alpha|_P = 1$.

To finish the proof of the proposition, it suffices to show that every nonzero ideal I of A_P is of the form $\pi^m A_P$. Let m and β be as in the theorem. Then $|\beta/\pi^m|_P = 1$ so that β/π^m is a unit in A_P and $I = \beta A_P = \pi^m A_P$. $\square$

Restricting the embedding $k \hookrightarrow k_P$ to the ideals P^n induces another commuting diagram

$$\begin{tikzcd}
\cdots \pi^n A_P \subset & \cdots & \subset \pi^2 A_P \subset & \pi A_P \arrow[r, phantom, "\subset"] & A_P \arrow[r, phantom, "\subset"] & k_P \\
\cdots\ P^n \arrow[u, hook] \arrow[r, phantom, "\subset"] & \cdots \arrow[r, phantom, "\subset"] & P^2 \arrow[u, hook] \arrow[r, phantom, "\subset"] & P \arrow[u, hook] \arrow[r, phantom, "\subseteq"] & A \arrow[u, hook] \arrow[r, phantom, "\subset"] & k \arrow[u, hook]
\end{tikzcd}$$

Proposition 51. *With notation as above.*

1. *The ring A is dense in A_P.*

2. The inclusion $A \hookrightarrow A_P$ induces an isomorphism $A/P^n \cong A_P/\pi^n A_P$ for $n = 1, 2, \ldots$.

3. $A_P = \varprojlim_n (A/P^n)$.

Proof. 1. For each $x \in A_P$, the fact that k is dense in k_P implies that for every $\epsilon > 0$ there are $\alpha, \beta \in A$ such that $|\alpha/\beta - x|_P < \epsilon$. Assuming that $\epsilon \leq 1$, the fact that $|x|_P \leq 1$ implies that $|\alpha/\beta|_P < 1$ since otherwise

$$\epsilon > |\alpha/\beta - x|_P = \max\{|\alpha/\beta|_P, |x|_P\} = |\alpha/\beta|_P \geq 1$$

Thus, $\mathrm{ord}_P(\alpha) \geq \mathrm{ord}_P(\beta)$ so that $\alpha \in P^{\mathrm{ord}_P(\beta)}$. It suffices to find an element $\gamma \in A$ such that $|\gamma - \alpha/\beta|_P < \epsilon$, since then

$$|\gamma - x|_P \leq |\gamma - \alpha/\beta|_P + |\alpha/\beta - x|_P < 2\epsilon$$

It is equivalent to find $\gamma \in A$ such that $|\alpha - \gamma\beta|_P < \epsilon|\beta|_P$. Furthermore, it suffices to show that $\alpha \in \beta A + P^n$ for $n \gg 0$, as this implies that for each such n there exists $\gamma_n \in A$ such that $\alpha - \gamma\beta \in P^n$ (so that $\mathrm{ord}_P(\alpha - \gamma\beta) \geq n$) and if we choose n such that $q^{-n} < \epsilon|\beta|_P$ then

$$|\alpha - \gamma_n\beta|_P = q^{-\mathrm{ord}_P(\alpha - \gamma_n\beta)} \leq q^{-n} < \epsilon|\beta|_P$$

as desired. Claim: for $n \geq \mathrm{ord}_P(\beta)$, $\beta A + P^n = P^{\mathrm{ord}_P(\beta)}$. Once the claim is proved, we are done, since we have already shown that $\alpha \in P^{\mathrm{ord}_P(\beta)}$. Since P is maximal, the only ideal containing $\beta A + P^n$ is P. Thus, the prime decomposition of $\beta A + P^n$ is of the form P^m. Since $\beta \in \beta A + P^n = P^m$, we see that $m \leq \mathrm{ord}_P(\beta)$. And the fact that $P^m = \beta A + P^n \subseteq P^{\mathrm{ord}_P(\beta)}$ implies that $m \geq \mathrm{ord}_P(\beta)$.

2. The ideal $\pi^n A_P$ is both open and closed in A_P, as

$$\pi^n A_P = \{\alpha \in A_P : |\alpha|_P \leq \tfrac{1}{q^n}\} = \{\alpha \in A_P : |\alpha|_P < \tfrac{1}{q^{n-1}}\}$$

Since A is dense in A_P and the coset $\alpha + \pi^n A_P$ is open for each $\alpha \in A_P$, it follows that $A \cap (\alpha + \pi^n A_P) \neq \emptyset$. This implies that the map $A \to A_P/\pi^n A_P$ is surjective for every n. Furthermore, the kernel is exactly $\pi^n A_P \cap A$. If we can show that this is exactly P^n, then we are done. This is clear, though, since $\pi^n A_P \cap A$ is exactly the collection of elements α of A with $|\alpha|_P \leq q^{-n}$, and this is exactly P^n.

3. By the completeness of A_P we see that $A_P = \varprojlim_n (A_P/\pi^n A_P) = \varprojlim_n (A/P^n)$. □

It follows from 3. that A_P is a compact topological ring, as it is the projective limit of finite (and therefore compact) topological rings. (We say that A_P is *profinite*.) Furthermore, k_P is locally compact as for every $\alpha \in k_P$, the translate $\alpha + A_P$ is a compact neighborhood. The advantage of working in k_P instead of $\mathbb{R}$ or $\mathbb{C}$ is that, in k_P, A is contained in the compact subring A_P. The images of A in $\mathbb{R}$ and $\mathbb{C}$ have no hope of being compact, as they are unbounded.

Recall that the Tychonoff Theorem implies that, with the product topology, the topological ring $\prod_{P \neq 0} A_P$ is compact, where the product is taken over all nonzero prime ideals P of A. The diagonal embedding $A \to \prod_P A_P$ given by $a \mapsto (a, a, \ldots)$ is a topological ring homomorphism.

Proposition 52. *The image of A under the diagonal embedding $A \to \prod_P A_P$ is a dense subring.*

Proof. By the definition of the product topology, to approach an element $x \in \prod_P A_P$, we must find $\alpha \in A$ which is arbitrarily close to x in any number of coordinates, indexed by a finite set of prime ideals. That is, if $P_1, \ldots, P_m$ are prime ideals and $m_i > 0$ for $i = 1, \ldots, m$, then we need to find an element $\alpha \in A$ such that $|\alpha - \alpha_i|_{P_i} < q_i^{-m_i}$ for $i = 1, \ldots, m$. This is equivalent to finding an element α such that $\alpha \equiv \alpha_i$ in $A_{P_i}/(P_i)_{P_i}^{m_i} = A/P_i^{m_i}$ for each i. The Chinese Remainder Theorem tells us that the homomorphism $A \to \prod_i A/P_i^{m_i}$ is surjective, since $i \neq j \Rightarrow P_i + P_j = A$. The result now follows. $\square$

We want a ring R which has the same properties with respect to k. That is, R should be locally compact and k should embed in R naturally. With the proposition in mind, our first candidate for R is $\prod_v k_v$ where the product is taken over all (finite and infinite) places. However, since the k_v are only locally compact (and not compact) and the product is infinite, this ring is no longer locally compact. The next reasonable candidate is $\coprod_v k_v$, which is locally compact. However, the diagonal map $k \to \coprod_v k_v$ is not well-defined. Therefore, the ring we want should be somewhere in between the coproduct and the product. This leads us to the Adèles $\mathbb{A}$ which is the locally compact subring of $\prod_v k_v$ consisting of those (a_v) such that $a_P \in A_P \subset k_P$ for almost all P. The diagonal embedding $k \to \prod_v k_v$ lands in $\mathbb{A}$ since, for $\alpha \in k$, $\mathrm{ord}_P(\alpha) = 0$ for all but finitely many P.

We describe the construction in a slightly more general context. Assume that V is some set indexing a collection of locally compact (abelian) groups $\{G_v\}$. How do we construct a locally compact subgroup of $\prod_v G_v$? Under an additional hypothesis we will do this via a "restricted" direct product $\underline{\prod}_v G_v$. Assume that, for all but finitely many $v \in V$, there is a distinguished compact, open subgroup H_v of G_v. Let V_∞ denote the finite collection of indices for which there is no H_v. The restricted direct product is then the subgroup $G = \underline{\prod}_v G_v$ of $\prod_v G_v$ consisting of those (g_v) such that $g_v \in H_v$ for almost all $v \in V \setminus V_\infty$. If S is a finite subset of V containing V_∞, then let

$$G_S = \Big(\prod_{v \in S} G_v\Big) \times \Big(\prod_{v \notin S} H_v\Big)$$

Since each G_v is locally compact and S is finite, $\prod_{v \in S} G_v$ is locally compact as well. And since each H_v is compact, $\prod_{v \notin S} H_v$ is also compact. It follow immediately that $G = \cup_S G_S$ where the union is taken over all such finite sets S. We also notice that if $S \subseteq T$, then $G_S \subseteq G_T$ is an open subgroup. Thus, the collection of G_S give an open system of neighborhoods for a topology on G which is locally compact. (Note that this is not the topology induced by the product topology on $\prod_v G_v$.)

If V now denotes the collection of (finite and infinite) valuations on k, we may take $G_v = k_v$ and for nonzero prime ideals P of A, $H_P = A_P$. In the previous notation, V_∞ is the collection of infinite valuations on k. For any finite subset S of V containing V_∞, we then have

$$\mathbb{A}_S = \Big(\prod_{v \in S} k_v\Big) \times \Big(\prod_{P \notin S} A_P\Big)$$

The benefit of the generality of the previous paragraph is that we can apply the same construction to the units of $\mathbb{A}$, taking $G_v = k_v^\times$ and $H_P = A_P^\times$. The resulting restricted direct product J is called the *idèles.* As abelian groups, $J = \mathbb{A}^\times$.

To convey somewhat the structure of $k_P^\times$, consider the short exact sequence of abelian groups

$$1 \to A_P^\times \to k_P^\times \xrightarrow{\mathrm{ord}_P} \mathbb{Z} \to 1$$

which necessarily splits. We see that a filtration on $A_P^\times$ will then induce a filtration on $k_P^\times$. Recall that a filtration of the ring A_P was given by powers of the maximal ideal P_P

$$\cdots \subset P_P^3 \subset P_P^2 \subset P_P \subset A_P$$

and since each $P_P^i = \pi^i$, it follows that each quotient in the filtration is a one dimensional vector space over the finite field $A_P/P_P \cong A/P$. The filtration of $A_P^\times$ is given by translates of powers of the maximal ideal

$$\cdots \subset 1 + P_P^3 \subset 1 + P_P^2 \subset 1 + P_P \subset A_P^\times$$

The first quotient is

$$A_P^\times/(1 + P_P) \cong (A/P)^\times$$

and for $i \geq 1$,

$$(1 + P_P^i)/(1 + P_P^{i+1}) \cong A/P$$

For more details, the interested reader should consult Serre *Local Fields*, Chapter IV, SS2..

As we noted above, the diagonal embedding $k \to \prod_v k_v$ is a continuous homomorphism of rings which lands in $\mathbb{A}$. The restriction to $k^\times$ is a continuous homomorphism of abelian groups which lands in $\mathbb{A}^\times$. In addition, we have the following.

Proposition 53. *With notation as above,*

1. *k is a discrete subring of $\mathbb{A}$ and the quotient $\mathbb{A}/k$ is compact.*
2. *$k^\times$ is a discrete subgroup of J, and the quotient $J/k^\times$ is almost compact.*

Definition. A space X is *almost compact* if it is of the form $C \times \mathbb{R}$ where C is compact. In the situation of the proposition, we can be more specific. There is a canonical surjective homomorphism $\| \, \| : J \to \mathbb{R}_+^\times$ given by $(a_v) \mapsto \prod_v |a_v|_v$. This is well-defined since the product is always finite. It is a multiplicative homomorphism, as each $| \, |_v$ is multiplicative. It is surjective, as k has at least one infinite place v. The completion k_v is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ as a valued field, and therefore $| \, |_v : k_v^\times \to \mathbb{R}_+^\times$ is surjective. To see that $\| \, \|$ is surjective, we apply it to an element of the form $(1, \ldots, a_v, 1, \ldots)$ where the non-identity entry is in the place indexed by the distinguished v. Furthermore, the kernel, which we shall denote by J_1, contains the image of $k^\times$, by the product formula (Theorem 42). Since the quotient $J/J_1 \cong \mathbb{R}_+^\times$ is isomorphic to the additive group of real numbers, part 2 of Proposition 53 is equivalent to the fact that $J_1/k^\times$ is compact.

Sketch of proof. If we write

$$\prod_{\text{all } v} k_v = \prod_{v|\infty} k_v \times \prod_{v\nmid\infty} k_v$$

then $\mathbb{A} \subset \prod_{\text{all } v} k_v$ has two distinguished subsets, namely

$$\prod_{v|\infty} k_v \times 1 \qquad \text{and} \qquad 1 \times \prod_{v\nmid\infty} A_v$$

As we noted above, $\prod_{v|\infty} k_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$, which contains A as a discrete, co-compact subset. Let D_∞ denote the fundamental domain for A acting on $\prod_{v|\infty} k_v$, which has compact closure, by co-compactness. Let $U_\infty \subset \mathbb{R}^n$ be an open subset containing 0 such that $A \cap U_\infty = (0)$, which exists by discreteness. Consider the subset

$$D = D_\infty \times \prod_{v\nmid\infty} A_v \subset \mathbb{A}$$

which has compact closure.

1. D is a fundamental domain for k acting on $\mathbb{A}$, i.e., $\mathbb{A}$ is the disjoint union of translates $\mathbb{A} = \cup_{\alpha\in k}(\alpha + D)$, so the quotient $\mathbb{A}/k$ is compact. Let

$$U = U_\infty \times \prod_{v\nmid\infty} A_v \subset \mathbb{A}$$

which is an open subset. Then $U \cap k = (0)$, as

$$k \cap \Big(1 \times \prod_{v\nmid\infty} A_v\Big) = A$$

Thus, k is discrete in $\mathbb{A}$.

2. If we now let

$$U = \prod_{v|\infty} k_v^\times \times \prod_{v\nmid\infty} A_v^\times$$

then U is an open subgroup of J and $U \cap k^\times = A^\times$. Using a bounded region in $\prod_{v|\infty} k_v^\times$, we can find a smaller open subset U_0 such that $U_0 \cap k^\times = (0)$. Thus, $k^\times$ is discrete in J. Since $U \cap k^\times = A^\times$, it follows that $k^\times \cdot U/U = k^\times/A^\times$. If we let $\mathbf{I}$ denote the group of all fractional ideals of A, let $\mathbf{P}$ denote the subgroup of principal fractional ideals and let C denote the ideal class group, then we have the following commuting diagram

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & U \arrow[r] \arrow[d, equal] & k^\times \cdot U \arrow[r] \arrow[d] & k^\times/A^\times \arrow[r, equal] \arrow[d] & \mathbf{P} \arrow[r] & 1 \\
1 \arrow[r] & U \arrow[r] & J \arrow[r] \arrow[d] & \coprod_P \mathbb{Z} \arrow[r, equal] \arrow[d] & \mathbf{I} \arrow[r] & 1 \\
 & & J/(k^\times \cdot U) \arrow[d] & C \arrow[d] & & \\
 & & 1 & 1 & &
\end{tikzcd}$$

in which the top two rows and the right-hand two columns are exact. It follows from the snake lemma that $J/(k^\times \cdot U) \cong C$, which is finite. The fact that $J/(k^\times \cdot U)$ is finite and the following short exact sequence

$$1 \to U/A^\times \to J/k^\times \to J/(k^\times \cdot U) \to 1$$

show that the index of $U/A^\times$ in $J/k^\times$ is finite. Thus, to prove that $J/k^\times$ is almost compact, it suffices to prove that $U/A^\times$ is almost compact. We have an inclusion

$$A^\times \hookrightarrow U = \prod_{v|\infty} k_v^\times \times \prod_{v\nmid\infty} A_v^\times$$

and a short exact sequence

$$1 \to \underbrace{1 \times \prod_{v\nmid\infty} A_v^\times}_{\text{compact}} \to U/A^\times \to \Big(\prod_{v|\infty} k_v^\times\Big)/\mathrm{Im}(A^\times) \to 1$$

so that we need only show that $(\prod_{v|\infty} k_v^\times)/\mathrm{Im}(A^\times)$ is almost compact. The short exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \prod_{v \text{ real}} \{\pm 1\} \times \prod_{v \text{ cpx.}} S^1 \arrow[r] & \prod_{v|\infty} k_v^\times \arrow[r, "\lambda"] & \bigoplus_{v|\infty} \mathbb{R}v \arrow[r] & 1 \\
 & & (\alpha_v) \arrow[r, mapsto] & \sum_v \log|\alpha_v|_v v &
\end{tikzcd}$$

induces a short exact sequence on quotients

$$1 \to \Big(\prod_{v \text{ real}} \{\pm 1\} \times \prod_{v \text{ cpx.}} S^1\Big)/A_{\text{tor}}^\times \to \Big(\prod_{v|\infty} k_v^\times\Big)/\mathrm{Im}(A^\times) \to \Big(\bigoplus_{v|\infty} \mathbb{R}v\Big)/\lambda(A^\times) \to 1$$

Since $\prod\{\pm 1\} \times \prod S^1$ is compact, so is the quotient $(\prod\{\pm 1\} \times \prod S^1)/A_{\text{tor}}^\times$. The Unit Theorem implies that $(\oplus_{v|\infty}\mathbb{R}v)/\lambda(A^\times)$ is almost compact. Thus, $\big(\prod_{v|\infty} k_v^\times\big)/\mathrm{Im}(A^\times)$ is almost compact and the proof is complete. $\square$

Notice that we used the finiteness of the class group and the Unit Theorem at key steps of the proof. It can be shown that the conclusions of the proposition are actually equivalent to these two results. (For example, see A. Weil *Basic Number Theory*, Champter V.)

Lecture 11

Now we introduce the zeta function of a number field and study its properties. In particular, we discuss the classical Riemann zeta function.

For a number field k and integer $n \geq 1$, let a_n denote the number of integral ideals I of A with $\mathbb{N}(I) = n$. For example, if $k = \mathbb{Q}$, then $A = \mathbb{Z}$ and $a_n = 1$ for all n since the unique such ideal is $n\mathbb{Z}$. If $k = \mathbb{Q}(\sqrt{D})$, then to calculate a_n, we must know the factorization of primes p in A. For example, if $pA = P_1P_2$ for distinct primes P_1 and P_2, then the ideals of index p are exactly the primes of characteristic p, namely, the P_i. The other cases are similar, and we summarize.

$$a_p = \begin{cases} 2 & \text{if } pA = P_1P_2 \text{ is split} \\ 1 & \text{if } pA = P^2 \text{ is ramified} \\ 0 & \text{if } pA = P \text{ is inert} \end{cases}$$

We can apply the same methods to a_{p^2}.

$$a_{p^2} = \begin{cases} 3 & \text{if } pA = P_1P_2 \text{ is split: the ideals are } P_1^2,\, P_2^2, \text{ and } P_1P_2 = pA \\ 1 & \text{if } pA = P^2 \text{ is ramified: the ideal is } P^2 = pA \\ 1 & \text{if } pA = P \text{ is inert: the ideal is } P = pA \end{cases}$$

Definition. Using the above notation, we define the *zeta function* of k as the formal series

$$\zeta_k(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where s is a complex variable.

Example. If $k = \mathbb{Q}$, then we have the Riemann zeta function

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Most properties of general zeta functions will be proved for the Riemann zeta function first, and the general case will follow from the specific case.

First, we study general series of the form $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ with all $a_i \in \mathbb{C}$. (A series of this form is called a *Dirichlet series.*) Assume that there are fixed real numbers $\sigma_0 \geq 0$ and $K > 0$ such that $|a_n| \leq Kn^{\sigma_0}$ for all n. (We say that $a_n = O(n^{\sigma_0})$.) Claim: Under these hypotheses, the Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges absolutely and defines an analytic function of s in the open half-plane $\mathrm{Re}(s) > \sigma_0 + 1$. In particular, the derivative of f may be taken term by term, and the series may be treated as a finite sum in terms of products, on the set of convergence. We prove this by the comparison test. We have

$$|n^{-s}| = |e^{-s\log n}| = e^{\mathrm{Re}(-s\log n)} = e^{-\sigma\log n} = n^{-\sigma}$$

where $\sigma = \mathrm{Re}(s)$. By assumption then, we have the inequality

$$\left|\frac{a_n}{n^s}\right| \leq K\frac{1}{n^{(\sigma-\sigma_0)}} = K\frac{1}{n^{\rho}}$$

where $\rho = \sigma - \sigma_0$. Thus, we compare the series $\sum_{n=1}^{\infty} \left| \frac{a_n}{n^s} \right|$ to the series $\sum_{n=1}^{\infty} \left| \frac{1}{n^\rho} \right| = \sum_{n=1}^{\infty} \frac{1}{n^\rho}$. The second series converges if $\rho > 1$ (by the integral test) and diverges if $\rho = 1$ (as this is the harmonic series). It follows that the original series converges absolutely for $\sigma - \sigma_0 = \rho > 1$, i.e., for $\sigma > 1 + \sigma_0$. Furthermore, for $\epsilon > 0$ and $c' \geq 1 + \epsilon$, the second series converges uniformly for $1 + \epsilon \leq \rho \leq c'$. Thus, $f(s)$ converges uniformly on compact subsets. Since each function in the sum is analytic, this proves the claim (cf. W. Rudin *Real and Complex Analysis*, Theorem 10.28). We rephrase the statement regarding products more precisely. Assume that $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ and $g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$ are Dirichlet series which converge absolutely and define an analytic function of s in the open half-plane $\mathrm{Re}(s) > \sigma_0 + 1$. Then the product $f(s)g(s)$ is another Dirichlet series

$$\Big(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{b_n}{n^s}\Big) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

which converges absolutely and defines an analytic function of s in the same open half-plane. The coefficients c_n are given by the formula

$$c_n = \sum_{\substack{de=n \\ d,e \geq 1}} a_d b_e$$

as expected.

We apply the claim to the Riemann zeta function. Since $a_n = 1$ for all n, the constants $\sigma_0 = 0$ and $K = 1$ tell us that $\zeta(s)$ is analytic on the open half-plane $\mathrm{Re}(s) > 1$. We shall prove later that the same convergence result holds for $\zeta_k(s)$ where k is any number field. As noted, $\zeta(s)$ does not converge at $s = 1$. We would like to know "how bad" the singularity is at $s = 1$.

Lemma 54. *The function $f(s) = \zeta(s) - \frac{1}{s-1}$ has an analytic continuation to the open half-plane $Re(s) > 0$. That is, $\zeta(s)$ is meromorphic on $Re(s) > 0$ with unique pole at $s = 1$ with residue $Res_{s=1}\zeta(s)ds = 1$.*

Proof. For $\mathrm{Re}(s) > 1$ we have

$$\int_1^\infty t^{-s}\, dt = \frac{t^{1-s}}{1-s}\Big|_1^\infty = \frac{1}{s-1}$$

Thus, for $\mathrm{Re}(s) > 1$

$$\begin{aligned}
\zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} \Big(\frac{1}{n^s} - \int_n^{n+1} t^{-s}\, dt \Big) \\
&= \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\, dt \\
&= \sum_{n=1}^{\infty} \phi_n(s)
\end{aligned}$$

where $\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s})\, dt$. Note that each $\phi_n(s)$ is defined for all s, and analytic on $\mathbb{C}$. As above, then , we need only show uniform convergence on compact subsets of $\mathrm{Re}(s) > 0$.

It is immediate that $|\phi_n(s)| \le \max_{n\le t\le n+1} |n^{-s} - t^{-s}|$. For fixed n, let $f_s(t) = n^{-s} - t^{-s}$. The Taylor series for $f_s(t)$ at $t = n$ is given by

$$f_s(t) = n^{-s} - t^{-s} = f_s(n) + f_s'(n)(t-n) + R(t) = \frac{s}{n^{s+1}}(t-n) + R(t)$$

where $R(t) = \frac{1}{2} f_s''(c)(t-n)^2$ for some c in the interval $[n, n+1]$. The fact that $|t-n| \le 1$ on this interval implies that

$$|f_s(t)| \le \frac{1}{n^{\sigma+1}}(|s| + \tfrac{1}{2}|s(s+1)|)$$

where $\sigma = \mathrm{Re}(s) > 0$. As before, we have absolute convergence for $\sigma > 0$ and uniform convergence on compact subsets of the half-plane, establishing the result. $\square$

Lemma 55. *For Re$(s) > 1$ we have an infinite product expansion*

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

Essentially, this result is a restatement of the unicity of prime factorization. This product is nice because each factor is analytic and nonzero for $\mathrm{Re}(s) > 0$. This implies that $\zeta(s)$ has no zeroes in the open half-plane $\mathrm{Re}(s) > 1$.

Proof. Let S be a finite set of prime numbers, and let $N(S)$ denote the infinite set of integers $n \ge 1$ whose prime factorization involves only the primes in S. The factor $(1 - p^{-s})^{-1}$ has an expansion as a geometric series

$$\frac{1}{1 - p^{-s}} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots$$

so that formal multiplication yields

$$\prod_{p\in S} (1 - p^{-s})^{-1} = \sum_{n\in N(S)} \frac{1}{n^s} \le \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$$

for $\mathrm{Re}(s) > 1$. Notice that this inequality holds for all such finite sets S, and as S becomes sufficiently large, $\sum_{n\in N(S)} \frac{1}{n^s} \to \sum_{n=1}^{\infty} \frac{1}{n^s}$. $\square$

Corollary 56. *As $s \to 1$ inside Re$(s) > 1$*

$$\sum_p \frac{1}{p^s} \sim \log\Big(\frac{1}{s-1}\Big)$$

where $\sim$ means that the quotient tends to 1.

Proof.

$$\begin{aligned}
\log(\zeta(s)) &= \log\Big(\prod_p (1 - p^{-s})^{-1}\Big) \\
&= \sum_p (-\log(1 - p^{-s})) \\
&= \sum_p \Big(p^{-s} + \frac{p^{-2s}}{2} + \frac{p^{-3s}}{3} + \cdots\Big)
\end{aligned}$$

using the Taylor expansion $-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$

$$= \sum_p \frac{1}{p^s} + \sum_p \sum_{k \geq 2} \frac{p^{-ks}}{k}$$

The series $\sum_p \sum_{k \geq 2} \frac{p^{-ks}}{k}$ is finite as $s \to 1$ and is bounded by

$$\sum_p \sum_{k \geq 2} \frac{p^{-k}}{k} \leq \sum_p \frac{1}{p(p-1)} \leq \sum_{n \geq 2} \frac{1}{n(n-1)} < 1$$

By Lemma 54,

$$\log(\tfrac{1}{s}) \sim \log(\zeta(s)) \sim \sum_p \frac{1}{p^s}$$

as desired. □

Corollary 57. *The sum $\sum_p \frac{1}{p}$ is infinite. In particular, there are an infinite number of prime numbers.*

Proof. Immediate. □

It has been shown that as $x \to \infty$, the function

$$\sum_{p \leq x} \frac{1}{p} \sim \log(\log(x))$$

Let $\pi(x)$ denote the number of prime numbers $p \leq x$, or equivalently, $\pi(x) = \sum_{p \leq x} 1$.

Theorem 58. *(Prime Number Theorem) As $x \to \infty$,*

$$\pi(x) \sim \frac{x}{\log(x)}$$

Riemann proved that the Prime Number Theorem is equivalent to the condition that $\zeta(s)$ has no zeros with $\mathrm{Re}(s) = 1$, $s \neq 1$. Hadamard then proved this statement. Furthermore, if we define $\mathrm{li}x = \int_2^x \frac{dt}{\log t}$, then it has been shown that

$$\pi(x) - \mathrm{li}x = O(xe^{-c(\log x)^{1/2}})$$

for a constant c, provided that $\zeta(s)$ has no zeroes for $\mathrm{Re}(s) \geq \rho$. Along these lines, we have the Riemann Hypothesis, which is still unsolved.

Conjecture 59. *(Riemann) The only zeroes of $\zeta(s)$ occur on the line $Re(s) = \frac{1}{2}$.*

There is much computational evidence for this conjecture. Also, it has been shown that

$$\#\{\rho \leq t : \zeta(\tfrac{1}{2} + i\rho) = 0\} = \frac{t}{2\pi} \log \frac{t}{2\pi} - \frac{t}{2\pi} + O(\log t)$$

(c.f., Davenport, *Multiplicative Number Theory*, p. 59).

Since we have been studying the properties of $\zeta(s) = \prod_p (1-p^{-s})^{-1}$, it seems reasonable for us to ask "What is $\prod_p (1-p^{-s})$?" We define the *Möbius function* $\mu : \mathbb{Z}_+ \to \{0, \pm 1\}$ as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ (-1)^t & \text{if } n \text{ is square-free with } t \text{ distinct prime factors} \end{cases}$$

Then we have the formula $\prod_p (1-p^{-s}) = \sum_{n-1}^{\infty} \frac{\mu(n)}{n^s}$. The proof of this is an exercise in bookkeeping, and is left to the interested reader. From this, we can prove the following.

Theorem 60. *(Möbius Inversion) Assume that $g : \mathbb{Z}_+ \to \mathbb{C}$ is a function such that for a fixed real number $\sigma_0 \geq 0$, $g(n) = O(n^{\sigma_0})$. Define $f : \mathbb{Z}_+ \to \mathbb{C}$ by the formula*

$$f(n) = \sum_{\substack{d|n \\ d \geq 1}} g(d)$$

Then we can recover g from f by the formula

$$g(n) = \sum_{\substack{n=de \\ d \geq 1}} f(d)\mu(e)$$

Proof. First, we observe that, given a sequence a_n, the formal series $\sum_n \frac{a_n}{n^s}$ satisfies the following property

$$\sum_n \frac{f(n)}{n^s} = \sum_n \frac{g(n)}{n^s} \sum_n \frac{a_n}{n^s} \quad \text{iff} \quad f(n) = \sum_{n=de} g(d) a_e$$

This equivalence follows from the following expansion

$$\sum_n \frac{g(n)}{n^s} \sum_n \frac{a_n}{n^s} = \sum_d \frac{g(d)}{d^s} \sum_e \frac{a_e}{e^s} = \sum_{d,e} \frac{g(d)a_e}{(de)^s} = \sum_n \frac{\sum_{n=de} g(d)a_e}{n^s}$$

If we write $f(n) = \sum_{n=de} g(d) 1_e$, then it follows that

$$\sum_n \frac{f(n)}{n^s} = \sum_n \frac{g(n)}{n^s} \sum_n \frac{1}{n^s} = \sum_n \frac{g(n)}{n^s} \zeta(s)$$

Multiplication by $\zeta(s)^{-1} = \prod_p (1-p^{-s}) = \sum_{n-1}^{\infty} \frac{\mu(n)}{n^s}$ yields

$$\sum_n \frac{g(n)}{n^s} = \sum_n \frac{f(n)}{n^s} \sum_{n-1}^{\infty} \frac{\mu(n)}{n^s}$$

so that our first observation implies the desired formula. $\square$

Lecture 12

We now return to the general zeta function $\zeta_k(s)$ for a number field k. As above, for $n = 1, 2, \ldots$, let a_n denote the number of integral ideals I of A with norm $\mathbb{N}(I) = n$. If P is a prime ideal of A of characteristic p, then P occurs in the factorization of pA, so we write $P|p$. Formally, we have

$$\zeta_k(s) = \sum_{I \subset A} \frac{1}{\mathbb{N}(I)^s} = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_P \Big(1 - \frac{1}{\mathbb{N}(P)^s}\Big)^{-1} = \prod_p \Big(\prod_{P|p} \Big(1 - \frac{1}{\mathbb{N}(P)^s}\Big)^{-1}\Big)$$

by the unicity of prime factorization of ideals. We want to show that $\zeta_k(s)$ converges absolutely on the open half-plane $\mathrm{Re}(s) > 1$ and describes an analytic function there. To accomplish this, we notice that the final expression may be written as

$$\lim_{x \to \infty} \prod_{p \leq x} \Big(\prod_{P|p} \Big(1 - \frac{1}{\mathbb{N}(P)^s}\Big)^{-1}\Big)$$

We shall show that the finite product in the limit satisfies

$$\Big|\prod_{p \leq x} \Big(\prod_{P|p} \Big(1 - \frac{1}{\mathbb{N}(P)^s}\Big)^{-1}\Big)\Big| \leq \zeta(s)^n$$

And therefore, the desired properties of $\zeta_k(s)$ follow from the corresponding properties of $\zeta(s)$. It should be noted that the equalities for the infinite sums and products are purely formal. However, taking limits of finite sums and products shows that the series also converge, and they converge to the same function as the infinite products. The equality of the sum with the product will be crucial in proving certain properties. In addition, we note that the individual factors $(1 - \frac{1}{\mathbb{N}(P)^s})^{-1}$ are all holomorphic on the region $\mathrm{Re}(s) > 0$.

Assume that p is an unramified prime, that is, $p \nmid d = \mathrm{disc}(k)$. (We shall only consider this case, as the ramified primes only contribute a finite number of factors to the product, each of which is holomorphic on the region $\mathrm{Re}(s) > 0$. Thus, with respect to questions of convergence, these factors may be ignored.) If $pA = \prod_{i=1}^N P_i$, then $p^n = \prod_{i=1}^N \mathbb{N}(P_i)$. Thus, $\prod_{i=1}^N (1 - p^{-f_i s})$ is a polynomial in p^{-s} of degree n. If we let $x = p^{-s}$, then

$$\prod_{i=1}^N (1 - p^{-f_i s}) = \prod_{i=1}^N (1 - x^{f_i})$$

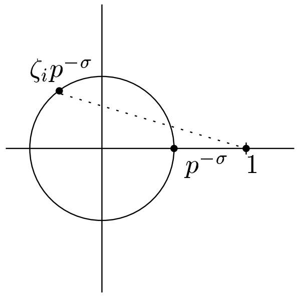
is a polynomial in x of degree n. We may factor each $1 - x^{f_i}$ as $\prod_{j=1}^{f_i} (1 - \zeta_j x)$ for f_ith roots of unity ζ_j. By renumbering, we see that there are roots of unity $\zeta_1, \ldots, \zeta_n$ such that

$$\prod_{i=1}^N (1 - x^{f_i}) = \prod_{i=1}^n (1 - \zeta_i x)$$

It follows that

$$\prod_{i=1}^N (1 - p^{-f_i s})^{-1} = \prod_{i=1}^n (1 - \zeta_i p^{-s})^{-1}$$

We estimate the size of $(1 - \zeta_i p^{-s})^{-1}$. If $\sigma = \mathrm{Re}(s) > 1$, then the distance from 1 to $\zeta_i p^{-s}$ is minimized when $\zeta_i = 1$, as the sketch shows.



It follows that

$$\Big|\frac{1}{1-\zeta_i p^{-s}}\Big| \leq \frac{1}{1-p^{-\sigma}}$$

so that

$$\Big|\prod_{P|p}\Big(1-\frac{1}{\mathbb{N}(P)^s}\Big)^{-1}\Big| \leq ((1-p^{-\sigma})^{-1})^n$$

and therefore

$$\Big|\prod_{p\leq x}\Big(\prod_{P|p}\Big(1-\frac{1}{\mathbb{N}(P)^s}\Big)^{-1}\Big)\Big| \leq \zeta(s)^n$$

as desired.

Next, we wish to understand the nature of the singularity of $\zeta_k(s)$ at $s=1$. First, recall some notions from the Unit Theorem. Let w denote the number of roots of unity in k, so that the group of roots of unity in K is $A^\times_{\text{tor}} \cong \mathbb{Z}/w\mathbb{Z}$. Let H denote the hyperplane in $\oplus_{v|\infty}\mathbb{R}v$, $H=\{\sum_v a_v v : \sum_v a_v = 0\}$. We define the map $\lambda : A^\times \to H$ as $\epsilon \mapsto \sum_v \log|\epsilon|_v v$. Let E denote the image of λ in H, which is free of rank $r = r_1 + r_2 - 1$. This gives a short exact sequence of abelian groups

$$1 \to \mathbb{Z}/w\mathbb{Z} \to A^\times \to E \to 1$$

which necessarily splits. Let $\epsilon_1, \dots, \epsilon_r \in A^\times$ such that the images of the ϵ_i in E form a basis. Then the matrix of λ is

$$M = \begin{pmatrix} \log|\epsilon_1|_{v_1} & \log|\epsilon_2|_{v_1} & \cdots & \log|\epsilon_r|_{v_1} \\ \vdots & \vdots & & \vdots \\ \log|\epsilon_1|_{v_{r+1}} & \log|\epsilon_2|_{v_{r+1}} & \cdots & \log|\epsilon_r|_{v_{r+1}} \end{pmatrix}$$

which is of order $(r+1)\times r$. Let M_j denote the matrix obtained by deleting the jth row of M. We claim that $|\det(M_j)|$ is independent of j. To see this, observe that since $E \subset H$, the sum of elements of any column of M is zero. It follows that M_j is obtained from any M_l by elementary row operations, so that the determinants differ only up to sign.

Definition. With the notation of the previous paragraph, we define the *regulator* of k as $R = |\det(M_j)|$.

There is an equivalent definition of R which is more geometric. Let μ denote the Haar measure on H induced by the short exact sequence

$$0 \to H \to \mathbb{R}^{r+1} \to \mathbb{R} \to 0$$

and the normalized Haar measures on $\mathbb{R}$ and $\mathbb{R}^{r+1}$. Let G be a free abelian subgroup of $A^\times$ which has finite index g in $A^\times$. It can be shown that

$$\frac{R}{w} = \frac{\mu(H/\lambda(G))}{g}$$

We shall not prove that these definitions are equivalent.

Theorem 61. *The function*

$$\zeta_k(s) - \frac{h\kappa}{s-1}$$

has an analytic continuation to the open half-plane $Re(s) > 1 - \frac{1}{n}$ where h is the class number of k and

$$\kappa = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d|}} \frac{R}{w}$$

In particular, $\zeta_k(s)$ has a meromorphic extension to this region with unique pole at $s = 1$ which is simple with residue $Res_{s=1}\zeta_k(s)ds = h\kappa$.

Below, we offer a sketch of the proof. For a more complete treatment, the interested reader should consult Borevich and Shafarevich *Number Theory*, Chapter 5.

Sketch of proof. Let C denote the ideal class group of k and fix and ideal class $c \in C$. For $m \in \mathbb{Z}_+$ we define

$$S_c(m) = \#\{I \subseteq A : cl(I) = c \text{ and } \mathbb{N}(I) \leq m\}$$

and

$$S(m) = \sum_{c \in C} S_c(m) = \#\{I \subseteq A : \mathbb{N}(I) \leq m\}$$

The key proposition one proves for this theorem is the following.

Proposition 62. *With notation as above*

$$S_c(m) = \kappa m + O(m^{(1-\frac{1}{n})})$$

In particular, the leading term in the expansion of $S_c(m)$ is independent of c.

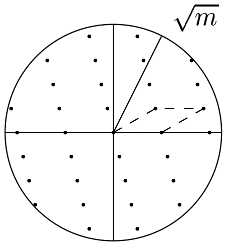
Sketch of proof in a simple case. Assume that $R = 1$, $r_2 = 1$ and $r_1 = 0$, so that k is an imaginary quadratic field. Furthermore, assume that $c = 1$ in C. Then

$$S_c(m) = \frac{\#\{\alpha \in A : |\mathbb{N}(\alpha)| \leq m\}}{w}$$

In this computation, we divide by w because every $I = \alpha A$ has w distinct generators, as $A^\times$ is finite of order w. If $\sigma : k \to \mathbb{C}$ is an embedding, then our assumptions imply that $\mathbb{N}(\alpha) = \sigma(\alpha)\overline{\sigma(\alpha)}$. It follows that

$$S_c(m) = \frac{\#\{\alpha \in A : |\sigma(\alpha)| \le \sqrt{m}\}}{w}$$

The following sketch



leads us to suspect that

$$\#\{\alpha \in A : |\sigma(\alpha)| \le \sqrt{m}\} \approx \frac{\text{volume of disc}}{\text{volume of fundamental domain for } A} = \frac{\pi m}{\frac{1}{2}|d|^{1/2}}$$

and this estimate is accurate with error $O(m^{1/2})$. With this estimate

$$S_c(m) = \frac{2\pi m}{w\sqrt{|d|}} + O(m^{1/2})$$

with our assumptions on R, r_1 and r_2 this is exactly the statement

$$S_c(m) = \kappa m + O(m^{(1-\frac{1}{n})})$$

which is the desired conclusion. $\square$

The following is an immediate consequence of Proposition 62.

Corollary 63. *With notation as above*

$$S(m) = h\kappa m + O(m^{(1-\frac{1}{n})})$$

The final piece of the puzzle is supplied by a lemma.

Lemma 64. *Assume that $f(s) = \sum_n \frac{b_n}{n^s}$ is a Dirichlet series.*

1. *If $|b_n| = O(n^{\sigma_0})$, then the series converges absolutely and defines an analytic function $f(s)$ on the open half-plane $Re(s) > 1 + \sigma_0$.*
2. *Let $T(m) = \sum_{n=1}^{m} b_n$ and suppose that $|T(m)| = O(m^\sigma)$ for some fixed real number $\sigma \ge 0$. Then the Dirichlet series converges and defines a holomorphic function $f(s)$ in the region $Re(s) > \sigma$. (It will not necessarily converge absolutely in this region.)*

Part 2 of the lemma is more subtle than our previous convergence results, as it is not saying that the series is absolutely convergent. Even though the condition $|b_n| = O(m^{\sigma_0})$ implies that $|T(m)| \leq \sum_{n=1}^{m} |b_n| = O(m^{\sigma_0 - 1})$, when we consider conditional convergence, cancellation can occur.

Example. Let $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$ be a nontrivial character (i.e., homomorphism of abelian groups). Extend χ to a map $\chi : \mathbb{Z} \to \mathbb{C}$ by defining $\chi(n) = 0$ if $(n, f) \neq 1$, and consider the Dirichlet series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. In the notation of the lemma, $|b_n| \leq 1$ for all n, so $\sigma_0 = 0$ and we have absolute convergence for $\mathrm{Re}(s) > 1$. However, $0 = \sum_{n=1}^{f} \chi(n) = \sum_{(n,f)=1} \chi(n)$, so $|T(m)| = O(1)$ and the original series converges in $\mathrm{Re}(s) > 0$, although not absolutely.

Proof. We proved part 1 in Lecture 11. For part 2, let $A_{p,m}$ denote the partial sum

$$A_{p,m} = \sum_{n=p}^{m} b_n = T(m) - T(p-1)$$

for all $m > p$. Then $|A_{p,m}| = O(m^\sigma)$ because $m^\sigma \geq (p-1)^\sigma$. Let $c_n = n^{-s}$. Then

$$\begin{aligned}
\sum_{n=p}^{m} b_n n^{-s} = \sum_{n=p}^{m} b_n c_n &= \sum_{n=p}^{m} (A_{p,n} - A_{p,n-1}) c_n \\
&= \sum_{n=p}^{m-1} A_{p,n}(c_n - c_{n+1}) + A_{p,m} c_m \\
&= \sum_{n=p}^{m-1} A_{p,n}\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big) + A_{p,m}\frac{1}{m^s}
\end{aligned}$$

The following bounds

$$\begin{aligned}
\Big|\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big| &\leq \frac{|s|}{n^{(\mathrm{Re}(s)+1)}} \\
|A_{p,n}| &\leq K n^\sigma \\
\Big|\frac{A_{p,m}}{m^s}\Big| &\leq \frac{K m^\sigma}{m^{\mathrm{Re}(s)}}
\end{aligned}$$

imply that

$$\Big|\sum_{n=p}^{m} b_n n^{-s}\Big| \leq K\Big[\sum_{n=p}^{m-1} \frac{|s|}{n^{(\mathrm{Re}(s)-\sigma+1)}} + \frac{1}{m^{(\mathrm{Re}(s)-\sigma)}}\Big]$$

Since $|s|$ is bounded in any compact region, we see that as $p, m \to \infty$ the terms

$$\sum_{n=p}^{m-1} \frac{|s|}{n^{(\mathrm{Re}(s)-\sigma+1)}} \qquad \text{and} \qquad \frac{1}{m^{(\mathrm{Re}(s)-\sigma)}}$$

both tend to zero, by the absolute convergence of $\zeta(s)$ in the region $\mathrm{Re}(s) > 1$. This implies uniform convergence in compact regions, so $f(s)$ is analytic in $\mathrm{Re}(s) > \sigma$, as desired.

□

To see how this completes the proof of the theorem, consider the function

$$f(s) = \zeta_k(s) - h\kappa\zeta(s) = \sum_n \frac{b_n}{n^s}$$

where $b_n = a_n - h\kappa$. By Corollary 63 we see that

$$T(m) = \sum_{n=1}^{m} b_m = (h\kappa m - h\kappa m) + O(m^{(1-\frac{1}{n})})$$

so that Lemma 64 implies that $f(s)$ is holomorphic on the region $\mathrm{Re}(s) > 1 - \frac{1}{n}$. The fact that

$$\zeta_k(s) - \frac{h\kappa}{s-1} = [\zeta_k(s) - h\kappa\zeta(s)] + h\kappa\Big[\zeta(s) - \frac{1}{s-1}\Big]$$

with Lemma 54 give the desired region of holomorphicity and the correct residue. $\square$

At the point $s = 1$ we may consider the formal product

$$\prod_p \Big(\prod_{P|p}\Big(1 - \frac{1}{\mathbb{N}(P)}\Big)^{-1}\Big) = \prod_p \Big(\prod_{P|p}\Big(\frac{\mathbb{N}(P)-1}{\mathbb{N}(P)}\Big)^{-1}\Big) = \prod_p \Big(\prod_{P|p}\frac{\mathbb{N}(P)}{\mathbb{N}(P)-1}\Big)$$

obtained by "evaluating" $\zeta_k(1)$. If we again disregard the finite number of ramified prime numbers, and consider the factor $\prod_{\mathrm{char}(P)=p}\frac{\mathbb{N}(P)}{\mathbb{N}(P)-1}$ where $p \nmid d$, then we have

$$\prod_{P|p}\frac{\mathbb{N}(P)}{\mathbb{N}(P)-1} = \frac{p^n}{\prod_{P|p}(\mathbb{N}(P)-1)} = \frac{p^n}{\prod_{P|p}\#(A/P)^\times} = \frac{p^n}{\#(A/pA)^\times}$$

since the Chinese Remainder Theorem implies that $A/pA = \prod_{P|p} A/P$.

Lecture 13

Given a nontrivial character $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$, we can extend χ to a function $\chi : \mathbb{Z} \to \mathbb{C}$ by defining $\chi(n) = 0$ if $(n, f) \neq 1$. (We shall apply this convention frequently below without formally restating it each time.) Let $L(\chi, s) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$. As we noted in Lecture 12, Lemma 24 implies that $L(\chi, s)$ converges and defines an analytic function in the region $\mathrm{Re}(s) > 0$. This allows us to restate an improvement of the converse to Corollary 34 which we proved in Lecture 6.

Theorem 65. *(Dirichlet's Reinterpretation of Quadratic Reciprocity) Let k be a quadratic field with discriminant d. Then there is a character $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ (i.e., a character $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi \neq 1$ and $\chi^2 = 1$) such that for every prime number p*

1. *p splits in k iff $\chi(p) = 1$*
2. *p is inert in k iff $\chi(p) = -1$*

3. p is ramified in k iff $\chi(p) = 0$

Moreover, we have a factorization $\zeta_k(s) = \zeta(s)L(\chi, s)$ in the region $Re(s) > 1$, and $\zeta_k(s)$ has a meromorphic continuation to the region $Re(s) > 0$ whose unique pole is at the point $s = 1$ and is simple.

Example. If $d = \ell \equiv 1 \pmod 4$ is a prime, then, as noted in Lecture 6, the character is exactly $\chi(n) = (\frac{n}{\ell})$, as

1. p splits in k iff $(\frac{p}{\ell}) = (\frac{\ell}{p}) = 1$
2. p is inert in k iff $(\frac{p}{\ell}) = (\frac{\ell}{p}) = -1$
3. p is ramified in k iff $p = \ell$.

Proof. The algebraic properties were proved in Lecture 6. Furthermore, we demonstrated that for any prime number p (ramified or unramified) the factor of $\zeta_k(s)$ corresponding to p is

$$\left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

so that

$$\zeta_k(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Since

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

it suffices to show that

$$L(\chi, s) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Factor any positive integer $n = \prod_i p_i^{a_i}$ so that $\chi(n) = \prod_i \chi(p_i)^{a_i}$. Since

$$(1 - \chi(p)p^{-s})^{-1} = 1 + \chi(p)p^{-s} + \chi(p^2)p^{-2s} + \cdots = \sum_{n=0}^{\infty} \chi(p^n)p^{-ns}$$

a bit of bookkeeping implies the desired result. $\square$

Corollary 66. *(Class Number Formula for Quadratic k) Let k be a quadratic field with discriminant d. If $d > 0$, then the regulator is given by $R = \log|\epsilon|$ for some $\epsilon > 1$ generating $A^\times/\{\pm 1\}$. If $d < 0$, then $R = 1$. Moreover,*

$$L(\chi, 1) = h\kappa = \begin{cases} \frac{2h\log|\epsilon|}{\sqrt{d}} & \textit{if } d > 0 \\ \frac{2\pi h}{w\sqrt{|d|}} & \textit{if } d < 0 \end{cases}$$

Proof. If $d > 0$ then $r_1 = 2$ and $r_2 = 0$, so $A^\times$ has rank 1. With the notation of Lecture 12, let $H \subset \mathbb{R}^2$ denote the hyperplane which contains the image E of $A^\times$ under the map $\lambda : A^\times \to \mathbb{R}^2$ given by $\epsilon \mapsto (\log|\epsilon|_{v_1}, \log|\epsilon|_{v_2})$. Fix an element $\epsilon \in A^\times$ which maps to a basis element of E. Without loss of generality, assume that $|\epsilon|_{v_1} > 1$, as $\epsilon \neq \pm 1$. Then $R = \log|\epsilon|_{v_1}$, by definition. If $d < 0$ then $A^\times$ has rank 0, and the definition of R shows that R is the "empty determinant" which is 1.

The final claim follows from considering the Taylor expansions of $\zeta(s)$ and $\zeta_k(s)$, and the facts that $\mathrm{Res}_{s=1}\zeta(s) = 1$ and $\mathrm{Res}_{s=1}\zeta_k(s) = h\kappa$ by Lemma 54 and Theorem 61. □

Corollary 67. $L(\chi, 1) > 0$

Proof. Immediate. □

We desire an independent evaluation of $L(\chi, 1)$ for any nontrivial character $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$. Our first tool shall be the *Gauss sum* of χ which we define to be the complex number

$$g(\chi) = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}$$

Lemma 68. *If $(n, f) = 1$, then*

$$\chi(n) g(\overline{\chi}) = \sum_{b=1}^{f} \overline{\chi}(b) e^{2\pi i b n/f}$$

where $\overline{\chi}$ denotes the conjugate character, i.e., $\overline{\chi} = \chi^{-1}$ as the image of χ is contained in the set of roots of unity in $\mathbb{C}$.

Proof. By making the substitution $b \equiv an^{-1} \pmod{f}$ so that $nb \equiv a \pmod{f}$ we have

$$\chi(n) g(\overline{\chi}) = \sum_{a=1}^{f} \chi(n)\overline{\chi(a)} e^{2\pi i a/f} = \sum_{b=1}^{f} \overline{\chi}(b) e^{2\pi i b n/f}$$

as desired. □

By definition,

$$g(\overline{\chi}) L(\chi, s) = \sum_{n=1}^{\infty} g(\overline{\chi}) \chi(n) n^{-s}$$

If $(n, f) \neq 1$ then $\chi(n) = 0$ and the corresponding terms in the series vanish. If $(n, f) = 1$, then the lemma applies, and it follows that

$$g(\overline{\chi}) L(\chi, s) = \sum_{\substack{b=1 \\ (f,b)=1}}^{f} \overline{\chi}(b) \Big(\sum_{n=1}^{\infty} \frac{e^{2\pi i b n/f}}{n^s} \Big) = \sum_{\substack{b=1 \\ (f,b)=1}}^{f} \overline{\chi}(b) \Big(\sum_{n=1}^{\infty} \frac{(e^{2\pi i b/f})^n}{n^s} \Big)$$

and we have absolute convergence in the region $\mathrm{Re}(s) > 1$. If $\zeta = e^{2\pi i/f}$, then the formula becomes

$$g(\overline{\chi})L(\chi, s) = \sum_{\substack{b=1 \\ (f,b)=1}}^{f} \overline{\chi}(b)\Big(\sum_{n=1}^{\infty} \frac{(\zeta^b)^n}{n^s}\Big) \tag{5}$$

We recall that the branch of $-\log(1-x)$ defined on the region $|x| < 1$ has power series expansion $-\log(1-x) = \sum_{n\geq 1} \frac{x^n}{n}$ and that the series actually converges to $-\log(1-x)$ for $|x| = 1$ such that $x \neq 1$. A lemma of Abel states that we may substitute the value $s = 1$ into equation (5) which yields

$$g(\overline{\chi})L(\chi, 1) = \sum_{\substack{b=1 \\ (f,b)=1}}^{f} \overline{\chi}(b)(-\log(1-\zeta^b)) \tag{6}$$

Lecture 14

Definition. A character $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$ is *primitive* if there is no proper divisor f' of f such that χ is induced by a character $\chi' : (\mathbb{Z}/f'\mathbb{Z})^\times \to \mathbb{C}^\times$. It follows immediately that, if f is prime, then χ is primitive iff χ is nontrivial. A character χ (not necessarily primitive) is said to be *even* if $\chi(-1) = 1$, and is said to be *odd* if $\chi(-1) = -1$.

Lemma 69. *(Gauss' Formula) If χ is primitive, then $g(\chi)g(\overline{\chi}) = \chi(-1)f$. In particular, $g(\chi) \neq 0$ and $|g(\chi)| = \sqrt{f}$.*

We shall prove this lemma in the case where f is prime.

Proof. Assume that $f = \ell$ is prime. For any function $F : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{C}$, the Fourier transform of F is the function $\hat{F} : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{C}$ given by the formula

$$\hat{F}(b) = \sum_{a=1}^{\ell} F(a)e^{2\pi i ab/\ell}$$

In particular, a character $\chi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mathbb{C}^\times$ can be extended to such a function, and we have

$$\hat{\chi}(b) = \sum_{a=1}^{\ell} \chi(a)e^{2\pi i ab/\ell}$$

For $b = 0$ the fact that χ is a nontrivial character implies that

$$\hat{\chi}(0) = \sum_{a=1}^{\ell-1} \chi(a) = 0$$

If $b \neq 0$, then we make the substitution $c \equiv ab \pmod{\ell}$ so that $a \equiv cb^{-1} \pmod{\ell}$ and

$$\hat{\chi}(b) = \sum_{c\neq 0} \chi(cb^{-1})e^{2\pi i c/\ell} = \chi(b)^{-1} \sum_{c\neq 0} \chi(c)e^{2\pi i c/\ell} = \chi(b)^{-1}g(\chi) \tag{7}$$

Thus, $\hat{\chi} = g(\chi)\chi^{-1}$. If $g(\chi) = 0$, then $\hat{\chi} = 0$, but this can not hold because of the Fourier inversion formula

$$\widehat{(\hat{F})}(-a) = \ell F(a)$$

Applying formula (7) twice yields

$$\hat{\hat{\chi}} = g(\chi)\widehat{\chi^{-1}} = g(\chi)g(\chi^{-1})\chi$$

and Fourier inversion implies that

$$g(\chi)g(\chi^{-1})\chi(-a) = \chi(a)\ell$$

Letting $a = -1$ we get

$$\chi(-1)\ell = g(\chi)g(\chi^{-1})\chi(1) = g(\chi)g(\overline{\chi})$$

as desired. If we conjugate the definition of $g(\chi)$ and make the substitution $a \mapsto -a$, this yields

$$\overline{g(\chi)} = \sum_{a=1}^{\ell} \overline{\chi(a)}e^{-2\pi ia/\ell} = \sum_{a=1}^{\ell} \overline{\chi(-a)}e^{2\pi ia/\ell} = \overline{\chi(-1)} \sum_{a=1}^{\ell} \overline{\chi(a)}e^{-2\pi ia/\ell} = \chi(-1)g(\overline{\chi})$$

so that

$$|g(\chi)| = [g(\chi)\overline{g(\chi)}]^{1/2} = [g(\chi)\chi(-1)g(\overline{\chi})]^{1/2} = [\chi(-1)\chi(-1)\ell]^{1/2} = \sqrt{\ell}$$

as desired. □

Assume that ℓ is a prime number and that χ is nontrivial. Then

$$\chi(n)g(\overline{\chi}) = \sum_{b=1}^{\ell} \overline{\chi}(b)e^{2\pi ibn/\ell}$$

for all $n \geq 1$: if $(n, \ell) = 1$ then this is Lemma 68, otherwise each side is zero. Thus

$$\begin{aligned} g(\overline{\chi})L(\chi, s) &= \sum_{n\geq 1} \Big(\sum_{b=1}^{\ell} \overline{\chi}(b)e^{2\pi ibn/\ell}\Big)n^{-s} = \sum_{b=1}^{\ell} \overline{\chi}(b)\Big(\sum_{n\geq 1} \frac{e^{2\pi ibn/\ell}}{n^s}\Big) \\ &= \sum_{b=1}^{\ell-1} \overline{\chi}(b)\Big(\sum_{n\geq 1} \frac{(\zeta^b)^n}{n^s}\Big) \end{aligned} \tag{8}$$

where $\zeta = e^{2\pi i/\ell}$. This series converges (conditionally) for $\mathrm{Re}(s) > 0$ by Lemma 64. The power series

$$-\log(1-x) = \sum_{n\geq 1} \frac{x^n}{n}$$

gives the branch of log given by

$$\log(z) = \log|z| + i\arg(z) \qquad \text{for} \qquad -\pi/2 < \arg(z) < \pi/2$$

Thus, substituting $s = 1$ into equation (8) yields

$$g(\overline{\chi})L(\chi,1) = \sum_{b=1}^{\ell-1} \overline{\chi}(b)\Big(\sum_{n\geq 1} \frac{(\zeta^b)^n}{n}\Big) = \sum_{b=1}^{\ell-1} \overline{\chi}(b)(-\log(1-\zeta^b))$$

To simplify the formula for $L(\chi, 1)$, we consider two cases.

If χ is even, then $\chi(-b) = \chi(b)$ for all b so that

$$g(\overline{\chi})L(\chi,1) = -\sum_{b=1}^{\ell-1} \overline{\chi}(b)\log(1-\zeta^b) = -\sum_{b=1}^{\ell-1} \overline{\chi}(b)\log|1-\zeta^b|$$

by our choice of the branch of $\log x$, since the argument terms cancel. By Lemma 69, this implies that

$$L(\chi,1) = -\frac{g(\chi)}{\ell}\sum_{b=1}^{\ell-1} \overline{\chi}(b)\log|1-\zeta^b| \tag{9}$$

If χ is odd, then $\chi(-b) = -\chi(b)$ for all b so that

$$g(\overline{\chi})L(\chi,1) = -i\sum_{b=1}^{\ell-1} \overline{\chi}(b)\arg(1-\zeta^b)$$

as in the even case. Thus,

$$L(\chi,1) = \frac{ig(\chi)}{\ell}\sum_{b=1}^{\ell-1} \overline{\chi}(b)\arg(1-\zeta^b)$$

This is not quite as nice as the final formula in the even case since $\arg(1-\zeta^b)$ is more complicated than $\log|1-\zeta^b|$. For $b = 1, \ldots, \ell-1$ the fact that arg is additive (up to multiple of 2π) implies that

$$\arg(1-\zeta^b) = \arg(\zeta^{b/2}(\zeta^{-b/2}-\zeta^{b/2})) = \arg(\zeta^{b/2}) + \arg(\zeta^{-b/2}-\zeta^{b/2})$$

The complex number $\zeta^{-b/2}-\zeta^{b/2}$ is purely imaginary, so its argument is $\pm\pi/2$. By definition, $\zeta^{b/2} = e^{2\pi ib/2\ell} = e^{\pi ib/\ell}$ and therefore has argument $\pi b/\ell$ which is in the interval $(0,\pi)$. It follows that, in order for $\arg(1-\zeta^b)$ to fall in the correct interval, $\zeta^{-b/2}-\zeta^{b/2}$ must have argument $-\pi/2$. Thus,

$$\arg(1-\zeta^b) = \pi(\tfrac{b}{\ell} - \tfrac{1}{2})$$

which implies that

$$L(\chi,1) = \frac{\pi i g(\chi)}{\ell}\sum_{b=1}^{\ell-1} \overline{\chi}(b)(\tfrac{b}{\ell} - \tfrac{1}{2}) \tag{10}$$

We note that, if $B_1(x) = x - \frac{1}{2}$ is the first Bernoulli polynomial, then

$$\sum_{b=1}^{\ell-1} \overline{\chi}(b)(\tfrac{b}{\ell} - \tfrac{1}{2}) = \sum_{b=1}^{\ell-1} \overline{\chi}(b)B_1(b/\ell)$$

which we shall denote by $B_{1,\overline{\chi}}$, and we may write

$$L(\chi, 1) = \frac{\pi i g(\chi)}{\ell} B_{1,\overline{\chi}}$$

Example. Let $k = \mathbb{Q}(\sqrt{\ell})$ where ℓ is a positive prime such that $\ell \equiv 1 \pmod 4$. Then Corollary 66 implies that

$$\mathrm{Res}_{s=1}\zeta_k(s) = \frac{2h \log|\epsilon|}{\sqrt{\ell}} = L(\chi, 1)$$

where $\chi(b) = (\frac{b}{\ell})$, as we noted in Lecture 6. Since χ is real-valued, we see that $\chi = \overline{\chi}$ and has order 2. By equation (9) it follows that

$$L(\chi, 1) = -\frac{g(\chi)}{\ell} \log\left|\frac{\prod_{(\frac{b}{\ell})=1}(1-\zeta^b)}{\prod_{(\frac{b}{\ell})=-1}(1-\zeta^b)}\right|$$

We know that $g(\chi)^2 = \ell$, so the coefficient is $\pm\frac{1}{\sqrt{\ell}}$. In fact, $g(\chi) = +\sqrt{\ell}$, but this is not easy to verify. (For a proof, see Borevich and Shafarevich, *Number Theory* Theorem 5.4.7.) If we let

$$u = \frac{\prod_{(\frac{b}{\ell})=1}(1-\zeta^b)}{\prod_{(\frac{b}{\ell})=-1}(1-\zeta^b)}$$

then this implies that

$$\frac{2h \log|\epsilon|}{\sqrt{\ell}} = -\frac{g(\chi)}{\ell} \log|u| = -\frac{1}{\sqrt{\ell}} \log|u|$$

Cancellation implies that

$$2h \log|\epsilon| = -\log|u|$$

and exponentiation yields

$$u = \pm\epsilon^{-2h}$$

Example. Let $k = \mathbb{Q}(\sqrt{-\ell})$ where ℓ is a positive prime such that $\ell \equiv 3 \pmod 4$. Then

$$\begin{aligned}\mathrm{Res}_{s=1}\zeta_k(s) = \frac{2\pi h}{w\sqrt{\ell}} = L(\chi, 1) &= \frac{\pi i g(\chi)}{\ell} \sum_{b=1}^{\ell} \chi(b)(\tfrac{b}{\ell} - \tfrac{1}{2}) \\ &= \frac{\pi i g(\chi)}{\ell}\Big(\sum_{b=1}^{\ell}\chi(b)(b/\ell) - \sum_{b=1}^{\ell}\chi(b)(1/2)\Big) = \frac{\pi i g(\chi)}{\ell}\sum_{b=1}^{\ell}\chi(b)(b/\ell)\end{aligned}$$

as

$$\sum_{b=1}^{\ell}\chi(b)(1/2) = \frac{1}{2}\sum_{b=1}^{\ell}\chi(b) = 0$$

Here $\chi(b) = (\frac{b}{\ell})$ as above, and $g(\chi)^2 = -\ell$ so that $g(\chi) = \pm i\sqrt{\ell}$. In fact, $g(\chi) = +i\sqrt{\ell}$, so

$$\frac{ig(\chi)}{\ell} = -\frac{1}{\sqrt{\ell}}$$

and therefore

$$\frac{2h}{w} = -\sum_{b=1}^{\ell} \chi(b)(b/\ell)$$

It should be noted that $w = 2$ unless $\ell = 3$.

Example. Let $k = \mathbb{Q}(i)$. We can recover the fact that the class number of k is $h = 1$ from the ideas above. Let $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$ be the character described in Theorem 65, so that $\zeta_k(s) = \zeta(s)L(\chi, s)$. By Corollary 66,

$$L(\chi, 1) = \frac{2\pi h}{w\sqrt{|d|}} = \frac{\pi h}{4}$$

By definition

$$L(\chi, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots$$

which lies between 1 and 2/3. It follows that $h = 1$.

Proposition 70. *Let ℓ be an odd prime number, $\zeta = \zeta_\ell$ a primitive ℓth root of unity, and $k = \mathbb{Q}(\zeta)$. Then*

$$\zeta_k(s) = \zeta(s) \prod_{\chi \neq 1} L(\chi, s)$$

where the product is taken over all nontrivial characters $\chi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mathbb{C}^\times$.

Proof. The Euler products of each function show that the desired equation is

$$\prod_p \prod_{P|p} (1 - \mathbb{N}(P)^{-s})^{-1} = \prod_p (1 - p^{-s}) \prod_{\chi \neq 1} \prod_{p \neq \ell} (1 - \chi(p)p^{-s})^{-1}$$

and we check equality factor-by-factor at each prime. The prime ℓ is completely ramified, so that $\ell A = P^{\ell-1}$ and $\mathbb{N}(P) = \ell$. In the infinite product on the left, this contributes a factor of $(1 - \ell^{-s})^{-1}$. In the factorization of $\zeta_k(s)$ we have a factor of $(1 - \ell^{-s})^{-1}$ contributed by ℓ, and no factor contributed to any of the $L(\chi, s)$. Thus, "over ℓ" the left and right-hand sides agree.

Let $p \neq \ell$, so that p is unramified. Then $pA = P_1 \cdots P_g$, and $\mathbb{N}(P_i) = p^f$ where f is the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. In particular, $g = \frac{\ell-1}{f}$. In $\zeta_k(s)$, p contributes factors

$$\prod_{i=1}^{g} (1 - p^{-fs})^{-1} = ((1 - p^{-fs})^{(\ell-1)/f})^{-1}$$

On the right-hand side of the desired equation, p contributes

$$(1-p^{-s})^{-1}\prod_{\chi\neq 1}(1-\chi(p)p^{-s})^{-1}$$

and we want to know that these expressions are equal. Let $X = p^{-s}$. Then the desired equality is

$$(1-X^f)^{(\ell-1)/f} = \prod_{\text{all }\chi}(1-\chi(p)X)$$

which we shall show is an identity on polynomials. We note that the zeroes of each side are fth roots of unity, so this is reasonable. The subgroup $\langle p\rangle \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times$ has order f. Let G denote the quotient $(\mathbb{Z}/\ell\mathbb{Z})^\times/\langle p\rangle$, which has order $g = \frac{\ell-1}{f}$. The short exact sequence

$$1 \to \langle p\rangle \to (\mathbb{Z}/\ell\mathbb{Z})^\times \to G \to 1$$

implies that the right-hand side of the desired equality is

$$\prod_{\substack{\text{all chars.}\\ \chi \text{ of } (\mathbb{Z}/\ell\mathbb{Z})^\times}}(1-\chi(p)X) = \prod_{\substack{\text{all chars.}\\ \psi \text{ of } \langle p\rangle}}(1-\psi(p)X)^{(\ell-1)/f}$$

and the factorization of cyclotomic polynomials implies that this is exactly the left-hand side of the desired equality. ☐

Next, we have some consequences of the proposition.

Corollary 71. *For nontrivial characters $\chi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mathbb{C}^\times$, $L(\chi, 1) \neq 0$.*

Proof. Immediate from the proposition, as $L(\chi, s)$ is regular at $s = 0$, and the fact that $\zeta_k(s)$ and $\zeta(s)$ both have simple pole at $s = 1$. ☐

Corollary 72. *(Dirichlet) If $\ell \nmid a$, then there are infinitely many prime numbers p such that $p \equiv a \pmod{\ell}$.*

This is the statement that there are infinitely many primes in an arithmetic progression modulo ℓ. Before we prove the corollary, we need a pair of lemmas.

Lemma 73. *For a nontrivial character χ, the function*

$$f_\chi(s) = \sum_{p\neq\ell}\frac{\chi(p)}{p^s}$$

is bounded as $s \to 1$.

Proof. For $\mathrm{Re}(s) > 1$, the power series expansion of $\log(1-x)$ implies that

$$\log(L(\chi, s)) = \log\Big(\prod_{p\neq\ell}\Big(1-\frac{\chi(p)}{p^s}\Big)^{-1}\Big) = \sum_{p\neq\ell}\sum_{n\geq 1}\frac{\chi(p)^n}{np^{ns}}$$

The rest of the proof is similar to that of Corollary 56. ☐

Definition. Let G be a finite abelian group and fix $g \in G$. Define the characteristic function of g, $\mathrm{char}(g) : G \to \mathbb{C}$, as $g \mapsto 1$ and $h \mapsto 0$ for $h \neq g$.

Lemma 74. *The characteristic function of g can be described by the formula*

$$char(g) = \frac{1}{\#G} \sum_{all\ \chi} \overline{\chi}(g)\chi$$

Proof of Lemma 74. For $h \in G$

$$\mathrm{char}(g)(h) = \frac{1}{\#G} \sum_{\text{all } \chi} \overline{\chi}(g)\chi(h) = \frac{1}{\#G} \sum_{\text{all } \chi} \chi(h/g)$$

If $h = g$, then this is

$$\mathrm{char}(g)(g) = \frac{1}{\#G} \sum_{\text{all } \chi} \chi(1) = 1$$

since the number of characters of G is exactly $\#G$. If $h \neq g$, then $h/g \neq 1$ and there exists a fixed character χ' of G such that $\chi'(h/g) \neq 1$ (c.f. Borevich and Shafarevich *Number Theory*, p. 417), and of course $\chi'(h/g) \neq 0$. As χ runs through all characters of G, so does $\chi'\chi$, so that

$$\sum_{\text{all } \chi} \chi(h/g) = \sum_{\text{all } \chi} \chi'(h/g)\chi(h/g) = \chi'(h/g) \sum_{\text{all } \chi} \chi(h/g)$$

which implies that the sum is zero. □

Proof of Corollary 72. In the notation of the lemmas, let $G = (\mathbb{Z}/\ell\mathbb{Z})^\times$. Then

$$\begin{aligned}\frac{1}{\ell - 1} \sum_{\text{all } \chi} \overline{\chi}(a) f_\chi(s) &= \frac{1}{\#G} \sum_{\text{all } \chi} \overline{\chi}(a) \sum_{p \neq \ell} \frac{\chi(p)}{p^s} = \sum_{p \neq \ell} \frac{1}{p^s} \frac{1}{\#G} \sum_{\text{all } \chi} \overline{\chi}(a)\chi(p) \\ &= \sum_{p \neq \ell} \frac{1}{p^s} \mathrm{char}(a)(p) = \sum_{p \equiv a (\mathrm{mod}\ \ell)} \frac{1}{p^s}\end{aligned}$$

For each $\chi \neq 1$, $f_\chi(s)$ is bounded as $s \to 1$, and $f_1(s) \sim \log(\frac{1}{s-1})$. Thus, up to a bounded function

$$\sum_{p \equiv a (\mathrm{mod}\ \ell)} \frac{1}{p^s} \sim \frac{1}{\ell - 1} \log\Big(\frac{1}{s-1}\Big)$$

as $s \to 1$, which implies that $\sum_{p \equiv a} \frac{1}{p}$ is infinite. In particular, the number of terms in the sum must be infinite, as desired. □

Notice that the proof of the corollary gives us a stronger result. Up to a bounded function

$$\sum_{p \equiv a (\mathrm{mod}\ \ell)} \frac{1}{p^s} \sim \frac{1}{\ell - 1} \log\Big(\frac{1}{s-1}\Big)$$

as $s \to 1$. This says that the density of such primes is $1/(\ell - 1)$.

Corollary 75. *(Kummer's Class Number Formula) For the cyclotomic field $k = \mathbb{Q}(\zeta_\ell)$*

$$\Big(\prod_{\chi\ odd} \frac{\pi i g(\chi)}{\ell} B_{1,\overline{\chi}}\Big) \cdot \Big(\prod_{\substack{\chi\ even \\ \chi \neq 1}} \frac{-g(\chi)}{\ell} \sum_{b=1}^{\ell} \overline{\chi}(b) \log|1-\zeta^b|\Big) = \frac{(2\pi)^{(\ell-1)/2}}{\ell^{(\ell-2)/2}} \cdot \frac{hR}{2\ell}$$

Proof. The right-hand side of the desired equality is

$$\mathrm{Res}_{s=1}\zeta_k(s) = \mathrm{Res}_{s=1}\Big(\zeta(s)\prod_{\chi\neq 1} L(\chi,s)\Big) = \mathrm{Res}_{s=1}\Big(\prod_{\text{all }\chi} L(\chi,s)\Big)$$

which is the left-hand side by Theorem 61. □

Lecture 15

We define the gamma function

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$$

for $\mathrm{Re}(s) > 0$. By integrating by parts, we see that $\Gamma(s)$ satisfies the functional equation $\Gamma(s+1) = s\Gamma(s)$. Thus, for $\mathrm{Re}(s) > -1$, we may define

$$\Gamma(s) = \frac{\Gamma(s+1)}{s}$$

to obtain a meromorphic continuation to the region $\mathrm{Re}(s) > -1$, with simple pole at $s = 0$. We may continue this process inductively to obtain a meromorphic continuation to all of $\mathbb{C}$ with only simple poles located at $s = 0, -1, -2, \dots$. Note that $\Gamma(1) = 1$, so that $\Gamma(m) = (m-1)!$ for $m = 1, 2, 3, \dots$.

Theorem 76. *(Hecke's Thesis) Let k be a number field.*

1. *$\zeta_k(s)$ has a meromorphic continuation all of $\mathbb{C}$, with a unique pole at $s = 1$ which is simple.*
2. *If we define*

   $$\xi_k(s) = \zeta_k(s)(\pi^{-s/2}\Gamma(s/2))^{r_1}((2\pi)^{-s}\Gamma(s))^{r_2}$$

   then $\xi_k(s)$ has a meromorphic continuation to all of $\mathbb{C}$, with unique poles at $s = 0, 1$ which are simple. Furthermore, $\xi_k(s)$ satisfies the functional equation

   $$\xi_k(s) = |d|^{\frac{1}{2}-s}\xi_k(1-s)$$

   where d is the discriminant of k.

For a complete proof, see Weil *Basic Number Theory*, Chapter VII. We shall continue with these ideas below. First, we give some motivation for the Gamma factors in this product by considering curves over finite fields.

Let $\mathbb{F}_q$ denote the finite field with $q = p^m$ elements, and let X be a complete, nonsingular curve over $\mathbb{F}_q$. Let $k = \mathbb{F}_q(X)$ be the field of rational functions on X, and let $A \subset k$ be the integral domain of functions regular outside a single place ∞. We define the zeta function of A as

$$\zeta_A(s) = \sum_{I \subseteq A} \frac{1}{\mathbb{N}(I)^s} = \prod_{\substack{P \subseteq A \\ P \neq 0}} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1}$$

for $\mathrm{Re}(s) > 1$, where the product is taken over all nonzero prime ideals of A.

For example, if $X = \mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}_q}$, then $k = \mathbb{F}_q(X) = \mathbb{F}_q(t) \supset \mathbb{F}_q[t] = A$. The nonzero prime ideals P of A are in bijection with the collection of irreducible, monic polynomials $f(t)$ over $\mathbb{F}_q$. Under this correspondence, if $f(t)$ has degree d, then $\mathbb{N}(P) = q^d$. Since $\mathbb{F}_q$ sits inside A/P for every such prime, we see that every P has characteristic p. (This is true in general, of course.) Furthermore, $A^\times = \mathbb{F}_q^\times$.

If q is odd and X is an elliptic curve, say given by the equation $y^2 = x^3 + Ax + B$, then

$$A = \mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B)$$

and $k = \mathbb{F}_q(X)$ is the quotient field of A.

Let X, k and A be as above. Since $\mathbb{F}_q \hookrightarrow A \subseteq K$, A has characteristic p. For every prime ideal P, $\mathbb{N}(P) = q^d$ for some positive integer d, which we call the *degree* of P and denote by $d = \deg(P)$. We define the expression $Z_A(T)$ by

$$Z_A(T) = \prod_{P \neq 0} (1 - T^{\deg(P)})^{-1}$$

and note that, by definition, $\zeta_A(s) = Z_A(q^{-s})$. As in the number field situation, we can use P to define a valuation on k by

$$|\alpha|_P = \mathbb{N}(P)^{-\operatorname{ord}_P(\alpha)}$$

For a valuation v on k, let A_v denote the ring of elements α of k such that $v(\alpha) \leq 1$. Then A_v is a local ring with maximal ideal equal to the set of elements α of k such that $v(\alpha) < 1$. In addition, A_v is a discrete valuation ring so that the maximal ideal is principal, generated by a uniformizing parameter which we denote by π_v. The degree of v is defined to be the dimension of the quotient $A_v/\pi_v A_v$ over $\mathbb{F}_q$, and this is exactly the degree of the prime ideal P which induced v. We define the complete zeta function of X

$$Z_X(T) = \prod_v (1 - T^{\deg(v)})^{-1} = Z_A(T)(1 - T^{\deg(\infty)})^{-1}$$

by using *all* the valuations of k, including the valuation at ∞, which does not correspond to a prime ideal of A. Using the power series $-\log(1 - x) = \sum_{n \geq 1} \frac{x^n}{n}$, which holds for $|x| < 1$, we see that in $\mathbb{Q}[\![T]\!]$

$$\log(Z_X(T)) = \sum_v \sum_{n \geq 1} \frac{T^{n \deg(v)}}{n} = \sum_v \sum_{n \geq 1} \frac{\deg(v) T^{n \deg(v)}}{n \deg(v)} = \sum_{n \geq 1} \frac{T^n}{n} A_n$$

where

$$A_n = \sum_{\deg(v)|n} \deg(v) \in \mathbb{Z}$$

A prime ideal P is determined by an orbit of the action of $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on sets of points of $\overline{X} = X(\overline{\mathbb{F}}_q)$ (the points of X defined over $\overline{\mathbb{F}}_q$) and the degree of P is the number of elements in the orbit. Fix a point x of X. G acts on $\overline{X}$ and therefore determines an orbit of x. The orbit is finite and appears as a set of points in $X(\mathbb{F}_{q^m})$ for some m. The sum $d = \sum_{\sigma \in G} x^\sigma$ is a prime divisor on X and therefore determines a prime ideal of A. It follows that $A_n = \#X(\mathbb{F}_{q^n})$ and so

$$\log(Z_X(T)) = \sum_{n \geq 1} \frac{T^n}{n}(\#X(\mathbb{F}_{q^n}))$$

Exponentiation yields the equation

$$Z_X(T) = \exp\Big(\sum_{n \geq 1} \frac{T^n}{n}(\#X(\mathbb{F}_{q^n}))\Big)$$

For example, if $X = \mathbb{P}^1$, then $\#X(\mathbb{F}_{q^n}) = q^n + 1$ and

$$\begin{aligned}\log(Z_X(T)) &= \sum_{n \geq 1} \frac{(q^n+1)T^n}{n} = \sum \frac{T^n}{n} + \sum \frac{(qT)^n}{n} \\ &= \log(1-T)^{-1} + \log(1-qT)^{-1} = \log\Big(\frac{1}{(1-T)(1-qT)}\Big)\end{aligned}$$

so that

$$Z_{\mathbb{P}^1}(T) = \frac{1}{(1-T)(1-qT)}$$

and the substitution $T = q^{-s}$ implies that

$$\zeta_X(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$$

Notice that this is a rational function in q^{-s}, which is meromorphic with poles only where $q^{-s} = 1$ and $q^{1-s} = 1$. This is similar to Theorem 76.

In general, $Z_X(T) = \frac{P(T)}{(1-T)(1-qT)}$, where $P(T)$ is a polynomial in T with integer coefficients having degree $2g$ where g is the genus of X. More specifically,

$$P(T) = 1 + \cdots + q^g T^{2g} = \prod_{i=1}^{2g}(1 - \alpha_i T)$$

for some algebraic integers α_i, and we may write

$$\begin{aligned}\exp\Big(\sum_{n \geq 1} \frac{T^n}{n}(\#X(\mathbb{F}_{q^n}))\Big) &= Z_X(T) = \exp\Big(\sum_{n \geq 1} \frac{\#X(\mathbb{F}_{q^n})T^n}{n}\Big) \\ &= \exp\Big(\#X(\mathbb{F}_q)T + \#X(\mathbb{F}_{q^2})\frac{T^2}{2} + \cdots\Big)\end{aligned}$$

If X is an elliptic curve, then $P(T) = 1 - aT + qT^2$ since $g_X = 1$. The only unknown coefficient is a. In fact, $a = 1 + q - \#X(\mathbb{F}_q)$, as can easily be verified by checking the coefficient of T in $Z_X(T)$.

Now, we return to the case where k is a number field. The definition of $\xi_k(s)$ may be restated, as follows. Every valuation v on k corresponds to a factor $\zeta_v(s)$ in the Euler product of $\xi_k(s)$. For the finite valuations (those corresponding to nonzero prime ideals of A) $\zeta_v(s) = (1 - \mathbb{N}(P)^{-s})^{-1}$, which is exactly the factor of $\zeta_k(s)$ corresponding to P. For a valuation arising from a real place, $\zeta_v(s) = \pi^{-s/2}\Gamma(s/2)$, which is meromorphic in $\mathbb{C}$ with (simple) poles at $s = 0, -2, -4, \ldots$. For a valuation arising from a complex place, $\zeta_v(s) = (2\pi)^{-s}\Gamma(s)$, which is meromorphic in $\mathbb{C}$ with (simple) poles at $s = 0, -1, -2, \ldots$.

We shall prove part of Theorem 76 for the case $k = \mathbb{Q}$. In this case, $d = 1$, $r_1 = 1$ and $r_2 = 0$. As with the zeta function of $\mathbb{Q}$, we denote $\xi_{\mathbb{Q}}(s)$ as $\xi(s)$.

Theorem 77. *The function*

$$\xi(s) = \zeta(s)\pi^{-s/2}\Gamma(s/2)$$

has a meromorphic continuation to all of $\mathbb{C}$ *with simple poles at* $s = 0, 1$. *Furthermore,* $\xi(s)$ *satisfies the functional equation* $\xi(1-s) = \xi(s)$.

Proof. For a fixed positive integer, we make the substitution $t = n^2\pi x$ into the definition of $\Gamma(s/2)$. Here, $\frac{dt}{t} = \frac{dx}{x}$ so that

$$\begin{aligned}
\Gamma(s/2) &= \int_0^\infty t^{s/2} e^{-t} \frac{dt}{t} \\
&= \int_0^\infty (n^2\pi x)^{s/2} e^{-n^2\pi x} \frac{dx}{x} \\
&= \int_0^\infty n^s \pi^{s/2} x^{s/2} e^{-n^2\pi x} \frac{dx}{x} \\
n^{-s}\pi^{-s/2}\Gamma(s/2) &= \int_0^\infty x^{s/2} e^{-n^2\pi x} \frac{dx}{x}
\end{aligned}$$

and summing over all $n \geq 1$ yields

$$\begin{aligned}
\xi(s) &= \zeta(s)\pi^{-s/2}\Gamma(s/2) \\
&= \pi^{-s/2}\Gamma(s/2) \sum_n \frac{1}{n^s} \\
&= \sum_{n\geq 1} \pi^{-s/2}\Gamma(s/2) n^{-s} \\
&= \sum_{n\geq 1} \int_0^\infty x^{s/2} e^{-n^2\pi x} \frac{dx}{x}
\end{aligned}$$

which converges absolutely for $\mathrm{Re}(s) > 1$, so we may interchange the sum and integral

$$\xi(s) = \int_0^\infty x^{s/2} \Big(\sum_{n\geq 1} e^{-n^2\pi x} \Big) \frac{dx}{x}$$

Let $\omega(x) = \sum_{n\geq 1} e^{-n^2\pi x}$.

Here, we introduce Jacobi's theta function. For $x > 0$, let

$$\theta(x) = \sum_{n\in\mathbb{Z}} e^{-n^2\pi x} = 1 + 2\omega(x)$$

If we write $f(t) = e^{-t^2\pi x}$ and let $\hat{f}(t)$ denote the Fourier transform of f, then by the Poisson summation formula

$$\theta(x) = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n)$$

Furthermore, the identity

$$\hat{f}(t) = \frac{e^{-t^2\pi/x}}{x^{1/2}}$$

implies that

$$\theta(x) = \sum_{n\in\mathbb{Z}} \hat{f}(n) = \frac{\theta(x^{-1})}{x^{1/2}} \tag{11}$$

which is Jacobi's famous theta identity. Thus,

$$\begin{aligned}\xi(s) &= \int_0^\infty x^{s/2}\omega(x)\frac{dx}{x}\\ &= \int_0^1 x^{s/2}\omega(x)\frac{dx}{x} + \int_1^\infty x^{s/2}\omega(x)\frac{dx}{x}\end{aligned}$$

we substitute $x \mapsto x^{-1}$ into the first integral

$$= \int_1^\infty x^{-s/2}\omega(x^{-1})\frac{dx}{x} + \int_1^\infty x^{s/2}\omega(x)\frac{dx}{x}$$

The fact that $\omega(x) = \frac{1}{2}(\theta(x) - 1)$ implies that

$$\omega(x^{-1}) = \frac{1}{2}(\theta(x^{-1}) - 1) = \frac{1}{2}(x^{1/2}\theta(x) - 1) = x^{1/2}\omega(x) - \frac{1}{2} + \frac{x^{1/2}}{2}$$

so that

$$\begin{aligned}\xi(s) &= \int_1^\infty x^{1/2}\omega(x)x^{-s/2}\frac{dx}{x} + \int_1^\infty x^{s/2}\omega(x)\frac{dx}{x}\\ &\quad - \frac{1}{2}\int_1^\infty x^{s/2}\frac{dx}{x} + \frac{1}{2}\int_1^\infty x^{1/2-s/2}\frac{dx}{x}\\ &= \int_1^\infty (x^{(1-s)/2} + x^{s/2})\omega(x)\frac{dx}{x} - \frac{1}{s} + \frac{1}{s-1}\\ &= \frac{1}{s(s-1)} + \int_1^\infty (x^{(1-s)/2} + x^{s/2})\omega(x)\frac{dx}{x}\end{aligned}$$

To see that $\xi(s)$ has the proper meromorphic continuation, it suffices to show that the final integral has an *analytic* continuation to all of $\mathbb{C}$. The essential fact is that, as $x \to \infty$, $\omega(x)$ decays exponentially so the integral converges. To see that $\xi(s)$ satisfies the desired functional equation, we simply observe that if we replace s by $1 - s$ in the final expression for $\xi(s)$, it remains the same. $\square$

Lecture 16

Next, we will discuss the analytic continuation of $L(\chi, s)$ and a functional equation satisfied by $L(\chi, s)$. Let $\tau = x + yi$ be a complex number with $y > 0$, and let $q = e^{\pi i \tau}$. We define a function $\Theta(\tau)$ similar to Jacobi's theta function, as

$$\Theta(\tau) = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau} = \sum_{n \in \mathbb{Z}} q^{n^2}$$

It readily follows from the definitions that $\Theta(iy) = \theta(y)$.

Example. Let $k = \mathbb{Q}(i)$. Then $A = \mathbb{Z}[i]$ and

$$\zeta_k(s) = \sum_{\substack{\mathfrak{a} \subseteq A \\ \mathfrak{a} = (a+bi)}} \frac{1}{\mathbb{N}(\mathfrak{a})^s} = \frac{1}{4} \sum_{(a,b) \neq (0,0)} \frac{1}{(a^2+b^2)^s}$$

as $\mathbb{N}(\mathfrak{a}) = a^2 + b^2$. If we define $f(\tau)$ as

$$f(\tau) = \sum_{(a,b)} q^{a^2+b^2} = (\Theta(\tau))^2$$

then f satisfies an equation similar to the equation satisfied by θ: $f(iy) = \frac{1}{y} f(iy^{-1})$.

Assume that $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$ is a primitive character. In order to uncover the functional equations for $L(\chi, s)$ we introduce functions $\xi(\chi, s)$ as we did for $\zeta_k(s)$. There are two cases.

If χ is even, then we define

$$\xi(\chi, s) = \pi^{-s/2} \Gamma(s/2) L(\chi, s) f^{s/2}$$

In this case, let $w_\chi = g(\chi)/\sqrt{f}$, where $g(\chi)$ is the Gauss sum from Lecture 13. Then $|w_\chi| = 1$ and $\xi(\chi, s)$ has a holomorphic continuation to all of $\mathbb{C}$ which satisfies the functional equation

$$\xi(\chi, s) = w_\chi \xi(\overline{\chi}, 1 - s)$$

If χ is odd, then we define

$$\xi(\chi, s) = \pi^{-(s+1)/2} \Gamma((s+1)/2) L(\chi, s) f^{s/2}$$

Let $w_\chi = g(\chi)/i\sqrt{f}$. Again $|w_\chi| = 1$ and $\xi(\chi, s)$ satisfies the functional equation

$$\xi(\chi, s) = w_\chi \xi(\overline{\chi}, 1 - s)$$

If $\chi^2 = 1$, then we say that χ is a *quadratic* character. In this case $\overline{\chi} = \chi$ and it can be shown that

$$g(\chi) = \begin{cases} \sqrt{f} & \text{if } \chi \text{ is even} \\ i\sqrt{f} & \text{if } \chi \text{ is odd} \end{cases}$$

(c.f., Borevich and Shafarevich *Number Theory*, Theorem 5.4.7) so that $w_\chi = 1$. Thus, the simpler functional equation

$$\xi(\chi, s) = \xi(\chi, 1 - s)$$

is satisfied. We shall only prove that χ satisfies the desired functional equation when χ is an even character. First, however, we note that there are ways of slightly changing the functions $\xi_k(s)$ to get the same meromorphic continuation properties and simpler functional equations.

For example, assume that k is a quadratic field, with character χ as is Theorem 65. It can be shown that k is real if and only if χ is even (c.f., Borevich and Shafarevich *Number Theory*, Chapter 5,SS4). Furthermore, it can be shown that every quadratic character $(\mathbb{Z}/f\mathbb{Z})^\times \to \{\pm 1\}$ corresponds to a quadratic field in this manner. If k is a real field, then we define

$$\xi_k^*(s) = (\pi^{-s/2}\Gamma(s/2))^2 f^{s/2}\zeta_k(s)$$

which is very similar to the definition of $\xi_k(s)$. It is straightforward to check that $\xi_k(s)$ satisfies the functional equation

$$\xi_k(s) = |d|^{\frac{1}{2}-s}\xi_k(1-s)$$

if and only if $\xi_k^*(s)$ satisfies the functional equation

$$\xi_k^*(s) = \xi_k^*(1-s)$$

which is simpler. To see that this second equation is satisfied, notice that the definitions of $\xi_k^*(s)$, $\xi(s)$ and $\xi(\chi, s)$ imply that

$$\xi_k^*(s) = \xi(s)\xi(\chi, s)$$

In the quadratic case, $\xi(\chi, s) = \xi(\chi, 1-s)$ and by Theorem 77, $\xi(1-s) = \xi(s)$. Thus,

$$\xi_k^*(s) = \xi(s)\xi(\chi, s) = \xi(1-s)\xi(\chi, 1-s) = \xi_k^*(1-s)$$

as desired. A similar change works for the case when k is imaginary.

Before we prove the real case, we need some notation and a lemma. Let g be an element of the real Schwarz space, so that g is C^∞, and g and all its derivatives decrease rapidly at ∞. The Fourier transform of g, denoted $\hat{g}$, is given by

$$\hat{g}(y) = \int_{\mathbb{R}} g(x)e^{-2\pi ixy}dx = \int_{\mathbb{R}} g(x)\overline{\langle x, y\rangle}, dx$$

where $\langle x, y\rangle = e^{2\pi ixy}$. (The assumption that g is in the real Schwarz space implies that we may take iterated Fourier transforms of g.) Define $\Theta_g(t; x, y)$ as

$$\Theta_g(t; x, y) = \sum_{n\in\mathbb{Z}} g((x+n)t)\langle y, n\rangle$$

It is immediate from this definition that $\Theta_g(t; 0, 0) = \sum_n g(nt)$.

Lemma 78. *(Generalized Jacobi Identity)*

$$\Theta_g(t; x, y) = \frac{\overline{\langle x, y\rangle}}{t}\Theta_{\hat{g}}(t^{-1}; -y, x)$$

Proof. To simplify notation, let $G(w) = g((x+w)t)\langle y, w\rangle$. Then by the Poisson summation formula

$$\Theta_g = \sum_{n\in\mathbb{Z}} G(n) = \sum_{n\in\mathbb{Z}} \hat{G}(n)$$

so we calculate $\hat{G}$. By definition

$$\begin{aligned}\hat{G}(u) &= \int_{\mathbb{R}} g((x+w)t)\langle y, w\rangle\overline{\langle u, w\rangle}\, dw \\ &= \int_{\mathbb{R}} g((x+w)t)\overline{\langle u-y, w\rangle}\, dw\end{aligned}$$

and we make the substitution $z = (x+w)t$ so that $w = \frac{z}{t} - x$, $dw = \frac{dz}{t}$ and

$$\begin{aligned}\hat{G}(u) &= \int_{\mathbb{R}} g(z)\overline{\left\langle u-y, \frac{z}{t} - x\right\rangle}\, \frac{dz}{t} \\ &= \frac{1}{t}\overline{\langle x, y\rangle}\langle u, x\rangle \int_{\mathbb{R}} g(z)\overline{\left\langle z, \frac{u-v}{t} - x\right\rangle}\, dz \\ &= \frac{\overline{\langle x, y\rangle}\langle u, x\rangle}{t}\hat{g}\Big(\frac{u-y}{t}\Big)\end{aligned}$$

Substituting $u = n$ and summing over all n yields

$$\begin{aligned}\Theta_g(t; x, y) &= \sum_{n\in\mathbb{Z}} \hat{G}(n) = \sum_{n} \frac{\overline{\langle x, y\rangle}\langle n, x\rangle}{t}\hat{g}\Big(\frac{n-y}{t}\Big) \\ &= \frac{\overline{\langle x, y\rangle}}{t}\sum_{n}\langle n, x\rangle\hat{g}\Big(\frac{n-y}{t}\Big) = \frac{\overline{\langle x, y\rangle}}{t}\Theta_{\hat{g}}(t^{-1}; -y, x)\end{aligned}$$

as desired. $\square$

Corollary 79. *For real numbers y and t*

$$\sum_{n\in\mathbb{Z}} e^{(-\pi n^2 t + 2\pi i n y)} = \frac{1}{\sqrt{t}}\sum_{n\in\mathbb{Z}} e^{-\pi(ny)^2/t}$$

Proof. Let $g(\alpha) = e^{-\pi\alpha^2}$. Then it is a standard fact that $\hat{g} = g$, and Lemma 78 implies that

$$\begin{aligned}\sum_{n\in\mathbb{Z}} e^{(-\pi n^2 t + 2\pi i n y)} &= \Theta_g(\sqrt{t}; 0, y) \\ &= \frac{\overline{\langle 0, y\rangle}}{\sqrt{t}}\Theta_{\hat{g}}(t^{-1/2}; -y, 0) \\ &= \frac{\overline{\langle 0, y\rangle}}{\sqrt{t}}\Theta_{g}(t^{-1/2}; -y, 0) \\ &= \frac{1}{\sqrt{t}}\sum_{n\in\mathbb{Z}} e^{-\pi(ny)^2/t}\end{aligned}$$

as desired. $\square$

Theorem 80. *Assume that* $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \{\pm 1\}$ *is a primitive, even character. Let*

$$\xi(\chi, s) = \pi^{-s/2}\Gamma(s/2)L(\chi, s)f^{s/2}$$

and let $w_\chi = g(\chi)/\sqrt{f}$*, where* $g(\chi)$ *is the Gauss sum. Then* $\xi(\chi, s)$ *has a holomorphic continuation to all of* $\mathbb{C}$*, and satisfies the functional equation*

$$\xi(\chi, s) = w_\chi \xi(\overline{\chi}, 1 - s)$$

Proof. Start with the identity

$$f^{s/2}\pi^{-s/2}\Gamma(s/2)n^{-s} = \int_0^\infty e^{-\pi n^2 x/f} x^{s/2} \frac{dx}{x}$$

which is proved as in the proof of Theorem 77. Let

$$\theta_\chi(x) = \sum_{n \in \mathbb{Z}} \chi(n) e^{-\pi n^2 x/f}$$

so that, when we sum over all $n \geq 1$ we have

$$\begin{aligned}
\xi(\chi, s) &= \pi^{-s/2}\Gamma(s/2)L(\chi, s)f^{s/2} \\
&= \sum_{n \geq 1} \chi(n) n^{-s} \pi^{-s/2}\Gamma(s/2) f^{s/2} \\
&= \int_0^\infty x^{s/2} \Big(\sum_{n \geq 1} \chi(n) e^{-\pi n^2 x/f}\Big) \frac{dx}{x} \\
&= \int_0^\infty x^{s/2} \Big(\frac{1}{2}\theta_\chi(x)\Big) \frac{dx}{x}
\end{aligned}$$

as $\chi(-n) = \chi(n)$ and $\chi(0) = 0$

$$= \frac{1}{2}\Big(\int_0^1 x^{s/2}\theta_\chi(x)\frac{dx}{x} + \int_1^\infty x^{s/2}\theta_\chi(x)\frac{dx}{x}\Big) \tag{12}$$

The first integral converges for $\mathrm{Re}(s) > 0$, while the second converges for all s. To obtain the desired properties, we need to find an equation relating $\theta_\chi(x)$ to $\theta_\chi(x^{-1})$.

By Lemma 68,

$$\chi(n) g(\overline{\chi}) = \sum_{b=1}^{f} \overline{\chi}(b) e^{2\pi i b n/f}$$

so that

$$\begin{aligned}
g(\overline{\chi})\theta_\chi(x) &= \sum_{n \in \mathbb{Z}} \Big(\sum_{b=1}^{f} \overline{\chi}(b) e^{2\pi i b n/f}\Big) e^{-\pi n^2 x/f} \\
&= \sum_{b=1}^{f} \overline{\chi}(b) \Big(\sum_{n \in \mathbb{Z}} e^{(-\pi n^2 x/f) + (2\pi i b n/f)}\Big)
\end{aligned}$$

and the substitutions $t = x/f$ and $y = b/f$ yield

$$= \sum_{b=1}^{f} \overline{\chi}(b) \Big(\frac{1}{\sqrt{x/f}} \sum_{n \in \mathbb{Z}} e^{-\pi (n+b/f)^2 f^2/(xf)} \Big)$$

$$= \sqrt{\frac{f}{x}} \sum_{b=1}^{f} \overline{\chi}(b) \sum_{n \in \mathbb{Z}} e^{-\pi (nf+b)^2/(xf)}$$

and the replacement $m = nf + b$ gives

$$= \sqrt{\frac{f}{x}} \sum_{n \in \mathbb{Z}} \overline{\chi}(m) e^{-\pi m^2/(fx)}$$

$$= \sqrt{\frac{f}{x}} \theta_{\overline{\chi}}(x^{-1})$$

If we substitute this final expression into (12), we find

$$\xi(\chi, s) = \frac{1}{2} \Big(\int_1^\infty x^{(1-s)/2} \frac{\sqrt{f}}{g(\overline{\chi})} \theta_{\overline{\chi}}(x) \frac{dx}{x} + \int_1^\infty x^{s/2} \theta_\chi(x) \frac{dx}{x} \Big)$$

which gives our analytic continuation. Furthermore, the substitution $s \mapsto 1 - s$ gives the desired functional equation. $\square$

We have shown that $\zeta_k(s)$ has order of vanishing -1 at $s = 1$ and residue

$$\mathrm{Res}_{s=1} \zeta_k(s) ds = \frac{2^{r_1} (2\pi)^{r_2}}{\sqrt{|d|}} \frac{hR}{w}$$

We shall use Hecke's functional equation for $\xi_k(s)$ to calculate the order of vanishing and residue at $s = 0$. By Theorem 76, we know that

$$\zeta_k(s) (\pi^{-s/2} \Gamma(s/2))^{r_1} ((2\pi)^{-s} \Gamma(s))^{r_2} = \xi_k(s) = |d|^{\frac{1}{2} - s} \xi_k(1 - s)$$

and that $\xi_k(s)$ has a simple pole (i.e., vanishing of order -1) at $s = 0$. Also, $\Gamma(s)$ has a simple pole at $s = 0$. Thus,

$$-1 = \mathrm{ord}_{s=0} \xi_k(s) = \mathrm{ord}_{s=0} \zeta_k(s) + r_1 \mathrm{ord}_{s=0} \Gamma(s) + r_2 \mathrm{ord}_{s=0} \Gamma(s) = \mathrm{ord}_{s=0} \zeta_k(s) - r_1 - r_2$$

so that

$$\mathrm{ord}_{s=0} \zeta_k(s) = r_1 + r_2 - 1 = \mathrm{rank}(A^\times)$$

and

$$\zeta_k(s) = c s^{r_1 + r_2 - 1} + O(s^{r_1 + r_2})$$

A further computation shows that $c = -\frac{hR}{w}$.

Lecture 17

In the final lectures, we shall give a basic treatment of Artin L functions to introduce the reader to the ideas behind Stark's Conjectures. For a very thorough treatment of these ideas, see Tate *Les conjectures de Stark sur les fonctions L d'Artin en s=O: notes d'un cours Orsay [de] John Tate*, Birkhäuser, Progress in Mathematics.

Let $\mathbb{Q} \subseteq k$ be a Galois extension of degree n with Galois group G which is necessarily finite of order n. Let A denote the ring of algebraic integers in k. G acts on A, so for every prime number p, G acts on A/pA. Therefore, G permutes the prime ideals P of A of characteristic p.

Proposition 81. *G permutes the primes P of characteristic p transitively.*

Proof. Fix a prime ideal P of A of characteristic p. Let $I = \prod_{P_i \neq P} P_i$ where the product is taken over all prime ideals P_i of characteristic p such that $P_i \neq P$. Since each prime ideal of characteristic p is maximal, we see that $P + I = A$. Fix $\alpha \in P$ and $\beta \in I$ such that $\alpha + \beta = 1$. It follows that $\alpha \notin P_i$ for any i. For any $\sigma \in G$, $\sigma(\alpha) \in \sigma(P)$ and if $P_i \neq \sigma(P)$ then $\sigma(\alpha) \notin P_i$. Now, $p\mathbb{Z} = P \cap \mathbb{Z}$ and this ideal contains $a = \mathbb{N}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. Thus, a is contained in exactly the primes P_i which are conjugate to P. Since $a \in p\mathbb{Z}$, we see that a lies in all the P_i, as desired. $\square$

Corollary 82. *In the prime factorization $pA = \prod_{i=1}^{g} P_i^{e_i}$, let $f_i = \deg(P_i) = (A/P_i : \mathbb{Z}/p\mathbb{Z})$. Then the e_i and f_i are independent of i and $n = efg$ where e and f denote the common value of e_i and f_i, respectively.*

Proof. The fact that the e_i and f_i are independent of i follows immediately from the fact that the P_i are all conjugate. The fact that $n = efg$ follows from the fact that the extension $\mathbb{Q} \subseteq k$ is Galois. $\square$

Corollary 83. *Let P be a fixed prime ideal of A dividing p. Let $G_P = \{\sigma \in G : \sigma(P) = P\}$ which is a subgroup of G of order ef. For an element τ of the coset space G/G_P, the ideal $P' = \tau(P)$ is a well-defined conjugate of P, and $G_{P'} = \tau G_P \tau^{-1}$ in G.*

Proof. This follows from the standard results regarding the transitive action of a group on a set. $\square$

With the notation of the corollary, we see that G_P acts on the finite field A/P since it stabilizes P. Let I_P denote the inertia subgroup, i.e., the kernel of this action. Then there is an exact sequence

$$1 \to I_P \to G_P \xrightarrow{\beta} \mathrm{Aut}(A/P)$$

by definition of I_P. Since A/P is finite of order p^f, the *Frobenius automorphism* $F : A/P \to A/P$ given by $\alpha \mapsto \alpha^p$ is a generator of $\mathrm{Aut}(A/P)$. Thus, $\mathrm{Aut}(A/P)$ is cyclic of order f.

Theorem 84. *The map β is surjective. Consequently, I_P has order e. In particular, if p does not divide the discriminant d_k of k, then I_P has order 1.*

Proof. We shall only prove the result under the additional hypotheses of Corollary 32, i.e., when $k = \mathbb{Q}(\alpha)$ with $\alpha \in A$ and p does not divide the index $(A : \mathbb{Z}[\alpha])$. By Corollary 32

$$A/pA = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = (\mathbb{Z}[x]/h(x))/p(\mathbb{Z}[x]/h(x)) = (\mathbb{Z}/p\mathbb{Z})[x]/\tilde{h}(x)$$

where $\tilde{h}(x)$ denotes the reduction of $h(x)$ modulo p. The irreducible factorization of $\tilde{h}(x)$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has the form

$$\tilde{h}(x) = \prod_{i=1}^{g} h_i(x)^e \tag{13}$$

where each $h_i(x)$ has degree f. Since every $\sigma(\alpha)$ satisfies $h(x)$, G permutes the zeroes of $h(x)$. G acts transitively on the zeroes: if α' is another root, then $k = \mathbb{Q}(\alpha')$ and the map $\alpha \mapsto \alpha'$ determines an element of G. Furthermore, G acts simply-transitively on the zeroes, that is, for each root α_i there exists a unique $\sigma \in G$ such that $\sigma(\alpha) = \alpha_i$. This follows from the fact that $h(x)$ has exactly n distinct zeroes where $n = (k : \mathbb{Q}) = \#(G)$, and G acts transitively on the zeroes.

There are $n = efg$ distinct zeroes of $h(x)$ over $\overline{\mathbb{Q}}$. The fact that $\mathbb{F}_p$ is perfect and the factorization 13 implies that there are exactly fg distinct zeroes of $\tilde{h}(x)$ over $\overline{\mathbb{F}}_p$, each of multiplicity e. By Corollary 32, the prime ideal P corresponds to one of the $h_i(x)$. Assume without loss of generality that P corresponds to $h_1(x)$. Let $\tilde{\alpha}_1$ denote the reduction modulo p of α to a zero of $h_1(x)$. For $\sigma \in G$, σ is an element of G_P if and only if $\sigma(\alpha)$ reduces to a zero of $h_1(x)$. Also, $\sigma \in I_P$ if and only if $\sigma(\alpha)$ is one of the e zeroes in characteristic 0 which reduces to $\tilde{\alpha}_1$. Since G acts simply transitively, this implies that $\#(I_P) \leq e$. $\#(I_P) \geq e$ because $\#(G_P) = ef$ and $\#(\mathrm{Aut}(A/P)) = f$. Thus, $\#(I_P) = e$ and β must be surjective. If p does not divide d_k, then Corollary 32 implies that $e = 1$, proving the final claim. □

Corollary 85. *There exists a coset $I_P F$ of I_P in G_P such that the action of any $\sigma \in I_P F$ on A/P is given by $\alpha \mapsto \alpha^p$.*

Proof. This follows from the fact that the Frobenius automorphism generates $\mathrm{Aut}(A/P)$ and the sequence

$$1 \to I_P \to G_P \xrightarrow{\beta} \mathrm{Aut}(A/P) \to 1$$

is exact. □

Corollary 86. *If p does not divide d_k, so that $e = 1$ and $I_P = 1$, then the decomposition group G_P is cyclic, with a canonical generator F_P which satisfies the condition*

$$F_P(\alpha) \equiv \alpha^p \pmod{P}$$

Proof. Immediate. □

If $P' = \tau(P)$ for some $\tau \in G$, then $G_{P'} = \tau G_P \tau^{-1}$ and $F_{P'} = \tau F_P \tau^{-1} \in G$. Thus, for all $p \nmid d_k$ we get a conjugacy class $F_P = \{F_P\}$ in G.

Example. Let $\zeta = \zeta_m = e^{2\pi i/m}$ be a fixed primitive mth root of unity. The minimal polynomial of ζ is denoted $\phi_m(x)$ and divides $x^m - 1$. If $k = \mathbb{Q}(\zeta)$ then the extension

$\mathbb{Q} \subset k$ is Galois with Galois group $G \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$. (Note that if F is any field such that $\mathrm{char}(F) \nmid m$ then we may consider the extension $F \subset F(\zeta_m)$ then the Galois group G embeds in $(\mathbb{Z}/m\mathbb{Z})^\times$ by mapping $\sigma \to a$ if $\sigma(\zeta_m) = \zeta_m^a$.) Gauss showed that over $\mathbb{Q}$ the embedding $G \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ is a surjection, i.e., that $\phi_m(x)$ is irreducible over $\mathbb{Q}$. (This is not true for an arbitrary field F.) We know that G is abelian, so for unramified p we get an element F_p which is F_P for any P dividing p. For $\alpha \in A$, the fact that $F_P(\alpha) \equiv \alpha^p \pmod{P}$ for every $P \mid p$ implies that $F_p(\alpha) \equiv \alpha^p \pmod{pA}$. If $p \nmid m$, then p is unramified in k, in fact, $p \nmid \mathrm{disc}(\mathbb{Z}[\zeta_m])$. Via the map $G \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$, F_p is some class in $(\mathbb{Z}/m\mathbb{Z})^\times$. It is the class of a where $F_p(\zeta) = \zeta^a$. Since $F_p(\zeta) \equiv \zeta^p \pmod{pA}$ it follows that $a = p$ so that F_p is the class of p in $(\mathbb{Z}/m\mathbb{Z})^\times$.

The Dirichlet Density Theorem states that, as $s \to 1$,

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} \sim \frac{1}{\phi_m(s)} \log\Big(\frac{1}{s-1}\Big)$$

and it follows from the above discussion that we can state this theorem in terms of the Galois group G, as

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \sum_{\substack{p \text{ with} \\ F_p = a \in G}} \frac{1}{p^s}$$

We return to the general case where $\mathbb{Q} \subseteq k$ is any (finite) Galois extension. Fix a general conjugacy class $C \subseteq G$. Can we find an unramified prime p such that $F_P \in C$?

Theorem 87. *(Cebotarev) There are infinitely many primes $p \nmid d_k$ with $F_P \in C$ and as $s \to 1$*

$$\sum_{\substack{p \text{ with} \\ F_P \in C}} \frac{1}{p^s} \sim \frac{\#(C)}{\#(G)} \log\Big(\frac{1}{s-1}\Big)$$

Corollary 88. *There are infinitely many primes $p \nmid d_k$ with $F_P = 1$ in G for some (equivalently, for every) P dividing p, i.e., $p = P_1 \cdots P_n$ splits completely. These have density $1/\#(G)$.*

Next, we develop the higher analogs of the $L(\chi, s)$.

Definition. Let k be a finite Galois extension of $\mathbb{Q}$. We define the *Artin L-function* of k, as follows. Let G be the Galois group of k over $\mathbb{Q}$ and let (V, ρ) be a finite-dimensional, complex representation of G. That is, V is a finite-dimensional, complex vector space and $\rho : G \to GL(V)$ is a homomorphism of groups. For a prime number $p \nmid d_k$, we have the conjugacy class F_p in G. For any element $F_P \in F_p$, the element $\rho(F_P)$ in $GL(V)$ has finite order. This implies that $\rho(F_P)$ is semisimple and determined up to conjugacy by its characteristic polynomial. Thus, for each such p the assignment

$$\det(1 - F_p t|V) = 1 - \mathrm{Tr}\,(F_p|V)t + \cdots + (-1)^n \det(F_p|V)t^n$$

is well-defined, where $n = \dim(V) = \deg(\det(1 - F_p t|V))$.

We define $L(V,s)$ as a product over all primes p,

$$L(V,s) = \prod_p \det(1 - F_P p^s | V^{I_P})^{-1}$$

where V^{I_P} denotes the subspace of V fixed by $\rho(I_P)$. The product converges absolutely and is nonzero in the region $\mathrm{Re}(s) > 1$.

Example. Let $V = \mathbb{C}$ and $\rho(\sigma) = 1$ for all $\sigma \in G$. (This is the *trivial representation* of G.) Then for every p

$$\det(1 - F_P p^{-s} | V^{I_P})^{-1} = (1 - p^{-s})^{-1}$$

as every $V^{I_P} = \mathbb{C}$. Thus, $L(\mathbb{C}, s) = \zeta(s)$.

Example. Let $k = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_\ell$ is a primitive ℓth root of unity. Then $G = (\mathbb{Z}/\ell\mathbb{Z})^\times$. If $\chi : G \to \mathbb{C}^\times$ is a character, then the fact that $GL_1(\mathbb{C}) = \mathbb{C}^\times$ implies that we may think of χ as a 1-dimensional representation. It follows that the L function of the representation is exactly the L function of the character, as defined before. In particular, we see that the L function of the representation has an analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation.

Artin Conjecture. With notation as above, $L(V,s)$ has a meromorphic continuation to all of $\mathbb{C}$ with a pole of order $\dim(V^G)$ at $s = 1$ and no other poles.

Brauer proved that $L(V,s)$ has a meromorphic continuation to all of $\mathbb{C}$. There are a few facts which allow us to reduce to certain basic cases.

Fact 1. If $V = V_1 + V_2$ as a linear representation of G, then

$$L(V,s) = L(V_1,s)L(V_2,s)$$

To see this, note that $V^{I_P} = V_1^{I_P} + V_2^{I_P}$ since the representation on V takes the form

$$\sigma \mapsto \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

This form also shows that the characteristic polynomial of $F_P | V^{I_P}$ is the product of the characteristic polynomials of the $F_P | V_i^{I_P}$.

Fact 2. $L(\mathbb{C}, s) = \zeta(s)$.

Fact 3. Let $V = \oplus_{g \in G} \mathbb{C} e_g$ denote the regular representation of G. Then

$$L(V,s) = \zeta_k(s)$$

To see this, note that for $p \nmid d_k$, the factor of $\zeta_k(s)$ corresponding to p can be written $((1 - p^{-fs})^{n/f})^{-1}$ where $f = \#(G_P)$ and $n = \#(G)$. As noted previously, F_P has order f in G: as a permutation of G, left multiplication by F_P has a cycle decomposition with n/f cycles, each of length f.

Fact 4. (Frobenius) The regular representation of G can be expressed in the form

$$V = \oplus_{\text{irred. } V} \dim(V) V$$

where the sum is taken over all irreducible representations of G. It follows from Facts 1 and 3 that

$$\zeta_k(s) = \prod_{\text{irred. } V} L(V,s)^{\dim(V)} = \zeta(s) \prod_{V \neq \mathbb{C}} L(V,s)^{\dim(V)}$$

This is known as the Artin factorization of $\zeta_k(s)$.

Example. The symmetric group S_3 has three irreducible representations: the trivial representation, the one-dimensional representation given by $\chi = \text{sgn}$, and a two-dimensional representation which we denote V. Frobenius' formula tells us that (in the representation ring) the regular representation is of the form $1 + \chi + 2V$. If k is a number field with Galois group $G = S_3$, then Fact 4 implies that $\zeta_k(s) = \zeta(s)L(\chi,s)L(V,s)^2$.

Theorem 89. *(Brauer) $\zeta_k(s)/\zeta(s)$ is an entire function of s.*

Lecture 18

Last lecture, we restricted our attention to the case of Galois extensions. Now, we wish to see what we can say in the general case.

Let k be a number field. Let K denote the Galois closure of k in $\overline{\mathbb{Q}}$, that is, K is the smallest subfield of $\overline{\mathbb{Q}}$ which contains all the conjugates of k. Then K is finite and Galois over $\mathbb{Q}$, say with Galois group G. Let H denote the subgroup of G which fixes k. The coset space G/H is a finite set which is in bijection with the set

$$\text{Hom}_{\mathbb{Q}}(k,\mathbb{C}) = \text{Hom}_{\mathbb{Q}}(k,\overline{\mathbb{Q}}) = \text{Hom}_{\mathbb{Q}}(k,K)$$

Note that the bijection depends on a fixed inclusion of k in K. This set has order $n = (k : \mathbb{Q})$. Also, there is an action of $\sigma \in G = \text{Aut}_{\mathbb{Q}}(K)$ on $\alpha \in \text{Hom}_{\mathbb{Q}}(k,K)$ given by $\sigma(\alpha) = \sigma \circ \alpha$.

If $k = \mathbb{Q}(\alpha)$, then the coset space G/H is in bijection with the n zeroes of $f_\alpha(x)$ in $\overline{\mathbb{Q}}$ by the assignment $\sigma \mapsto \sigma(\alpha)$. If we assume that $p \nmid \text{disc}(f)$, then distinct zeroes in characteristic zero pass to distinct zeroes modulo p, so this set is in bijection with the n zeroes of $f_\alpha(x) \pmod{p}$ in $\overline{\mathbb{F}}_p$. In this set of zeroes, F_P acts by $\alpha_i \mapsto \alpha_i^p$.

Assume that p is a prime number such that $p \nmid d_K$ so that p is unramified in K and $pA_K = P_1 \cdots P_g$. As in the discussion of Lecture 17, G permutes the P_i transitively, and if $P = P_1$, then the stabilizer of P is $G_p = \langle F_P \rangle \cong \mathbb{Z}/f\mathbb{Z}$. We claim (without proof) that the factors of p in k are in bijection with the elements in the (finite) double-coset space $G_P\backslash G/H$. We may think of $G_P\backslash G/H$ either as the set of G_P-orbits on G/H or as the H-orbits on $G_P\backslash G$. Under this correspondence, if a factor $\mathfrak{p}$ of pA_k corresponds to the double coset G_PgH, then the degree of $\mathfrak{p}$ is exactly the number of single G/H cosets in G_PgH.

We rewrite the Euler factor of p in $\zeta_k(s)$. Assume that $P_1, \ldots, P_g$ are the factors of pA_k with degrees $f_1, \ldots, f_g$, respectively. Then the Euler factor corresponding to p is

$$\prod_{i=1}^{g}(1 - p^{-f_i s})^{-1} = \det(1 - F_P p^{-s} | \mathbb{C}[G/H])^{-1}$$

as the Frobenius element F_p has a block form

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_g \end{pmatrix}$$

where A_i is the $f_i \times f_i$ square matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

We define the *induced representation* of G as

$$\mathrm{Ind}_H^G(\mathbb{C}) = \mathbb{C}[G/H]$$

Then

$$\mathrm{Ind}_H^G(\mathbb{C}) = \oplus_{\substack{\text{irred. reps.} \\ V \text{ of } G}} \dim(V^H)V$$

by Frobenius reciprocity, as

$$\mathrm{Hom}_G(V, \mathrm{Ind}_H^G(\mathbb{C})) = \mathrm{Hom}_H(\mathrm{Res}V, \mathbb{C})$$

It follows that

$$\zeta_k(s) = L(\mathrm{Ind}_H^G(\mathbb{C}), s) = \prod_{\substack{\text{irred. reps.} \\ V \text{ of } G}} L(V, s)^{\dim(V^H)}$$

Problem. Can we find two non-isomorphic (i.e., not conjugate in $\overline{\mathbb{Q}}$) number fields k and k' with the same zeta function? This occurs if and only if every p decomposes identically in A_k and $A_{k'}$. Suppose that two such fields exist with the same Galois closure K. We must have $(k, \mathbb{Q}) = (k' : \mathbb{Q})$ and they must have the same number of real places, complex places and roots of unity. By the class number formula, this implies that $hR = h'R'$. It is not necessarily true, however, that $h = h'$. We know that k and k' are isomorphic subfields of K if and only if the corresponding subgroups H and H' are conjugate in G. (Under these conditions, we say that H and H' are *globally conjugate.*) By our previous work, $\zeta_k(s) = \zeta_{k'}(s)$ if and only if $\mathrm{Ind}_H^G(\mathbb{C}) \cong \mathrm{Ind}_{H'}^G(\mathbb{C})$ as representations of G. This occurs if and only if, for every $\sigma \in G$, $\mathrm{Tr}\,(\sigma : \mathrm{Ind}_{H'}^G(\mathbb{C})) = \mathrm{Tr}\,(\sigma : \mathrm{Ind}_H^G(\mathbb{C}))$. If we write $\mathrm{Ind}_H^G(\mathbb{C}) = \oplus_{G/H} \mathbb{C} e_{gH}$, then $\sigma(e_{gH}) = e_{\sigma gH}$ so that

$$\begin{aligned} \mathrm{Tr}\,(\sigma : \mathrm{Ind}_H^G(\mathbb{C})) &= (\text{the number of cosets } gH \text{ such that } \sigma gH = gH) \\ &= (\text{the number of cosets } gH \text{ such that } g^{-1}\sigma gH = H) \\ &= \#(\{g : g^{-1}\sigma g \in H\}/\{g \sim g' \Leftrightarrow gH = g'H\}) \\ &= \#(C_\sigma \cap H)/(\#(H)/\#(Z_\sigma(H))) \end{aligned}$$

Thus, $\zeta_k(s) = \zeta_{k'}(s)$ if and only if, for every conjugacy class C_σ in G, $\#(C_\sigma \cap H) = \#(C_\sigma \cap H')$. (Under these conditions, we say that H and H' are *locally conjugate*.)

We now give two examples of subgroups $H, H' \subset G$ which are locally conjugate but not globally conjugate.

Example. Let $G = S_6$ and consider the subgroups

$$\begin{aligned} H &= \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \\ H' &= \{e, (1\,2)(3\,4), (1\,2)(5\,6), (3\,4)(5\,6)\} \end{aligned}$$

The subgroups each have order 4, and they have the same cycle structure (2,2,1,1), and are therefore locally conjugate. (It is straightforward to verify this fact directly, as a conjugacy class is uniquely determined by the cycle structure of a representative.) However, H fixes the numbers 5 and 6, while H' fixes nothing, so H and H' are not globally conjugate.

Example. Let $G = \mathrm{GL}_3(\mathbb{F}_2) = \mathrm{GL}(V)$ where V is a three-dimensional vector space over $\mathbb{F}_2$. Then G has order 168. If we let P denote the stabilizer of a line and P' the stabilizer of a plane, then P and P' each have index 7 in G. In fact, P and P' are locally conjugate, but they are not globally conjugate.