Algebra 2

Vorlesung im
Wintersemester 1999/00
TU-Berlin

gehalten von
Dr. C. Fieker

Inhaltsverzeichnis

KAPITEL 1

Gruppentheorie

Definition 1.1 ($\mathfrak{S}_n$): $\mathfrak{S}_n$ bezeichne die Menge aller Permutationen der Menge $\mathbb{N}_n = \{1, 2, \dots, n\}$, d.h. die Menge der bijektiven Abbildungen von $\mathbb{N}_n$. $\mathfrak{S}_n$ heißt symmetrische Gruppe.

Bemerkungen:

Um später Verwirrung in der Notation zu vermeiden, schreiben wir $\pi[i]$ um das Bild von i unter der Permutation π zu bezeichnen. Gebräuchlich sind auch andere Schreibweisen: i^π, $\pi(i)$ oder πi.

$\pi \in \mathfrak{S}_n$ schreibt man auch als

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \pi[1] & \pi[2] & \pi[3] & \dots & \pi[n-1] & \pi[n] \end{pmatrix}.$$

$\mathfrak{S}_n$ ist Gruppe! Für $n \geq 3$ ist $\mathfrak{S}_n$ nicht kommutativ! Es gilt: $\sharp\mathfrak{S}_n = n!$

Definition 1.2 (Zykel): $\pi \in \mathfrak{S}_n$ heißt r-Zykel, falls es eine Teilmenge $\{i_1, \dots, i_r\}$ von r Elementen von $\{1, \dots, n\}$ mit

$$\pi[i_\nu] = i_{\nu+1} \ (1 \leq \nu < r), \ \pi[i_r] = i_1, \ \pi[j] = j \ \ \forall j \notin \{i_1, \dots, i_r\}$$

gibt.
2-Zykel heißen Transposition.

Schreibweise:

$$\pi = (i_1, \dots, i_r) = \begin{pmatrix} 1 & \dots & n \\ \pi[1] & \dots & \pi[n] \end{pmatrix}.$$

Vereinbarung: id $= (1)$ ist einziger 1-Zykel.

Bemerkung: Für Transpositionen π gilt: $\pi^2 = \mathrm{id}$ bzw. $\pi = \pi^{-1}$.

Hilfssatz 1.3: In $\mathfrak{S}_n$ ist jedes Element als Produkt von höchstens n Transpositionen darstellbar. (Konvention: id = leeres Produkt.)

Beweis:

Sei $\pi \in \mathfrak{S}_n$ vorgegeben und o.B.d.A. $\pi \neq \mathrm{id}$.

Dann existiert $i \in \mathbb{N}$ minimal mit $\pi[i] > i$, etwa $\pi[i] = j$. Es sei $\tau_{ij} := (i, j)$ diejenige Transposition, die i und j vertauscht, bilde $\tau_{ij}\pi$. Hierfür gilt: $\tau_{ij}\pi[k] = k$ für $1 \leq k \leq i$.

Iterierte Anwendung liefert $l \leq n-1$ Transpositionen $\tau_1, \dots, \tau_l$, so daß für $\tilde{\pi} = \tau_l \tau_{l-1} \dots \tau_2 \tau_1 \pi$ gilt:

$\tilde{\pi}[\kappa] = \kappa$ für $1 \leq \kappa \leq n-1$. Damit gilt auch $\tilde{\pi}[n] = n$ (Permutationen sind surjektiv!), also $\tilde{\pi} = \mathrm{id}$. Also ist

$$\begin{aligned} \tau_l &= \tau_l\tilde{\pi} = \tau_{l-1}\dots\tau_1\pi \\ \tau_{l-1}\tau_l &= \tau_{l-1}\tau_l\tilde{\pi} = \tau_{l-2}\dots\tau_1\pi \\ &\text{usw.} \\ \tau_1\dots\tau_l &= \pi. \end{aligned}$$

□

Beispiel:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \qquad \in \mathfrak{S}_6$$

$$\tau_{13}\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 6 & 5 \end{pmatrix}$$

$$\tau_{23}\tau_{13}\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}$$

$$\tau_{56}\tau_{23}\tau_{13}\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$\pi = \tau_{13}\tau_{23}\tau_{56} = (1,3)(2,3)(5,6)$$

Bemerkung:

$$\mathfrak{V}_4 \cong \{(1),\ (1\,2)\,(3\,4),\ (1\,3)\,(2\,4),\ (1\,4)\,(2\,3)\}$$

als Untergruppe von $\mathfrak{S}_4$.

Hilfssatz 1.4 (Rechenregeln für Zykel): (1) Zykel entsprechen Bahnen unter der Operation

$$\mathfrak{S}_n \times \{1,\dots,n\} \to \{1,\dots,n\} \ : \ \pi \times \nu \mapsto \pi[\nu],$$

d.h. π besitzt genau eine mehrelementige Bahn.

(2) $(i_1,\dots,i_r) = (i_\nu,\dots,i_r,\ i_1,\dots,i_{\nu-1})\ \ (1 \leq \nu \leq r)$.

(3) $(i_1,\dots,i_r) = (i_1,\dots,i_\nu)\,(i_\nu,\dots,i_r)\ \ (2 \leq \nu \leq r-1)$, mit Anwendung

$$(i_1,\dots,i_r) = \prod_{j=1}^{r-1}(i_j, i_{j+1}).$$

(4) $\mathrm{ord}(i_1,\dots,i_r) = r$,

(5) $(i_1,\dots,i_r)^{-1} = (i_r, i_{r-1},\dots,i_1)$,

(6) $\pi(i_1,\dots,i_r)\pi^{-1} = (\pi[i_1],\dots,\pi[i_r])\ \ \forall \pi \in \mathfrak{S}_n$.

Beweis:

Bis auf (6) sind die Aussagen unmittelbar klar. Es genügt, (6) für Transpositionen zu zeigen, da gemäß (3)

$$\pi\,(i_1,\dots,i_r)\,\pi^{-1} = \prod_{j=1}^{r-1}\pi(i_j,i_{j+1})\pi^{-1}$$

ist. Ist nun $\nu \in \{1,\dots,n\}$ mit $\pi^{-1}[\nu] \notin \{i_j, i_{j+1}\}$, dann bleibt ν invariant. Schließlich ist

$$\pi^{-1}[\nu] = i_{j+1} \quad \Leftrightarrow \quad \nu = \pi[i_{j+1}],$$

also gilt insgesamt:

$$\pi(i_j, i_{j+1})\pi^{-1} = (\pi[i_j], \pi[i_{j+1}]).$$

□

Definition 1.5 (Fehlstand): Für $\pi \in \mathfrak{S}_n$ heißt jedes Paar (i, j) von Indizes $1 \leq i < j \leq n$ mit $\pi[i] > \pi[j]$ ein Fehlstand von π.

Beispiel:

$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in \mathfrak{S}_3$ hat die Fehlstände $(1,3), (2,3)$.

Bemerkung: Die Anzahl der Fehlstände ist $\leq \binom{n}{2}$.

Definition 1.6 (sign π): Das Vorzeichen (Signum) von $\pi \in \mathfrak{S}_n$ wird definiert als:

$$\begin{aligned} \operatorname{sign}(\pi) &:= \begin{cases} 1 & \text{, falls } \pi \text{ eine gerade Anzahl von Fehlständen hat} \\ -1 & \text{, falls } \pi \text{ eine ungerade Anzahl von Fehlständen hat} \end{cases} \\ &= (-1)^{\sharp \text{ Fehlstände von } \pi} \end{aligned}$$

Entsprechend heißt $\pi \in \mathfrak{S}_n$ mit $\operatorname{sign}(\pi) = 1$ gerade, mit $\operatorname{sign}(\pi) = -1$ ungerade.

Beispiel:

Es sei $\tau \in \mathfrak{S}_n$ Transposition, die i mit j vertauscht, $1 \leq i < j \leq n$. Fehlstände von

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & 3 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

sind

$$\begin{array}{llll} (i, i+1), & (i, i+2), & \dots & (i, j-1), \quad (i, j) \\ (i+1, j), & (i+2, j), & \dots & (j-1, j), \end{array}$$

Anzahl ist ungerade, d.h. $\operatorname{sign}(\tau) = -1$.

Hilfssatz 1.7: Für $\pi \in \mathfrak{S}_n$ gilt:

$$\operatorname{sign}(\pi) = \prod_{1 \leq i < j \leq n} \frac{\pi[i] - \pi[j]}{i - j}.$$

Beweis:

Für jedes Paar (i, j) mit $1 \leq i < j \leq n$ ist $x_{ij} := \frac{\pi[i]-\pi[j]}{i-j} \in \mathbb{Q}\backslash\{0\}$ $(= \mathbb{Q}^\times)$ sowie

$\operatorname{sign}(x_{ij}) = \begin{cases} 1 & \text{für } x_{ij} > 0 \\ -1 & \text{für } x_{ij} < 0 \end{cases}$. Damit wird

$$\left| \prod_{1 \leq i < j \leq n} \frac{\pi[i] - \pi[j]}{i - j} \right| = \left| \prod_{1 \leq i < j \leq n} (\pi[i] - \pi[j]) \right| \left| \prod_{1 \leq i < j \leq n} (i - j) \right|^{-1} = 1.$$

(Beachte: Mit (i, j) durchläuft auch $\pi[i], \pi[j]$ alle Paare verschiedener Zahlen aus $\{1, \dots, n\}$, allerdings bedingt $i < j$ i.a. nicht $\pi[i] < \pi[j]$.)

Wegen der Definition von $\operatorname{sign}(\pi)$ hat man nun:

$$\begin{aligned}\operatorname{sign}(\pi) &= (-1)^{\sharp \text{ Fehlstände von } \pi} \\ &= \prod_{1\le i<j\le n} \operatorname{sign}\left(\frac{\pi[i]-\pi[j]}{i-j}\right) \\ &= \operatorname{sign}\left(\prod_{1\le i<j\le n} \frac{\pi[i]-\pi[j]}{i-j}\right) \\ &= \prod_{1\le i<j\le n} \frac{\pi[i]-\pi[j]}{i-j}.\end{aligned}$$

□

Satz 1.8: Die Abbildung $\operatorname{sign} : \mathfrak{S}_n \to C_2 : \pi \mapsto \operatorname{sign}(\pi)$ ist Gruppenhomomorphismus, für $n \ge 2$ ist sie surjektiv.

Beweis:

Surjektivität klar, wegen $\operatorname{sign}(\mathrm{id}) = 1,\ \operatorname{sign}(\tau) = -1$ für Transpositionen.

Zu zeigen bleibt für $\pi, \varrho \in \mathfrak{S}_n$:

$\operatorname{sign}(\pi\varrho) = \operatorname{sign}(\pi)\operatorname{sign}(\varrho)$

$$\begin{aligned}\operatorname{sign}(\pi\varrho) &\overset{1.7}{=} \prod_{1\le i<j\le n} \frac{\pi\varrho[i]-\pi\varrho[j]}{i-j} \\ &= \prod_{1\le i<j\le n} \frac{\pi\varrho[i]-\pi\varrho[j]}{\varrho[i]-\varrho[j]}\,\frac{\varrho[i]-\varrho[j]}{i-j} \\ &\overset{!}{=} \prod_{1\le i<j\le n} \underbrace{\frac{\pi[\varrho[i]]-\pi[\varrho[j]]}{\varrho[i]-\varrho[j]}}_{=\operatorname{sign}(\pi)}\,\underbrace{\frac{\varrho[i]-\varrho[j]}{i-j}}_{\overset{1.7}{=}\operatorname{sign}(\varrho)}\end{aligned}$$

(Beachte:

Mit (i,j) $(1 \le i < j \le n)$ durchläuft auch $\varrho[i], \varrho[j]$ alle Paare, jedoch gilt nicht notwendig $\varrho[i] < \varrho[j]$. Für $\varrho[i] > \varrho[j]$ ist aber

$$\frac{\pi[\varrho[i]]-\pi[\varrho[j]]}{\varrho[i]-\varrho[j]} = \frac{\pi[\varrho[j]]-\pi[\varrho[i]]}{\varrho[j]-\varrho[i]},$$

d.h. Vertauschung der Reihenfolge nach Größe ändert Wert des Quotienten nicht. D.h.

$$\prod_{1\le i<j\le n} \frac{\pi[\varrho[i]]-\pi[\varrho[j]]}{\varrho[i]-\varrho[j]} = \prod_{1\le \mu<\nu\le n} \frac{\pi[\mu]-\pi[\nu]}{\mu-\nu}.)$$

□

Korollar 1.9: Ist π Produkt von Transpositionen $\tau_1, \ldots, \tau_r \in \mathfrak{S}_n$, so ist $\operatorname{sign}(\pi) = (-1)^r$. (D.h. jede Darstellung von π als Produkt von Transpositionen enthält immer gerade bzw. ungerade viele Faktoren.) Jede (un)gerade Permutation ist stets Produkt (un)gerade vieler Transpositionen.

Beweis: Folgt unmittelbar aus Hilfssatz 1.3 und Satz 1.8. □

Bemerkung: Die Signatur (sign eines r-Zykels ist $(-1)^{r-1}$.

Definition 1.10 ($\mathfrak{A}_n$): Die geraden Permutationen von $\mathfrak{S}_n$ bilden für $n \geq 2$ einen Normalteiler $\mathfrak{A}_n$ der Ordnung $\frac{n!}{2}$ von $\mathfrak{S}_n$, die sog. alternierende Gruppe. ($\mathfrak{A}_n := \ker \operatorname{sign}$)

Bemerkung: Für $n = 1$ ist $\mathfrak{A}_1 := \mathfrak{S}_1$.

Beispiel: $n = 3$

$$\begin{aligned} \mathfrak{A}_3 = C_3 &= \{(), (1,2,3), (1,2,3)^2\} \\ &= \{(), (1,2,3), (1,3,2)\} \\ \tau &= (1,2) = \tau_{12}, \end{aligned}$$

$$\mathfrak{A}_3\tau = \Big\{ \underbrace{()(1,2)}_{\substack{(1,2) \\ \| \\ \tau_{12}}}, \underbrace{(1,2,3)(1,2)}_{\substack{(1,3) \\ \| \\ \tau_{13}}}, \underbrace{(1,3,2)(1,2)}_{\substack{(2,3) \\ \| \\ \tau_{23}}} \Big\}.$$

Es gilt $\mathfrak{S}_3 = \mathfrak{A}_3 \cup \mathfrak{A}_3\tau_{1,2}$.

Hilfssatz 1.11: Für $n \in \mathbb{N}$ hat $\mathfrak{S}_{n+1}$ eine disjunkte Zerlegung in $n+1$ (Links-) Nebenklassen nach $\mathfrak{S}_n$.

$$\left(\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+1} : \begin{pmatrix} 1 & 2 & \dots & n \\ \pi[1] & \pi[2] & \dots & \pi[n] \end{pmatrix} \mapsto \begin{pmatrix} 1 & \dots & n & n+1 \\ \pi[1] & \dots & \pi[n] & n+1 \end{pmatrix} \right)$$

Beweis:

Setze $\pi_{n+1} := \mathrm{id} \in \mathfrak{S}_{n+1}$ und $\pi_\nu := (\nu, n+1)$ $(1 \leq \nu \leq n)$. Wir zeigen:

$$\mathfrak{S}_{n+1} = \bigcup_{\nu=1}^{n+1} \pi_\nu \mathfrak{S}_n.$$

Sei dazu $\tau \in \mathfrak{S}_{n+1}$ mit $\tau[n+1] = j$. Für $j = n+1$ gilt $\tau \in \pi_{n+1}\mathfrak{S}_n$. Andernfalls bildet $(j, n+1)\,\tau$ das Element $n+1$ auf sich ab, also ist

$$(j, n+1)\,\tau \in \pi_{n+1}\,\mathfrak{S}_n \quad \text{und} \quad \tau \in (j, n+1)\,\pi_{n+1}\,\mathfrak{S}_n = (j, n+1)\,\mathfrak{S}_n.$$

Wir zeigen noch, daß die Zerlegung disjunkt ist, obwohl dies bereits aus den Elementanzahlen folgt.

$$\begin{aligned} \pi_\nu\,\mathfrak{S}_n = \pi_\mu\,\mathfrak{S}_n &\Leftrightarrow \pi_\mu\pi_\nu\,\mathfrak{S}_n = \mathfrak{S}_n \\ &\Rightarrow \pi_\mu\pi_\nu[n+1] = n+1 \\ &\Rightarrow \pi_\nu[n+1] = \pi_\mu[n+1] \\ &\Leftrightarrow \nu = \mu. \end{aligned}$$

□

Bemerkung: Dies ist ein weiterer Beweis für $\sharp\mathfrak{S}_n = n!$

Hilfssatz 1.12:

$$\begin{aligned} \mathfrak{S}_n &= \langle (i,\, n) \mid 1 \leq i \leq n-1 \rangle \quad (\text{für } n \geq 2). \\ &= \langle (1,\, i) \mid 1 < i \leq n \rangle \end{aligned}$$

Beweis:

Jede Permutation ist als Produkt von höchstens n Transpositionen der Form (i,j) $(1 \le i < j \le n)$ darstellbar (Hilfssatz 1.3). Ferner gilt:

$$(i,j) = (1,i)(1,j)(1,i)$$

nach 1.4.(6) für $i > 1$. Analog gilt

$$(i,j) = (i,n)(j,n)(i,n)$$

für $1 \le i < j \le n$. □

Definition 1.13: Zwei Zykel $(i_1,\dots,i_r), (j_1,\dots,j_s)$ heißen elementfremd, falls

$$\{i_1,\dots,i_r\} \cap \{j_1,\dots,j_s\} = \emptyset$$

ist.

Hilfssatz 1.14: Elementfremde Zykeln kommutieren.

Beweis:

Es seien $I = \{i_1,\dots,i_r\}$, $J = \{j_1,\dots,j_s\}$ und $\mathbb{N}_n = \{1,\dots,n\}$, $K = (\mathbb{N}_n \backslash I) \backslash J$, $I \cap J = \emptyset$. Dann gilt

$$\begin{aligned}(i_1,\dots,i_r)\,(j_1,\dots,j_s)[\nu] &= \begin{cases} \nu & \text{für } \nu \in K \\ j_{l+1} & \text{für } \nu = j_l \ (1 \le l < s) \\ j_1 & \text{für } \nu = j_s \\ i_{l+1} & \text{für } \nu = i_l \ (1 \le l < r) \\ i_1 & \text{für } \nu = i_r \end{cases} \\ &= (j_1,\dots,j_s)\,(i_1,\dots,i_r)[\nu].\end{aligned}$$

□

Satz 1.15: Jede Permutation $\pi \in \mathfrak{S}_n$, $\pi \neq \mathrm{id}$, läßt sich eindeutig (bis auf die Reihenfolge) als Produkt elementfremder Zykeln darstellen.

Beweis:

π operiert auf $\mathbb{N}_n$ bzgl. $(\pi,\nu) \mapsto \pi[\nu]$. $\mathbb{N}_n$ zerfällt diesbezüglich in Bahnen $B_1,\dots,B_{\tilde{k}}$. Nach Weglassen der einelementigen Bahnen verbleiben etwa $B_1,\dots,B_k$ (bei passender Numerierung) mit

$$B_1 \dot\cup \dots \dot\cup B_k = M_k, \quad B_i = (\nu_i,\, \pi[\nu_i],\dots,\, \pi^{r_i-1}[\nu_i]) \text{ und } \pi^{r_i}[\nu_i] = \nu_i.$$

Dabei liege

$$\begin{aligned}\nu_1 &:= \min M_k \text{ in } B_1, \\ \nu_2 &:= \min M_k \backslash B_1 \text{ in } B_2, \\ &\vdots \\ \nu_{k-1} &:= \min M_k \backslash (B_1 \dot\cup \dots \dot\cup B_{k-2}) \text{ in } B_{k-1}.\end{aligned}$$

Hierfür ist dann $(\nu_k := \min B_k)$

$$\pi = (\nu_1, \pi[\nu_1],\dots,\pi^{\sharp B_1-1}[\nu_1])(\nu_2,\pi[\nu_2],\dots,\pi^{\sharp B_2-1}[\nu_2])\dots(\nu_k,\pi[\nu_k],\dots,\pi^{\sharp B_k-1}[\nu_k]).$$

Diese Darstellung ist auch eindeutig, da jedes $\nu \in \mathbb{N}_n$ durch π entweder invariant gelassen wird, oder es wird auf ein Element der gleichen Bahn abgebildet, d.h. für $\pi[\nu] \neq \nu$ tritt stets der Zykel

$$\left(\nu, \pi[\nu], \dots, \pi^{l_\nu - 1}[\nu]\right) \text{ auf } \left(\pi^{l_\nu}[\nu] = \nu\right).$$

□

Beispiel:

Für

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \end{pmatrix}$$

ist

$$\pi = (1,2,4,8)(3,6,12,9)(5,10)(7,14,13,11).$$

Satz 1.16: Für $n \geq 3$ wird die alternierende Gruppe von 3-Zykeln erzeugt. Speziell gilt:

$$\mathfrak{A}_n = \langle (1,2,i) \mid 3 \leq i \leq n \rangle.$$

Beweis:

$\mathfrak{A}_n$ besteht aus geraden Permutationen, ihre Elemente sind also Produkte jeweils einer geraden Anzahl von Transpositionen. Also gilt:

$$\mathfrak{A}_n = \langle (i,j)(k,l) \mid 1 \leq i < j \leq n, 1 \leq k < l \leq n \rangle.$$

Die erzeugenden Elemente hierin sind nun Produkte von 3-Zyklen:

(1) $\sharp\{i,j,k,l\} = 2 \Rightarrow$ (eventuelles Umnumerieren) $k = i$, $l = j$, also

$$(i,j)(i,j) = \mathrm{id} = (1,2,3)^3;$$

(2) $\sharp\{i,j,k,l\} = 3 \Rightarrow j = k,\ i \neq l$:

$$(i,j)(j,l) = (i,j,l),$$

(3) $\sharp\{i,j,k,l\} = 4$:

$$\begin{aligned} (i,j)(k,l) &= ((i,j)(j,k))((j,k)(k,l)) \\ &= (i,j,k)(j,k,l), \end{aligned}$$

wie in (2).

Schließlich:

$$(i,j,k) = (2,k,i)(2,i,j)$$

und

$$\begin{aligned} (2,i,j) &= (1,2,j)^2(1,2,i) \\ &= (1,j,2)(1,2,i). \end{aligned}$$

□

Beispiel:

$$\mathfrak{A}_3 = \{(1,2,3)^k \mid k = 0,1,2\}, \quad \mathfrak{A}_2 = \{\mathrm{id}\}.$$

Hilfssatz 1.17: Für $n \geq 5$ sind alle 3-Zyklen von $\mathfrak{A}_n$ konjugiert.

Beweis:

Wir zeigen: Zu (i,j,k) und $(1,2,3)$ existiert $\pi \in \mathfrak{A}_n$ mit

$$\pi\,(1,\,2,\,3)\,\pi^{-1} = (i,\,j,\,k).$$

Wegen $n \geq 5$ existieren $l,\, m \in \mathbb{N}_n$ mit $\sharp\{i,j,k,l,m\} = 5$. Da $\tau \notin \mathfrak{A}_n$ folgt, daß entweder

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & l & m & \dots & \end{pmatrix} \quad \text{oder} \quad (l,\,m)\,\tau$$

in $\mathfrak{A}_n$ liegt ($(\mathfrak{S}_n : \mathfrak{A}_n) = 2!$). Nach 1.4.(6) gilt nun

$$\begin{aligned} \tau\,(1,2,3) &\overset{1.4.(6)}{=} (\tau[1],\tau[2],\tau[3]) \\ &= (i,j,k) \\ &= (\tau[1],\tau[2],\tau[3])(l,m)^{-1}(l,m) \\ &\overset{1.14}{=} (l,m)\tau(1,2,3)\,\tau^{-1}(l,m). \end{aligned}$$

□

Satz 1.18: Für $n \geq 5$ ist $\mathfrak{A}_n$ einfach.

Bemerkung:

Dies hat weitreichende Konsequenzen. Speziell gilt für

$$p \mid \frac{n!}{2} \quad (n \geq 5)$$

stets, daß mehrere p-Sylow-Untergruppen von $\mathfrak{A}_n$ existieren.

Beweis:

Es sei $N \neq \langle \mathrm{id} \rangle$ Normalteiler von $\mathfrak{A}_n$ und $n \geq 5$. Gemäß 1.16 und 1.17 genügt es zu zeigen, daß N einen 3-Zykel enthält, da dann bereits $N = \mathfrak{A}_n$ folgt.

Dazu sei $\pi \in N$, $\pi \neq \mathrm{id}$, in eindeutiger Darstellung als Produkt elementfremder Zykeln gemäß 1.15 gegeben.

1. Fall:

Es tritt ein r-Zykel $(i,j,k,l,\dots)$ mit $r \geq 4$ auf. Für $\tau = (i,j,k)$ liegt dann $\pi\,(\tau\,\pi^{-1}\tau^{-1})$ ebenfalls in N.

$$\begin{aligned} N \ni\ \pi\,(\tau\,\pi^{-1}\tau^{-1}) &= (i,\,j,\,k,\,l,\,\dots)\,(\dots,\,\pi\,[l],\,\pi,\,[k],\,\pi\,[j],\,\pi\,[i]) \\ &= (i,\,j,\,k,\,l,\,\dots)\,(\dots,\,l,\,i,\,k,\,j) \\ &= (i,\,l,\,j) \end{aligned}$$

$\pi\,(\tau\,\pi^{-1}\tau^{-1})$ hat keinen Effekt außerhalb des r-Zykels $(i,j,k,l,\dots)$, und dort bewirkt es:

$$(i,\,j,\,k,\,l,\,\dots)\begin{pmatrix} \dots, & \pi\,[l], & \pi\,[k], & \pi\,[j] & \pi\,[i] \\ \dots, & l, & i, & k, & j \end{pmatrix} = (i,\,l,\,j).$$

2. Fall:

In der Faktorisierung von π tritt mindestens ein 3-Zykel auf. Bei mehreren Faktoren gilt also

$$\pi = (i,\, j,\, k)\,(l,\, m,\, ?)\,\ldots\,.$$

Setze $\tau = (i, j, l)$ und bilde

$$\begin{aligned}\pi\,(\tau\,\pi^{-1}\tau^{-1}) &= (i,\, j,\, k)\,(l,\, m,\, ?)\,\ldots\,(k,\, l,\, j)\,(?,\, m,\, i)\\ &= (i,\, l,\, k,\, m,\, j) \quad \in N,\end{aligned}$$

dann weiter mit Fall 1.

3. Fall:

π Produkt elementfremder Transpositionen, $\pi = (i,j)(k,l)\ldots$, $\exists m \in \mathbb{N}_n \setminus \{i,j,k,l\}$. Setze $\tau = (i,k,m)$ und bilde

$$\begin{aligned}\pi\,(\tau\,\pi^{-1}\tau^{-1}) &= (\pi\,\tau\,\pi^{-1}|, \tau^{-1})\\ &= (j,\, l,\, \pi\,[m])\,(m,\, k,\, i).\end{aligned}$$

Für $\pi\,[m] \neq m$ geht es mit Fall 2 weiter, für $\pi\,[m] = m$ folgt

$$\pi\,(\tau\,\pi^{-1}\tau^{-1}) = (i,\, j,\, l,\, m,\, k),$$

und wir schließen wie im Fall 1. □

Definition 1.19 (auflösbar): Eine endliche Gruppe G heißt auflösbar, falls eine Kette von Untergruppen

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$$

existiert, so daß $G_{i+1} \lhd G_i$ gilt und G_i/G_{i+1} abelsch ist $(0 \leq i < n)$.

Bemerkung:

(1) Existiert eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{e\}$$

mit $G_{i+1} \lhd G_i$ und G_i/G_{i+1} abelsch $(0 \leq i < n)$, dann ist G auflösbar.

(2) Eine solche Untergruppenkette heißt Normalreihe.

Beispiel:

$\mathfrak{S}_3 = G_0 \supset G_1 = \mathfrak{A}_3 \supset \{e\} = G_2$;

$D_n = G_0 \supset G_1 = \langle b\rangle \supset \{e\} = G_2$;

G abelsch $G = G_0 \supset G_1 = \{e\}$;

$\mathfrak{S}_4 = G_0 \supset G_1 = \mathfrak{A}_4 \supset G_2 = \mathfrak{V}_4 \supset \{e\} = G_3$.

Hilfssatz 1.20: (1) Jede endliche abelsche Gruppe ist auflösbar mit zyklischen Faktorgruppen.

(2) Eine endliche Gruppe ist genau dann auflösbar, falls eine Untergruppenkette

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\} \text{ mit } G_{i+1} \lhd G_i$$

und G_i/G_{i+1} zyklisch existiert.

Beweis:

(1) Induktion über $m = (G : 1)$. $m = 1$ ist trivial. Sei also $m > 1$. Ist G selbst zyklisch, so ist nichts zu zeigen. Andernfalls sei $H = \langle x \rangle$ zyklische Untergruppe von G mit $x \neq \{e\}$. Nach Induktionsvoraussetzung ist dann G/H auflösbar mit zyklischen Faktorgruppen, d.h. es existierten Untergruppe G_i/H $(0 \leq i \leq r)$, $G_0 = G$, $G_r = H$ mit

$$G_i/H \Big/ G_{i+1}/H \cong G_i/G_{i+1}$$

zyklisch. Dann leistet

$$G = G_0 \supset G_1 \supset \ldots \supset G_{r-1} \supset G_r = H \supset \{e\}$$

das gewünschte. (Anderer Beweis direkt mittels (Hauptsatz über endliche abelsche Gruppen Algebra 1, 1.25).)

(2) $\Leftarrow$ klar nach Definition.
$\Rightarrow$ gemäß (1).
G_i/G_{i+1} ist abelsch, falls nicht zyklisch.

$$G_{i_0} = G_i/G_{i+1} \supset \overline{G}_{i_1} \supset \ldots \supset \overline{G}_{i_k} = G_{i+1}$$

mit zyklischer Faktorgruppe

$$\overline{G}_{i_\nu} = G_{i_\nu}/G_{i+1};$$

verfeinere alte Normalreihe mittels

$$G_i = G_{i_0} \supset G_{i_1} \supset \ldots \supset G_{i_{k_i}} = G_{i+1},$$

$$G_{i_\nu} \Big/ G_{i_{\nu+1}} \cong \overline{G}_{i_\nu} \Big/ G_{i_{\nu+1}}$$

zyklisch.

□

Hilfssatz 1.21: Es sei G eine endliche Gruppe mit Untergruppe H.
(1) Ist G auflösbar, so auch H und im Fall $H \lhd G$ und H auflösbar ist auch G/H auflösbar.
(2) Ist H Normalteiler und sind H sowie G/H auflösbar, dann ist auch G auflösbar.

Beweis:

(1) Es sei

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$$

(Normalreihe von G) mit $G_{i+1} \lhd G_i$, G_i/G_{i+1} abelsch. Bilde

$$H_i := G_i \cap H \quad (0 \leq i \leq n).$$

$H_{i+1} \lhd H_i$: Für $x \in H_i$ gilt:

$$x\, H_{i+1} x^{-1} \subseteq x\, G_{i+1} x^{-1} \cap x\, H\, x^{-1} = G_{i+1} \cap H = H_{i+1}.$$

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \overset{\text{Algebra1,1.20}}{\cong} H_i G_{i+1}/G_{i+1} < G_i/G_{i+1}.$$

Gilt außerdem $H \lhd G$, so bilde mittels $\tilde{G}_i := G_i H < G$ $(0 \leq i \leq n)$ Kette

$$\tilde{G}_0/H \supseteq \tilde{G}_1/H \supseteq \ldots \supset \tilde{G}_n/H = H$$

(Untergruppenkette von G/H). Betrachte Abbildung

$$\varphi : \tilde{G}_i \to G_i/G_{i+1} \ : \ g_i h \mapsto g_i\, G_{i+1}$$

surjektiv. φ ist Homomorphismus:

$$\begin{aligned}\varphi(g_iH)\,\varphi(\tilde{g}_i\tilde{h}) &= (g_i\,G_{i+1})\,\tilde{g}_i\,G_{i+1})\\ &\overset{G_{i+1}\lhd G_i}{=} g_i\tilde{g}_i\,G_{i+1}\\ &= \varphi(g_i\tilde{g}_ih'\tilde{h})\\ &= \varphi(g_ih\,\tilde{g}_i\tilde{h})\end{aligned}$$

wobei zunächst $h'\tilde{h}\in H$ beliebig, wähle h' so, daß $g_ih' = hg_i$ gilt (Da $H\lhd G$ geht dies!). φ Surjektivität ist klar,

$$\ker\varphi = \{g_ih\in\tilde{G}_i \mid g_i\in G_{i+1}\} = G_{i+1}H = \tilde{G}_{i+1}.$$

Also gilt: $\tilde{G}_{i+1}\lhd\tilde{G}_i$ und

$$\tilde{G}_i/\tilde{G}_{i+1}\cong G_i/G_{i+1},$$

also abelsch. Wende nun 2. Isomorphiesatz Algebra 1, 1.21 an:

$$(\tilde{G}_i/H)\,\big/\,(\tilde{G}_{i+1}/H)\cong\tilde{G}_i/\tilde{G}_{i+1}.$$

(2) H auflösbar:

$$H = H_0\supset H_1\supset\ldots\supset H_r = \{e\}$$

mit H_i/H_{i+1} abelsch. G/H auflösbar:

$$G = G_0\supset G_1\supset\ldots\supset G_s = H$$

von G mit

$$(G_i/H)\,\big/\,(G_{i+1}/H)\overset{\text{Algebra1,1.21}}{\cong}G_i/G_{i+1}$$

abelsch. Also ist

$$G = G_0\supset G_1\supset\ldots\supset G_s = H = H_0\supset H_1\supset\ldots\supset H_r = \{e\},$$

d.h. G auflösbar.

□

Bemerkung: Für $n\geq 5$ ist $\mathfrak{S}_n$ nicht auflösbar, da $\mathfrak{A}_n$ für $n\geq 5$ nach 1.18 nicht auflösbar ist.

KAPITEL 2

Ringe

Definition 2.1: Es sei R ein kommutativer Ring mit 1. Ein Polynom

$$f(\underline{t}) \in R[\underline{t}] \quad (\underline{t} = (t_1, \ldots, t_n))$$

heißt symmetrisch, falls

$$f(t_1, \ldots, t_n) = f(t_{\pi[1]}, \ldots, t_{\pi[n]})$$

für alle $\pi \in \mathfrak{S}_n$ gilt. Speziell heißen

$$\begin{aligned} \sigma_0(\underline{t}) &:= 1 \\ \sigma_j(\underline{t}) &:= \sum_{1 \le i_1 < i_2 < \ldots < i_j \le n} t_{i_1} \cdot \ldots \cdot t_{i_j} \quad (1 \le j \le n) \end{aligned}$$

elementarsymmetrische Funktionen in $t_1, \ldots, t_n$ ($\sigma_j = \sigma_j^{(n)}$).

Beispiele:

(1)

$$\begin{aligned} \sigma_1 &= t_1 + \ldots + t_n, \\ \sigma_2(t_1, t_2, t_3) &= t_1t_2 + t_1t_3 + t_2t_3, \\ \sigma_n(t_1, \ldots, t_n) &= t_1 \ldots t_n. \end{aligned}$$

(2) Potenzsummen:

$$S_k(\underline{t}) := \sum_{j=1}^{n} t_j^k \quad (\text{Potenzsummen}),\ (k \in \mathbb{Z}^{\ge 0}),$$

$$\begin{aligned} S_2(\underline{t}) &= t_1^2 + \ldots + t_n^2 \\ &= (t_1 + \ldots + t_n)^2 - 2\sum_{i<j} t_i\, t_j. \end{aligned}$$

Es gilt (für $n = 2$):

$$\begin{aligned} S_2 &= \sigma_1^2 - 2\sigma_2 \\ &= \sigma_1\, S_1 - 2\sigma_2, \\ S(\underline{t}) &= t_1^2 + t_2^2 \\ &= (t_1 + t_2)^2 - 2t_1t_2 \\ &= \sigma_1(\underline{t})^2 - 2\,\sigma_2(\underline{t}). \end{aligned}$$

(3)

$$\begin{aligned} f(t_1,\dots,t_n,t) &:= \prod_{i=1}^{n}(t-t_i) \\ &= \sum_{j=0}^{n}(-1)^{n-j}\,\sigma_{n-j}(\underline{t})\,t^j, \\ &= \sum_{i=0}^{n}(-1)^{i}\,\sigma_i(\underline{t})\,t^{n-i}. \end{aligned}$$

(4) Es sei $A \in \mathbb{C}^{n\times n}$ und J_c die zug. Jordan-Normal-Form Lin. Alg. 1, ??

$$J_c = \begin{pmatrix} \lambda_1 & *_1 & & \\ & \ddots & \ddots & \\ & & \ddots & *_{n-1} \\ & & & \lambda_n \end{pmatrix}$$

mit λ_i Eigenwert zu A $(1 \le i \le n)$ und $*_j \in \{0,1\}$ $(1 \le j \le n-1)$.

$$\begin{aligned} f_A &= \det(t - J_c) \\ &= \prod_{i=1}^{n}(t-\lambda_i) \\ &= \sum_{j=0}^{n}(-1)^j\,\sigma_j(\lambda_1,\dots,\lambda_n)\,t^{n-j} \end{aligned}$$

$$\sigma_1(\lambda_1\ \dots\ \lambda_n) = \mathrm{Sp}(A), \quad \sigma_n(\lambda_1\ \dots\ \lambda_n) = \det A.$$

(5) $\sigma_k^{(n)}(t_1\ \dots\ t_n) = \sigma_k^{(n+m)}(t_1\ \dots\ t_n, \underbrace{0\ \dots\ 0}_{m})$.

Bemerkung: Die symmetrischen Polynome bilden einen Unterring von $R[t_1,\dots,t_n]$. Der Einsetzungshomomorphismus

$$\Phi_{(\sigma_1\dots\sigma_n)} : R[t_1,\dots,t_n] \to R[t_1,\dots,t_n] : t_i \mapsto \sigma_i$$

$\Phi(f) = f(\sigma_1,\dots,\sigma_n)$ ist symmetrisch, d.h. $\Phi(f)$ ist symmetrisch, falls f dies war.

Falls $f(t_1,\dots,t_{n-1},0) = 0$, so folgt $\sigma_n | f$. Denn: $f(t_1,\dots,t_n) = \sum f_i(t_1,\dots,t_{n-1})t_n^i$ mit $f_i \in R[t_1,\dots,t_{n-1}]$. $f(t_1,\dots,t_{n-1},0) = 0$ impliziert $f_0(t_1,\dots,t_{n-1}) = 0$ also $t_n | f$. f symmetrisch $\Rightarrow t_i | f$ für jedes i, also $\sigma_n | f$.

Satz 2.2 (Hauptsatz über elementarsymmetrische Funktionen): Es sei R ein kommutativer Ring mit 1. Dann gibt es für jedes symmetrische Polynom $f(\underline{t}) \in R[\underline{t}]$ genau ein $g \in R[\underline{t}]$ mit $f = g(\sigma_1,\dots,\sigma_n)$.

Beweis: Wir definieren das Gewicht eines Monoms

$$g(\underline{t}) = a\,t_1^{m_1}\cdot\ldots\cdot t_n^{m_n} \text{ als } w(t_k) = k,\ w(g) := \sum_{k=1}^{n} k\,m_k.$$

Das Gewicht eines Polynoms $f \in R[\underline{t}]$ wird dann als Maximum der Gewichte seiner Monome festgelegt, d.h.

$$f = \sum a_{i_1\dots i_n}\,t_1^{i_1}\dots t_n^{i_n} =: \sum a_{\underline{i}}\underline{t}^{\underline{i}}, \quad w(f) = \max\{w(\underline{t}^{\underline{i}})\}.$$

(1) Wir zeigen: Zu $f \in R[\underline{t}]$ symmetrisch vom Grad d existiert $g \in R[t]$ mit $w(g) \leq d$ und $f(t_1, \ldots, t_n) = g(\sigma_1, \ldots, \sigma_n)$.
Der Beweis erfolgt mittels Induktion nach n.
Für $n = 1$ ist $f = g$ und $\sigma_1 = t_1$. $n-1 \Rightarrow n$: Beweis per Induktion nach $d = \deg(f)$. Für $d \leq 0$ ist f konstant und $g = f$ tut's.
Sei also $d > 0$. Dann ist

$$f^{(n-1)}(t_1, \ldots, t_{n-1}) := f(t_1, \ldots, t_{n-1}, 0)$$

mit $\deg(f^{(n-1)}) \leq d$ symmetrisch in $t_1, \ldots, t_{n-1}$. Nach Induktionsvoraussetzung über n existiert also ein Polynom $g_1(t_1, \ldots, t_{n-1}) \in R[t_1, \ldots, t_{n-1}]$ vom Gewicht $\leq d$ mit

$$f^{(n-1)}(t_1, \ldots, t_{n-1}) = g_1(\sigma_1^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}),$$

wobei $\sigma_i^{(n-1)} = \sigma_i(t_1, \ldots, t_{n-1}, 0)$ gesetzt wurde.
Hiernach ist

$$h(\underline{t}) := f(\underline{t}) - g_1(\sigma_1, \ldots, \sigma_{n-1})$$

ebenfalls symmetrisch vom Grad $\leq d$. Wegen $h(\underline{t})$ symmetrisch und

$$h(t_1, \ldots, t_{n-1}, 0) = 0$$

folgt $\sigma_n | h$, bzw. $h = \sigma_n h_1$, $\deg(h_1) = \deg(h) - n$. Wiederum ist h_1 symmetrisch vom Grad $d - n < d$. Nach Induktionsannahme existiert daher $g_2 \in R[t_1, \ldots, t_n]$ vom Gewicht $\leq d - n$ mit

$$h_1(t_1, \ldots, t_n) = g_2(\sigma_1, \ldots, \sigma_n),$$

und insgesamt leistet

$$g(\sigma_1, \ldots, \sigma_n) = g_1(\sigma_1, \ldots, \sigma_{n-1}) + \sigma_n \, g_2(\sigma_1, \ldots, \sigma_n)$$

das Verlangte.

(2) Eindeutigkeit:
Dazu zeigen wir: Für $f \in R[t_1, \ldots, t_n]$ mit $f(\sigma_1, \ldots, \sigma_n) = 0$ gilt $f = 0$.
Der Beweis erfolgt per Induktion über n.
Für $n = 1$ ist die Aussage wegen $\sigma_1 = t_1$ trivial.
Sei also $n > 1$ und $f \neq 0$ von minimalem Grad > 0 mit $f(\sigma_1, \ldots, \sigma_n) = 0$. Aus dem Ansatz

$$f(t_1, \ldots, t_n) = \sum_{i=0}^{l} f_i(t_1, \ldots, t_{n-1}) \, t_n^i$$

folgt zunächst $f_0(t_1, \ldots, t_{n-1}) \neq 0$, da sonst f durch t_n teilbar wäre, d.h.

$$f(\underline{t}) = t_n \, \tilde{f}(\underline{t}) \quad \text{mit} \quad 0 = f(\underline{\sigma}) = \sigma_n \, \tilde{f}(\underline{\sigma}),$$

im Widerspruch zur Minimalität des Grades. Daher gilt:

$$0 = f(\sigma_1, \ldots, \sigma_n) = \sum_{i=0}^{l} f_i(\sigma_1, \ldots, \sigma_{n-1}) \, \sigma_n^i.$$

Setzen wir hierin $t_n = 0$, so erhalten wir

$$0 = f(\sigma_1^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}, 0) = f_0(\sigma_1^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)})$$

im Widerspruch zur Induktionsannahme!

```
to_elementary := function(f)

  pr := Parent(f);
  n := Rank(pr);
  if n eq 1 then
    return f;
  end if;

  if f in CoefficientRing(pr) then
    return f;
  end if;

  pr1 := PolynomialRing(CoefficientRing(pr), n-1);

  red := [ pr1.x : x in [ 1..n-1] ] cat [pr1.1 * 0];
  red := hom<pr -> pr1 | red>;
  fn1 := red(f);

  g1 := $$(fn1);

  es := [ ElementarySymmetricPolynomial(pr, i) : i in [1..n-1] ];
  es := hom<pr1 -> pr | es>;
  h := f - es(g1);

  h1 := pr ! (h/ElementarySymmetricPolynomial(pr, n));
  g2 := $$(h1);

  ext := hom< pr1 -> pr | [ pr.x : x in [1..n-1]] >;

  return ext(g1) + pr.n*g2;

end function;
```

□

Beispiel:

Für

$$f(t_1, t_2, t_3) = (t_1 - t_2)^2 \, (t_1 - t_3)^2 \, (t_2 - t_3)^2$$

ist

$$\begin{aligned} f(t_1, t_2, 0) &= (t_1 - t_2)^2 \, (t_1 t_2)^2 \\ &= ((\sigma_1^{(2)})^2 - 4\,\sigma_2^{(2)}) \, (\sigma_2^{(2)})^2; \end{aligned}$$

folglich gilt $h(\underline{t}) = \sigma_3\, h_1(\underline{t})$ mit

$$\begin{aligned} h_1(t_1,t_2,0) &= 18\,\sigma_1^{(2)}\sigma_2^{(2)} - 4\,(\sigma_1^{(2)})^3 \\ h_2(\underline{t}) &= h_1(\underline{t}) - 18\,\sigma_1^{(3)}\,\sigma_2^{(3)} + 4\,\sigma_1^{(3)} \\ &= -27\,t_1t_2t_3 \\ &= -27\,\sigma_3 \end{aligned}$$

$\Rightarrow$

$$f(t_1,t_2,t_3) = \sigma_1^2\,\sigma_2^2 - 4\,\sigma_2^3 + \sigma_3\,(18\,\sigma_1\,\sigma_2 - 4\,\sigma_1^3 - 27\,\sigma_3).$$

Zusammenhang zwischen Potenzsummen und elementarsymmetrischen Funktionen:

SATZ 2.3: Für die Potenzsummen $S_k(\underline{t})$ und die elementarsymmetrischen Funktionen $\sigma_j(\underline{t})$ gelten die „Newtonschen Relationen“:

(1) $\displaystyle\sum_{i=0}^{k-1}(-1)^i\,\sigma_i(\underline{t})\,S_{k-i}(\underline{t}) + k\,(-1)^k\,\sigma_k(\underline{t}) = 0 \quad (0 \le k \le n),$

(2) $\displaystyle\sum_{i=0}^{n}(-1)^i\,\sigma_i(\underline{t})\,S_{k-i}(\underline{t}) = 0 \quad (k \ge n).$

Beweis: Für

$$f(t_1,\ldots,t_n,t) = \sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,t^{n-j} = \prod_{j=1}^{n}(t-t_j)$$

gilt (Einsetzen von $t := t_i$):

$$0 = \sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,t_i^{n-j} \quad (1 \le i \le n)$$

bzw. (Multiplikation mit t_i^{k-n})

$$0 = \sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,t_i^{k-j} \quad (1 \le i \le n,\ k \ge n).$$

Summation über i dieser n Gleichungen liefert

$$\sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,S_{k-j}(\underline{t}) = 0,$$

also (2) bzw. (1) für $k = n$. Der Rest von (1) wird bei festem k mittels Induktion nach n bewiesen:

Induktionanfang: $n = k$ ist bereits gezeigt.

$n-1 \Rightarrow n$:

Wir setzen

$$F(t_1,\ldots,t_n) := \sum_{i=0}^{k-1}(-1)^i\sigma_i(\underline{t})S_{k-i}(\underline{t}) + k(-1)^k\,\sigma_k(\underline{t})$$

und erhalten eine symmetrische Funktion F mit $\deg F \le k < n$. Nach Induktionsannahme gilt $F(t_1,\ldots,t_n,0) = 0$. Also ist $F(\underline{t})$ durch t_n — wegen der Symmetrie durch $\sigma_n(\underline{t})$ — teilbar. Wegen $\deg(F) < n$ muß F folglich identisch verschwinden. □

Beispiel:

$$\begin{aligned} S_1(\underline{t}) &= \sigma_1(\underline{t}), \\ S_2(\underline{t}) &= \sigma_1(\underline{t})\, S_1(\underline{t}) - 2\,\sigma_2(\underline{t}) \\ &= \sigma_1^2(\underline{t}) - 2\,\sigma_2(\underline{t}), \\ S_3(\underline{t}) &= \sigma_1(\underline{t})\, S_2(\underline{t}) - \sigma_2(\underline{t})\, S_1(\underline{t}) + 3\,\sigma_3(\underline{t}) \\ &= \sigma_1^3(\underline{t}) - 3\,\sigma_1(\underline{t})\,\sigma_2(\underline{t}) + 3\,\sigma_3(\underline{t}), \end{aligned}$$

usw. Sind die natürlichen Zahlen in R keine Nullteiler, so gilt in $\mathfrak{Q}(R)$ auch:

$$\begin{aligned} \sigma_1(\underline{t}) &= S_1(\underline{t}), \\ \sigma_2(\underline{t}) &= \frac{1}{2}\,(S_1(\underline{t})^2 - S_2(\underline{t})), \\ \sigma_3(\underline{t}) &= \frac{1}{3}\left(S_2(\underline{t}) - S_1(\underline{t})^3 + 3\,S_1(\underline{t})\,\frac{1}{2}\,(S_1(\underline{t})^2 - S_2(\underline{t}))\right) \\ &= \frac{1}{6}\,(2\,S_3(\underline{t}) + S_1(\underline{t})^3 - 3\,S_1(\underline{t})\,S_2(\underline{t})), \end{aligned}$$

usw.

DEFINITION 2.4 (Diskriminante): In $R[\underline{t}]$ heißt

$$D(\underline{t}) = \prod_{1\le i<j\le n} (t_i - t_j)^2$$

Diskriminante von $\underline{t}$.

Beispiel: $f := t^2+at+b : x_{1,2} := -\frac{a}{2} \pm \sqrt{\frac{a^2-4b}{4}}$ $\frac{a^2-4b}{4} = (x_1-x_2)^2$ heißt Diskriminante von f.

HILFSSATZ 2.5: In $R[\underline{t}]$ gilt:

$$D(\underline{t}) = \det\left((S_{i+j-2}(\underline{t})_{1\le i,j\le n}\right).$$

Ferner gilt $D(\underline{t}) \in R$!

Beweis in den Übungen.

SATZ 2.6 (Fundamentalsatz der Algebra): Jedes Polynom $f \in \mathbb{C}[t]$ mit $\deg(f) \ge 1$ besitzt eine Nullstelle in $\mathbb{C}$, d.h. über $\mathbb{C}$ zerfällt f in Linearfaktoren:

$$f(t) = l(f) \prod_{j=1}^{\deg(f)} (t - x_j) \quad x_j \in \mathbb{C}).$$

„$\mathbb{C}$ ist algebraisch abgeschlossen."

Beweis:

(1) Wir führen den Beweis auf die gleiche Aussage für Polynome aus $\mathbb{R}[t]$ zurück. Für $f \in \mathbb{C}$ bilden wir

$$g(t) := f(t)\,\overline{f}(t) \in \mathbb{R}[t].$$

Wir erhalten dann

$$g(t) := |l(f)|^2 \prod_{j=1}^{2\deg(f)} (t - c_j).$$

Hier ist mit c_j auch $\overline{c}_j$ Nullstelle von g (!) und wir bekommen

$$f(t) = l(f) \prod_{i=1}^{\deg(f)} (t - c_{j_i}) \quad (1 \le j_1 < j_2 < \ldots < j_{\deg(f)} \le 2\deg(f)).$$

(2) Wir zeigen: Jedes Polynom

$$f(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \ldots + (-1)^n a_n \in \mathbb{R}[t]$$

mit $n \geq 1$ besitzt in $\mathbb{C}$ eine Nullstelle.
Für n ungerade folgt dies aus dem Zwischenwertsatz der Analysis.
Sei also n von der Form $2^k q$ mit $k \in \mathbb{Z}^{\geq 0}$, q ungerade, $q \in \mathbb{N}$.
Wir führen den Beweis mittels Induktion nach k. Induktionsanfang: $k = 0$ ist bereits geklärt.
Sei nun $k \geq 1$ und die Behauptung für $1, \ldots, k-1$ bereits bewiesen. Nach Algebra 1, 2.67 existiert ein Erweiterungskörper K von $\mathbb{R}$ mit

$$f(t) = l(f) \prod_{j=1}^{n} (t - x_j)$$

in $K[t]$. Wir bilden nun für jede reelle Zahl r das Polynom

$$L_r(t) := \prod_{1 \leq \mu < \nu \leq n} (t - x_\mu - x_\nu - r\, x_\mu x_\nu) \ \in K[t]$$

Hierbei ist L_r eine symmetrische Funktion in $x_1, \ldots, x_n$, also sind die Koeffizienten reelle Polynome in den elementarsymmetrischen Funktionen $\sigma_j(\underline{x}) = (-1)^j a_j$, d.h. es gilt $L_r(t) \in \mathbb{R}[t]$. Wegen

$$\deg(L_r) = \frac{n}{2}(n-1) = 2^{k-1} q (2^k q - 1) = 2^{k-1} \tilde{q},$$

$\tilde{q}$ ungerade, besitzt L_r für jedes $r \in \mathbb{R}$ eine Nullstelle in $\mathbb{C}$. Für jedes $r \in \mathbb{R}$ existieren also Indizes μ, ν mit

$$z_r := x_\mu + x_\nu + r\, x_\mu x_\nu \ \in \mathbb{C}.$$

Da die Anzahl der Indexpaare μ, ν endlich, die der $r \in \mathbb{R}$ unendlich ist, existieren $r \neq \tilde{r}$ in $\mathbb{R}$, $1 \leq \mu < \nu \leq n$ mit

$$x_\mu + x_\nu + r\, x_\mu x_\nu,\ x_\mu + x_\nu + \tilde{r}\, x_\mu x_\nu \ \in \mathbb{C}.$$

Hieraus folgt $x_\mu + x_\nu \in \mathbb{C}$, $x_\mu x_\nu \in \mathbb{C}$, d.h. x_μ, x_ν sind Nullstellen von

$$t^2 - (x_\mu + x_\nu)\, t + x_\mu x_\nu \ \in \mathbb{C}[t],$$

also x_μ, $x_\nu \in \mathbb{C}$. da sich in $\mathbb{C}$ Quadratwurzeln ziehen lassen.

□

KOROLLAR 2.7: Jedes Polynom $f \in \mathbb{R}[t]$ mit $\deg(f) \geq 1$ besitzt eine — bis auf Reihenfolge der Faktoren — eindeutige Darstellung

$$f(t) = l(f) \prod_{i=1}^{k} (t - c_i) \prod_{j=1}^{l} q_j(t)$$

($c_i \in \mathbb{R}$, $q_j(t) = t^2 + u_j t + v_j \in \mathbb{R}[t]$ irreduzibel $(1 \leq j \leq l)$).

Beweis:

Es seien $c_1, \ldots, c_k$ alle reellen Nullstellen von f, und es sei g durch

$$f(t) = l(f) \prod_{i=1}^{k} (t - c_i)\, g(t)$$

eindeutig bestimmt. Da für jede Nullstelle x von g wegen

$$0 = \sum_{\nu=0}^{m} g_\nu \, x^\nu = \sum_{\nu=0}^{m} \overline{g}_\nu \, \overline{x}^\nu = \sum_{\nu=0}^{m} g_\nu \, \overline{x}^\nu$$

für

$$g(t) = \sum_{\nu=0}^{m} g_\nu \, t^\nu$$

auch $\overline{x}$ Nullstelle ist, ist $\deg(g)$ gerade! Es seien $z_1, \ldots, z_l, \overline{z}_1, \ldots, \overline{z}_l$ alle Nullstellen von g in $\mathbb{C}$. Dann setzen wir

$$q_j(t) = t^2 - (z_j + \overline{z}_j)\, t + z_j \, \overline{z}_j \ \in \mathbb{R}[t] \ (1 \leq j \leq l).$$

Eindeutigkeit: Ist $x_j \in \mathbb{R}$ Nullstelle von f so gilt $(t - x_j) \mid f(t)$. Ist $z_j \in \mathbb{C}\backslash\mathbb{R}$ Nullstelle von f, dann auch $\overline{z}_j$, und es gilt

$$\mathbb{R}[t] \ni \ (t^2 - (z_j + \overline{z}_j)\, t + z_j \, \overline{z}_j) \mid f(t).$$

□

Korollar 2.8: Die irreduziblen Elemente von $\mathbb{C}[t]$ sind die Polynome ersten Grades aus $\mathbb{C}[t]$. Die irreduziblen Elemente von $\mathbb{R}[t]$ sind die Polynome ersten Grades und diejenigen Polynome $c(t^2 + ut + v)$ zweiten Grades mit $u^2 - 4v < 0$.

Satz 2.9: Es sei K ein unitärer nullteilerfreier kommutativer Oberring von $\mathbb{R}$, in dem jedes Element algebraisch über $\mathbb{R}$ ist. Dann ist K isomorph zu $\mathbb{R}$ oder $\mathbb{C}$.

Beweis:

Es sei $K \neq \mathbb{R}$. Für $x \in K\backslash\mathbb{R}$ ist $V := \mathbb{R}1 + \mathbb{R}x$ ein zweidimensionaler $\mathbb{R}$-Vektorraum. Ferner existiert $0 \neq f \in \mathbb{R}[t], \ \deg(f) \geq 1$, mit $f(x) = 0$. Da K nullteilerfrei ist, folgt bereits, daß x Nullstelle eines normierten Polynoms zweiten Grades ist: $g(x) = 0$ für

$$g(t) = t^2 + ut + v \ \in \mathbb{R}[t] \ \ (u^2 - 4v < 0).$$

Also gilt: $x^2 = -ux - v$ in K. Damit läßt sich V mittels $V \cong \mathbb{R}[t]/(g)$ zu einem RIng machen. (V ist Ring der Gleichung $g = 0$) Also ist V ein kommutativer nullteilerfreier unitärer Oberring von $\mathbb{R}$ mit 2-elementiger Basis. V ist (als Ring) zu $\mathbb{C}$ isomorph durch den $\mathbb{R}$-Isomorphismus

$$\phi : a + bx \mapsto a + \frac{b}{2}(-u + iD) \quad \text{für} \quad D = \sqrt{4v - u^2}.$$

Nach Algebra 1, Bemerkung (iii) nach 2.64 ist ϕ ein Ringhomomorphismus da $-u + iD$ eine Nullstelle von g in $\mathbb{C}$ ist. Da $\operatorname{Im}\phi$ offensichtlich 2 dimensional über $\mathbb{R}$ ist, folgt das ϕ ein Isomorphismus (zunächst als $\mathbb{R}$-Vektorraum, dann als Ringisomorphismus) ist.

Es bleibt $K = V$ zu zeigen. Es seien dazu $y \in K\backslash\mathbb{R}$ beliebig, $f \in \mathbb{R}[t]$ mit $f(y) = 0$. Über $V \cong \mathbb{C}$ zerfällt f in Linearfaktoren $t - \lambda$ ($\lambda \in V$), also folgt $y = \lambda$ für passende Wahl von λ. □

Satz 2.10: Jede endliche Untergruppe G der multiplikativen Gruppe $K^\times$ eines Körpers K ist zyklisch.

Beweis:

Es sei $|G| = n$ und $m \in \mathbb{N}$ minimal mit $x^m = 1 \ \forall x \in G$. Dann existiert hierzu ein Element $a \in G$ mit $\operatorname{ord}(a) = m$ (vergleiche Übungen, Blatt 3, Aufgabe 1). Wegen

$m|n$ ist sicherlich $m \leq n$. Andererseits sind alle $x \in G$ Nullstellen von $t^m - 1$, woraus $m \geq n$ folgt. Insgesamt gilt daher $m = n$ und $G = \langle a \rangle$. □

DEFINITION 2.11 (Derivation): Es sei R (kommutativer) Ring mit 1. $D : R \to R$ heißt Derivation, falls

$$D(a+b) = D(a) + D(b), \quad D(ab) = D(a)\,b + a\,D(b) \quad \forall a, b \in R$$

gilt.

Beispiel: $D : R[t] \to R[t] \; : \; f \mapsto f'$.

KAPITEL 3

Körper

DEFINITION 3.1: Es sei L/K eine Körpererweiterung. Ein Polynom $f \in K[t]$ heißt *separabel*, falls für jeden irreduziblen Faktor g von f gilt: $\mathrm{ggT}(g, g') = 1$. Ein über K algebraisches Element $x \in L$ heißt *separabel* über K, falls sein Minimalpolynom $m_{x/K}$ separabel ist. Schließlich heißt L/K *separabel*, falls L/K algebraisch und jedes $x \in L$ separabel über K ist. Ist L/K algebraisch und nicht separabel, heißt L/K *inseparabel*. Ein Körper K heißt *vollkommen*, falls er keine inseparablen Erweiterungskörper besitzt.

SATZ 3.2: Genau die Körper K mit $\chi(K) = p$ und $K^p = K$ und die Körper der Charakteristik 0 sind vollkommen.

Beweis: Es sei $\chi(K) = 0$ und L eine algebraische Erweiterung von K.

Ist dann $x \in L$, so folgt $\mathrm{ggT}(m_x, m_x') = 1$, also $m_x'(x) \neq 0$, x ist über K separabel.

Andererseits sei $\chi(K) = p$. Wir unterscheiden zwei Fälle.

(1) $K^p := \{x^p \mid x \in K\} = K$.
Wir nehmen an, daß $x \in L$ inseparabel über K ist. Dann folgt $m_x' = 0$ und $m_x(t) = \sum_{i=0}^{n} a_i t^{pi}$. Wegen $a_i = \tilde{a}_i^p \quad (0 \leq i \leq n)$ folgt $m_x(t) = \sum_{i=0}^{n} \left(\tilde{a}_i\, t^i\right)^p = \left(\sum_{i=0}^{n} \tilde{a}_i\, t^i\right)^p$ im Widerspruch zur Irreduzibilität von m_x.
- Also ist in diesem Fall L/K separabel.

(2) Es sei K vollkommen.
Zu $a \in K$ betrachten wir das Polynom $t^p - a \in K[t]$.
Wir nehmen an, daß es keine Wurzel in K besitzt. Ist nun $g \in K[t]$ ein irreduzibler Teiler von $t^p - a$, so bilden wir eine Erweiterung L/K, in der g eine Nullstelle b besitzt. In $L[t]$ ist dann $t^p - a = t^p - b^p = (t-b)^p$, d.h. $g(t) = (t-b)^m$ für einen Exponenten $m \in \mathbb{Z}^{\geq 2}$. Dann ist jedoch b eine mehrfache Nullstelle des irreduziblen Polynoms $g \in K[t]$ im Widerspruch zur Vollkommenheit von K. Also muß $K^p = K$ gelten.

□

KOROLLAR 3.3: Alle endlichen Körper sind vollkommen.

Beweis: Die *Frobenius-Abbildung* $x \mapsto x^p$ ist dort wegen der Endlichkeit notwendig surjektiv. □

Beispiel eines nicht vollkommenen Körpers: $\mathbb{F}_q(t)$, $t \neq \left(\frac{f(t)}{g(t)}\right)^p$.

Bemerkung:

Algebraische Erweiterungen vollkommener Körper sind separabel.

Definition 3.4: $a \in L$ heißt *rein inseparabel* über K, falls $m_a(t) = (t-a)^m$ für ein $m \in \mathbb{N}$ gilt.

Im weiteren werden wir uns mit inseparablem Erweiterungen beschäftigen. Ab jetzt gilt für alle Körper:

$$\chi(K) = p > 0.$$

Satz 3.5: Es sei $a \in L$ rein inseparabel über K. Dann gilt:
(1) $\deg(m_a) = p^e$ für passendes $e \in \mathbb{Z}^{\geq 0}$.
(2) $\deg(m_a) = p^e \Rightarrow a^{p^e} \in K \wedge a^{p^f} \notin K$ für $0 \leq f < e$.

Beweis:

(1) $m_a(t) = (t-a)^m$ ist in $K[t]$ irreduzibel.
Es sei $m = p^e\tilde{m}$ mit $p \nmid \tilde{m}$. Dann folgt

$$(t-a)^m = (t^{p^e} - a^{p^e})^{\tilde{m}} = t^{p^e m} - a^{p^e}\tilde{m}t^{p^e(m-1)} + \ldots \in K[t]$$

also $\tilde{m}a^{p^e} \in K$ bzw. $a^{p^e} \in K$.
Folglich ist $t^{p^e} - a^{p^e} \in K[t]$ und notwendig $\tilde{m} = 1$.
(2) Für $a^{p^f} \in K$ ist $(t-a)^{p^f} = t^{p^f} - a^{p^f} \in K[t]$ mit Nullstelle a. □

Definition 3.6: L/K heißt *rein inseparabel*, falls L/K algebraisch und jedes Element aus L rein inseparabel über K ist.

Korollar 3.7: Ist L/K endlich und L/K rein inseparabel $\Rightarrow$ $[L : K]$ ist p-Potenz.

Beweis: L/K endlich $\Rightarrow L = K(\alpha_1, \ldots, \alpha_r)$ mit algebraischen Elementen α_i. Setze $K_i := K(\alpha_1, \ldots, \alpha_i)$, $K_0 = K, K_r = L$.

α_1 rein inseparabel über $K \Rightarrow [K_1 : K_0] = \deg(m_{\alpha_1}) = p^{e_1}$.

Ist α_i rein inseparabel über K, so folgt $m_{\alpha_i}(t) = (t-\alpha_i)^{p^{e_i}} \in K[t]$, also ist das Minimalpolynom von α_i/K_{i-1} eine Potenz von $t - \alpha_i$, α_i/K_{i-1} rein inseparabel, $[K_i : K_{i-1}]$ ist p-Potenz.

Also folgt die Behauptung nach dem Gradsatz. □

Satz 3.8: $a \in K \setminus K^p \Rightarrow t^{p^e} - a \in K[t]$ irreduzibel für jedes $e \in \mathbb{Z}^{\geq 0}$.

Beweis: Es sei $g(t)$ ein irreduzibler Teiler von $t^{p^e} - a$ in $K[t]$.

Dann gibt es dazu eine Erweiterung L/K vom Grad $\deg(g)$, in der $g(t)$ eine Nullstelle β besitzt. Also ist auch $\beta^{p^e} = a$, $t^{p^e} - a = (t-\beta)^{p^e}$ in $L[t]$. Folglich ist β rein inseparabel über K, also $g(t) = (t-\beta)^{p^f}$ für ein $f \in \mathbb{Z}^{\geq 0}$, $0 \leq f \leq e$.

Ferner ist $a = \beta^{p^e} = \beta^{p^f p^{e-f}} = c^{p^{e-f}}$ für $c = \beta^{p^f} \in K$.

Nach Voraussetzung muß also $e = f$ gelten. □

Hilfssatz 3.9: $a \in L$ mit $a^{p^e} \in K$ für ein $e \in \mathbb{Z}^{\geq 0} \Rightarrow a$ rein inseparabel über K.

Beweis: Setze $b = a^{p^e}$. Dann ist a Nullstelle von $t^{p^e} - b \in K[t]$, also $t^{p^e} - b = (t-a)^{p^e}$ in $L[t]$.

Das Minimalpolynom von a ist demnach eine Potenz von $t-a$ und demnach a über K inseparabel. □

Hilfssatz 3.10: $a \in L$ separabel und rein inseparabel über $K \Rightarrow a \in K$.

Beweis: $a \in L$ rein inseparabel über $K \Rightarrow m_a(t) = t^{p^e} - b$ für passendes $b \in K$ und ein $e \in \mathbb{Z}^{\geq 0}$.

a separabel impliziert $m_a'(t) \neq 0$, also $e = 0$ und somit $a = b$. □

Satz 3.11: L/K separabel $\Rightarrow KL^p = L$.
L/K endlich mit $KL^p = L \Rightarrow L/K$ separabel.

Beweis: Zunächst sei L/K separabel.

Wegen $L^p \subseteq KL^p \subseteq L$ ist $\alpha^p \in KL^p$ für alle $\alpha \in L$, also ist jedes solche α nach 3.9 rein inseparabel über KL^p.

Ist andererseits $m_\alpha(t) \in K[t]$ Minimalpolynom von α/K (L/K separabel!), so besitzt $m_\alpha(t)$ in keinem Erweiterungskörper mehrfache Nullstellen.

Dies gilt dann natürlich auch für $m_{\alpha/KL^p}(t) \in KL^p[t]$, welches ja $m_\alpha(t)$ in $KL^p[t]$ teilt. Also ist α/KL^p (und damit L/KL^p) separabel. Nach 3.10 ist damit $\alpha \in KL^p$ und die behauptete Gleichheit folgt.

Es sei nunmehr L/K endlich mit $L = KL^p$. Wir nehmen an, daß $\alpha \in L$ mit $m_\alpha(t) \in K[t]$ existiert, welches über K nicht separabel ist. Es muß notwendig $m_\alpha(t) = \sum_{i=0}^{m} a_{ip}\, t^{ip}$ $(a_{mp} = 1)$ gelten!

Dies bedeutet, daß $1, \alpha^p, \ldots, \alpha^{mp} \in L$ K-linear abhängig sind. Ferner sind $1, \alpha, \ldots, \alpha^m \in L$ K-linear unabhängig wegen $\deg(m_\alpha) = mp > m$.

Es sei nun $\omega_1, \ldots, \omega_n$ eine Basis von L/K. Also ist für $\beta \in L$:

$$\begin{aligned} \beta &= b_1\,\omega_1 + \ldots + b_n\,\omega_n \in K\omega_1 + \ldots + K\omega_n = L, \\ \beta^p &= b_1^p\,\omega_1^p + \ldots + b_n^p\,\omega_n^p, \end{aligned}$$

also ist $\omega_1^p, \ldots, \omega_n^p$ ein Erzeugendensystem von L^p/K^p. Nach Voraussetzung gilt:

$$\begin{aligned} L = KL^p &= K(K^p\omega_1^p + \ldots + K^p\omega_n^p) \\ &\subseteq K\omega_1^p + \ldots + K\omega_n^p \subseteq L, \end{aligned}$$

folglich ist auch $\omega_1^p, \ldots, \omega_n^p$ eine Basis von L/K.

Ergänzen wir also $1, \alpha, \ldots, \alpha^m$ zu einer Basis $1, \alpha, \ldots, \alpha^m, \beta_{m+1}, \ldots, \beta_{n-1}$ von L/K, so ist $1, \alpha^p, \ldots, \alpha^{mp}, \beta_{m+1}^p, \ldots, \beta_{n-1}^p$ wieder eine, und speziell sind $1, \alpha^p, \ldots, \alpha^{mp}$ k-linear unabhängig. □

KOROLLAR 3.12: (1) Die folgenden Aussagen für $\alpha \in L/K$ algebraisch sind äquivalent:
(a) $K(\alpha) = K(\alpha^p)$,
(b) $K(\alpha)/K$ ist separabel,
(c) α/K ist separabel.
(2) M/L und L/K endlich separabel $\Rightarrow$ M/K endlich separabel.
(3) $\alpha_1, \dots, \alpha_r \in L$ über K separabel $\Rightarrow$ $K(\alpha_1, \dots, \alpha_r)/K$ separabel.
(4) M/L und L/K separabel $\Rightarrow$ M/K separabel.
(5) Für L/K beliebige Erweiterung ist

$$\begin{aligned} L_{\text{sep}} &= \{\alpha \in L \mid \alpha/K \text{ separabel}\} \\ &= L_{sep/K} \end{aligned}$$

ein Teilkörper von L, der K enthält.

Beweis:

(1) (a) $\Rightarrow$ (b)
Es ist $K(\alpha) = K(\alpha^p)$ und $K(\alpha)/K$ endlich.
Es gilt $K(K(\alpha))^p = KK^p(\alpha^p) = K(\alpha^p) = K(\alpha)$, und die Behauptung folgt mittels 3.11.
(b) $\Rightarrow$ (c) trivial.
(c) $\Rightarrow$ (a) $\alpha \in L$ ist über K separabel, also über $K(\alpha^p)$.
Wegen $\alpha^p \in K(\alpha^p)$ ist $\alpha/K(\alpha^p)$ rein inseparabel.
Folglich ist $\alpha \in K(\alpha^p)$ und $K(\alpha) \subseteq K(\alpha^p) \subseteq K(\alpha)$.
(2) Wir haben $LM^p = M$, $KL^p = L$, $L^p \subseteq M^p$, folglich $KM^p = KL^pM^p = LM^p = M$ und M/K ist nach 3.11 separabel.
(3) Setze $K_0 = K$, $K_i = K(\alpha_1, \dots, \alpha_i)$ mit $K_r = L$.
Nach (1) ist K_1/K_0 separabel. Ferner ist α_i/K_0 und damit über K_{i-1} separabel, also K_i/K_{i-1}. Damit folgt die Behauptung nach (2).
(4) Es sei $\alpha \in M$. α/L ist separabel mit Minimalpolynom $m_{\alpha/L}(t) = \sum_{i=0}^{m} a_i\, t^i$.
Hierbei sind $a_0, \dots, a_m$ über K separabel.
Also ist $\hat{L} := K(a_0, \dots, a_m)$ über K nach (3) separabel.
Ferner ist $m_{\alpha/\hat{L}}(t) = m_{\alpha/L}(t)$ wegen $\hat{L} \subseteq L$, also $\alpha/\hat{L}$ separabel.
Demnach ist nach (1) $\hat{L}(\alpha)/\hat{L}$ und somit $\hat{L}(\alpha)$ nach (3) über K separabel, also ist α/K separabel.
(5) Sind $\alpha, \beta \in L$ über K separabel, so ist $K(\alpha, \beta)/K$ separabel nach (3), also sind $\alpha \overset{+}{\cdot} \beta$, $\alpha\,\beta^{-1}$ (für $\beta \neq 0$) separabel über K.
L_{sep} ist somit Körper. $K \subseteq L_{\text{sep}}$ folgt nach 3.10. □

Bemerkungen:

$L_{\text{sep}} = L_{sep/K}$ heißt *separabler Abschluß* (*separable Hülle*) von K in L.

SATZ 3.13: Es sei L/K algebraisch. Dann ist L/L_{sep} rein inseparabel.

Beweis: Es sei $\alpha \in L$ über K inseparabel mit $m_\alpha(t) \in K[t]$. Es folgt $m_\alpha(t) = f_1(t^p)$ mit $f_1(t) \in K[t]$. Hierbei ist $f_1(t)$ natürlich irreduzibel, es ist $f_1(t) = m_{\alpha^p}(t)$.

Ist α^p nicht separabel über K, folgt $f_1(t) = f_1(t^p)$ mit $f_1(t) \in K[t]$, $f_1(t) = m_{\alpha^{p^2}}(t)$.

Nach endlich vielen Schritten ($\deg(m_\alpha) < \infty$) erhalten wir $f_e(t) = m_{\alpha^{p^e}}(t) \in K[t]$ mit α^{p^e}/K separabel. Also ist $\alpha^{p^e} \in L_{\text{sep}}$ (und p^e ist der minimale Exponent mit dieser Eigenschaft). Also ist α/L_{sep} rein inseparabel nach 3.9. □

Bemerkungen:

$[L_{\text{sep}} : K]$ heißt *Separabilitätsgrad* von $L/K =: [L : K]_{\text{sep}}$,

$[L : L_{\text{sep}}]$ heißt *Inseparabilitätsgrad* von $L/K =: [L : K]_i$.

Ist $[L : K]_i < \infty$, so ist es nach 3.7 Potenz der Charakteristik.

Ist $\chi(K) = 0$, so kann man alles ähnlich formulieren, nur ist stets $L_{\text{sep}} = L$, $[L : K]_i = 1$.

Satz 3.14: L/K endlich, $p \nmid [L : K] \Rightarrow L/K$ separabel.

Beweis: Ist $\alpha \in L \backslash K$ über K inseparabel, so ist $[K(\alpha) : K] = \deg(m_\alpha)$ ein p-Vielfaches, das $[L : K]$ teilt. □

Es sei L/K algebraisch und $\alpha \in L$ mit $n = \deg(m_\alpha)$. Es sei e maximal mit $m_\alpha(t) \in K[t^{p^e}]$ und $n = n_0\, p^e$. Dann heißen n_0 der *reduzierte Grad* von $m_\alpha(t)$ $(\deg_r(m_\alpha))$ und p^e der *Inseparabilitätsgrad* von m_α $(\deg_i(m_\alpha))$.

Satz 3.15: Es sei $f(t) \in K[t]$ irreduzibel mit $n = n_0 p^e$ und $L = K(\alpha)$ für eine Wurzel α von $f(t)$.
Dann gilt: $[L : K]_{\text{sep}} = n_0, \quad [L : K]_i = p^e$.

Beweis: Es ist α^{p^e}/K separabel mit $\deg(m_{\alpha^{p^e}}) = n_0$.

Also ist für $K_1 = K(\alpha^{p^e})$: $[K_1 : K] = n_0$, $[L : K_1] = p^e$ und $K_1 \subseteq L_{\text{sep}}$.

Es bleibt Gleichheit zu zeigen. Sei also $\beta \in L_{\text{sep}}$. Dann ist β über K und somit über K_1 separabel.

Ferner ist L/K_1 rein inseparabel (Übungen), also β/K_1 rein inseparabel. Folglich ist $\beta \in K_1$.

Übung:

α/K rein inseparabel $\Rightarrow [K(\alpha) : K]$ rein inseparabel. Denn sei $\alpha^{p^e} \in K$.

Ist $\gamma \in K(\alpha)$, also $\gamma = \sum_{i=0}^{m} c_i \alpha^i$, so ist $\gamma^{p^e} = \sum_{i=0}^{m} c_i^{p^e} (\alpha^{p^e})^i$ aus K. Also ist $m_\gamma(t)$ ein Teiler von $t^{p^e} - \gamma^{p^e} = (t - \gamma)^{p^e}$ (in $L[t]$), γ daher rein inseparabel über K. □

Ab hier ist $\chi(K) = 0$ wieder erlaubt!

Korollar 3.16: Es sei L/K algebraisch. L/K ist normal, falls jedes Element von L in einem Zerfällungskörper M eines Polynoms aus $K[t]$ enthalten ist, für den $M \subseteq L$ gilt.

Beweis: Es sei $\alpha \in L$ mit $m_\alpha(t) \in K[t]$. Dann ist α im Zerfällungskörper von $m_\alpha(t) \in K[t]$, etwa M, enthalten, und es gilt $M \subseteq L$. M ist über K normal, also zerfällt $m_\alpha(t)$ in M (und damit in L) in Linearfaktoren. □

(Beachte, jedes irreduzible Polynom aus $K[t]$, welches in L eine Wurzel besitzt, ist - nach Normierung - Minimalpolynom von einem $\alpha \in L$.)

Bemerkung:

M/K normal, $K \subset L \subset M \Rightarrow L/M$ normal (Beweis in den Übungen).

Satz 3.17: Es seien L/K endlich, M/K normal mit $L \subseteq M$.
Es sei $n_0 = [L : k]_{\text{sep}}$. Dann gibt es genau n_0 verschiedene K-Isomorphismen von L auf Teilkörper von M.

Beweis: Gemäß Algebra 1, 3.30 können wir $[M : K] < \infty$ wählen, da die möglichen Bilder von Elementen aus L bereits in der minimalen normalen Erweiterung M/K liegen!

Wir beweisen den Satz mittels Induktion über n_0.

$n_0 = 1 : L/K$ ist rein inseparabel. $\chi(K) = 0 \Rightarrow L = K$, die Identität ist die einzig mögliche Abbildung.

$\chi(K) = p$: Für $\alpha \in L$ ist $\alpha^{p^e} \in K$ bei passendem $e \in \mathbb{Z}^{\geq 0}$, jeder K-Isomorphismus σ leistet $\sigma(\alpha)^{p^e} = \sigma(\alpha^{p^e})$, also $(\sigma(\alpha) - \alpha)^{p^e} = 0$ und $\sigma(\alpha) = \alpha$.

Also gibt es auch hier nur die Möglichkeit $\sigma = \mathrm{id}_L$.

Sei nun $n_0 > 1$. Zunächst betrachten wir den Fall, daß L/K einfach ist, also $L = K(\alpha)$ gilt. Es ist $m_\alpha(t) = f(t^{p^e})$ mit $e = 0$ für α/K separabel. Im Zerfällungskörper von m_α, also speziell in M, gilt dann

$$m_\alpha(t) = \prod_{j=1}^{n_0} (t^{p^e} - \tilde{\alpha}_j), \quad \text{in } L_{\text{sep}} \;\; m_\alpha(t) = \prod_{j=1}^{n_0} (t - \alpha_j)^{p^e}.$$

Hierbei sind die α_j paarweise verschieden. Ein K-Isomorphismus σ von L kann demnach α nur auf ein α_j abbilden („Konjugierte“ von α), und σ ist durch die Vorgabe des Bildes $\sigma(\alpha)$ bereits eindeutig festgelegt. Also gibt es genau n_0 verschiedene K-Isomorphismen von L in M:

$$\sigma_j : K(\alpha) \to K(\alpha_j) : \alpha \mapsto \alpha_j.$$

Schließlich sei $n_0 > 1$ und der Satz für $[L : K]_{\text{sep}} < n_0$ bereits bewiesen. Nach Voraussetzung existieren in L über K separable Elemente, die nicht selbst in K liegen. Wähle ein solches $\alpha \in L_{\text{sep}/K} : K \subset K(\alpha) \subseteq L_{sep/K} \subseteq L \subseteq M$. Nun ist M auch über $K(\alpha)$ normal, und es ist $[L : K(\alpha)]_{\text{sep}} = r < n_0$. Nach Induktionsannahme existieren gerade r $K(\alpha)$-Isomorphismen $\tau_1, \ldots, \tau_r$ von L in M. Ferner existieren gerade $s := [K(\alpha) : K]$ K-Isomorphismen σ_i von $K(\alpha)$ in M, und wir haben $n_0 = [L : K]_{\text{sep}} = [L_{\text{sep}} : K(\alpha)]\,[K(\alpha) : K] = rs$.

Nach Satz Algebra 1, 3.29 kann jedes $\sigma_i \quad (1 \leq i \leq s)$ zu einem K-Automorphismus $\bar{\sigma}_i$ von M fortgesetzt werden.

Man beachte, daß wir $\bar{\sigma}_i$ zwar fest wählen können, $\bar{\sigma}_i$ jedoch i.a. nicht eindeutig ist.

Wir erhalten somit $n_0 = rs$ K-Isomorphismen von L in M mittels:

$$\sigma_{ij} := \bar{\sigma}_i \tau_j \quad (1 \leq i \leq s,\ 1 \leq j \leq r).$$

Ist nun ϕ irgendein K-Isomorphismus von L in M, so ist $\phi\,|_{K(\alpha)} = \sigma_{i_0}$ für ein $i_0 \in \{1, \dots, s\}$.

Also läßt $\bar{\sigma}_{i_0}^{-1}\,\phi : L \to M$ gerade $K(\alpha)$ fest, d.h. $\bar{\sigma}_{i_0}^{-1}\,\phi = \tau_{j_0}$ für ein $j_0 \in \{1, \dots, r\}$.

Also ist insgesamt $\phi = \bar{\sigma}_{i_0}\,\tau_{j_0}$.

Wir haben noch $\sigma_{ij} \neq \sigma_{kl}$ für $(i,j) \neq (k,l)$ zu zeigen. Sei also $\sigma_{ij} = \sigma_{kl}$, also $\bar{\sigma}_i\,\tau_j = \bar{\sigma}_k\,\tau_l$ bzw. $\bar{\sigma}_k^{-1}\,\bar{\sigma}_i\,\tau_j = \tau_l$. Die Einschränkung auf $K(\alpha)$ liefert $\bar{\sigma}_k^{-1}\bar{\sigma}_i\,|_{K(\alpha)} = \mathrm{id}$ bzw. $\sigma_i = \bar{\sigma}_i\,|_{K(\alpha)} = \bar{\sigma}_k\,|_{K(\alpha)} = \sigma_k$, also $i = k$. Danach ist dann auch $\bar{\sigma}_i = \bar{\sigma}_k$ und $\tau_j = \tau_l$, folglich $j = l$. □

Bemerkungen:

(1) Isomorphe Teilkörper heißen „Konjugierte“.
Ist M/K normal und endlich, so hat L als Zwischenkörper mit $[L:K]_{\mathrm{sep}} =: n_0$ maximal n_0 verschiedene K-Konjugierte.
(2) Ist M/K eine endliche normale Erweiterung, so ist $\#G(M/K) = [M:K]_{\mathrm{sep}}$.

SATZ 3.18: Es sei M/K endlich und normal.
Ist für $\alpha \in M : \sigma(\alpha) = \alpha\,\forall\,\alpha \in G(M/K)$, dann ist α über K rein inseparabel.

Beweis: Das Minimalpolynom von α kann nur eine Wurzel haben. □

Bemerkungen: Ist L/K endlich und normal, so ist $F := \{\alpha \in L \,|\, \sigma(\alpha) = \alpha\,\forall\,\sigma \in G(L/K)\}$ ein Körper(!), der K enthält. Nach 3.18 ist F/K rein inseparabel. Ferner ist L/F separabel, wie wir im Rahmen der Galoistheorie bald zeigen werden.

Normen und Spuren

Im folgenden sei L/K endlich mit $[L:K]_{\mathrm{sep}} = n_0$ und Γ/K endlich und normal mit $\Gamma \supseteq M$ fixiert. Gemäß 3.17 existieren gerade n_0 K-Isomorphismen $\sigma_1, \dots, \sigma_{n_0}$ von L auf Teilkörper von Γ, die K enthalten.

DEFINITION 3.19: Für Elemente $\alpha \in L$ definieren wir *Norm*

$$N_{L/K}(\alpha) = \left(\prod_{j=1}^{n_0} \sigma_j(\alpha)\right)^{[L:K]_i}$$

und *Spur*(*Trace*)

$$\mathrm{Tr}_{L/K}(\alpha) = [L:K]_i \sum_{j=1}^{n_0} \sigma_j(\alpha).$$

HILFSSATZ 3.20: Ist $m_{\alpha/K}(t) = t^r + c_1\,t^{r-1} + \dots + c_r \in K[t]$, so gilt

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \left((-1)^r\,c_r\right)^{[L:K(\alpha)]}, \\ \mathrm{Tr}_{L/K}(\alpha) &= -[L:K(\alpha)]c_1. \end{aligned}$$

Bemerkung: Für einen Körperturm $M/L/K$ gilt $[M:K]_x = [M:L]_x[L:K]_x$ für $x \in \{\ , \mathrm{sep}, i\}$.

Beweis: Es sei $m_0 = [K(\alpha):K]_{\mathrm{sep}}$. Also existieren gerade $\tau_1, \dots, \tau_{m_0}$ K- Isomorphismen von $K(\alpha)$ in Teilkörper von Γ. Deren Fortsetzungen (fixiert!) zu Γ-Automorphismen seien $T_1, \dots, T_{m_0}$. Ist $r_0 = [L:K(\alpha)]_{\mathrm{sep}}$, so existieren genau r_0 $K(\alpha)$-Isomorphismen κ_j von L auf Teilkörper von Γ, und wie im Beweis zu 3.17 sind dann $\rho_{ij} := T_i\,\kappa_j$ alle K-Isomorphismen von L. Also erhalten wir:

$$\begin{array}{rcl} \mathrm{N}_{L/K}(\alpha) & = & \left(\prod_{i=1}^{m_0}\prod_{j=1}^{r_0} T_i\,\kappa_j(\alpha)\right)^{[L:K]_i} = \left(\prod_{j=1}^{m_0}\tau_j(\alpha)\right)^{r_0[L:K]_i}, \\ \mathrm{Tr}_{L/K}(\alpha) & = & [L:K]_i\sum_{i=1}^{m_0}\sum_{j=1}^{r_0} T_i\,\kappa_j(\alpha) = r_0[L:K]_i\sum_{i=1}^{m_0}\tau_i(\alpha) \\ & = & [L:K(\alpha)]_{\mathrm{sep}}\,[L:K(\alpha)]_i\,[K(\alpha):K]_i\sum_{i=1}^{m_0}\tau_i(\alpha) \\ & = & [L:K(\alpha)]\,[K(\alpha):K]_i\sum_{i=1}^{m_0}\tau_i(\alpha) \quad . \end{array}$$

Andererseits ist in $\Gamma[t]$:

$$m_{\alpha/K}(t) = \left(\prod_{i=1}^{m_0}\left(t-\tau_i(\alpha)\right)\right)^{[K(\alpha):K]_i}, \text{ also}$$

$$c_r = \left((-1)^{m_0}\left(\prod_{i=1}^{m_0}\tau_i(\alpha)\right)\right)^{[K(\alpha):K]_i}, c_1 = -\,[K(\alpha):K]_i\sum_{i=1}^{m_0}\tau_i(\alpha),$$

$$(-1)^r\,c_r = \left(\prod_{i=1}^{m_0}\tau_i(\alpha)\right)^{[K(\alpha):K]_i}.$$

□

Bemerkungen:

(1) Norm und Spur sind Elemente des Grundkörpers K.
(2) Norm und Spur sind unabhängig von der Wahl von Γ.

Eigenschaften von Norm und Spur

HILFSSATZ 3.21: Es seien $M/L/K$ endlich, $a \in K$, $\alpha, \beta \in L$, $x \in M$.
Dann gilt:
(1) $\mathrm{N}_{L/K}(\alpha\,\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$, $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$;
(2) $\mathrm{N}_{L/K}(a) = a^{[L:K]}$, $\mathrm{Tr}_{L/K}(a) = [L:K]a$;
(3) $\mathrm{N}_{M/K}(x) = \mathrm{N}_{L/K}\left(\mathrm{N}_{M/L}(x)\right)$, $\mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(x)\right)$.

Beweis: Übungen.

DEFINITION 3.22: Sind L/K endlich vom Grad n und $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L, so heißt $d(\alpha_1, \ldots, \alpha_n) := \det\left(\mathrm{Tr}_{L/K}(\alpha_i\,\alpha_j)\right)$ *Diskriminante* der Basis.

Sind $\alpha_1, \ldots, \alpha_n$ sowie $\beta_1, \ldots, \beta_n$ zwei Basen von L/K, so ist $d(\alpha_1, \ldots, \alpha_n) = d(\beta_1, \ldots, \beta_n)a^2$ mit $a \in K$, $a \neq 0$. Man kann also als Diskriminante $d(L/K)$ von L/K die Quadratklasse $d(\alpha_1, \ldots, \alpha_n)\,(K^\times)^2$ erklären.

SATZ 3.23: $d(L/K) = 0 \Leftrightarrow \mathrm{Tr}_{L/K}(\alpha) = 0\ \forall\ \alpha \in L$.

Beweis: „⇐“ trivial. „⇒“ Die Spalten der Matrix $(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))$ sind linear abhängig.

Also existieren $b_1, \ldots, b_n \in K$, nicht alle gleich 0, mit

$$\sum_{j=1}^{n} b_j \operatorname{Tr}_{L/K}(\alpha_i \alpha_j) = 0 \qquad (1 \le i \le n).$$

Folglich ist $\beta := \sum_{j=1}^{n} b_j \alpha_j \neq 0$. Für $\alpha \in L$ existiert demnach $\gamma = \sum_{j=1}^{n} c_i \alpha_i \in L$ mit $\alpha = \beta \gamma$.

Es folgt:

$$\operatorname{Tr}_{L/K}(\alpha) = \operatorname{Tr}_{L/K}\left(\sum_{i=1}^{n} c_i \alpha_i \sum_{j=1}^{n} b_j \alpha_j\right) = \sum_{i=1}^{n} c_i \operatorname{Tr}_{L/K}\left(\sum_{j=1}^{n} b_j \alpha_i \alpha_j\right) = 0.$$

□

Satz 3.24: $d(L/K) \neq 0 \Leftrightarrow L/K$ ist separabel.

Beweis:

(1) L/K inseparabel $\Rightarrow \operatorname{Tr}_{L/K}(\alpha) = 0 \ \forall\ \alpha \in L \ \Rightarrow_{(3.51)} d(L/K) = 0$

(2) L/K separabel $\overset{Algebra1,3.32}{\Rightarrow}$ $L = K(\alpha)$, $m_{\alpha/K}(t)$ hat keine mehrfachen Wurzeln. Es ist $1, \alpha, \ldots, \alpha^{n-1}$ $(n = \deg(m_{\alpha/K}))$ eine Basis von L/K. Hierfür ist

$$d(1, \alpha, \ldots, \alpha^{n-1})$$

Quadrat einer Vandermonde Determinante, also von 0 verschieden. □

Beispiel:

$K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{m}),\ [L : K] = 2,\ L/K$ separabel.

Eine Basis ist $1,\ \sqrt{m}$.

Für $\alpha = a + b\sqrt{m}$ ist

$$\begin{array}{rcl} \operatorname{Tr}(\alpha) & = & 2a,\ \mathrm{N}(\alpha) \qquad = \quad a^2 - mb^2 \\ d(1,\alpha) & = & \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\alpha) \\ \operatorname{Tr}(\alpha) & \operatorname{Tr}(\alpha^2) \end{pmatrix} \quad = \quad \begin{pmatrix} 2 & 2a \\ 2a & 2(a^2 + mb^2) \end{pmatrix} \\ & = & 4mb^2. \end{array}$$

Es ist $m_{\alpha/\mathbb{Q}}(t) = \begin{cases} t - a & \text{für } b = 0 \\ t^2 - \operatorname{Tr}(\alpha) t + \mathrm{N}(\alpha) & \text{sonst.} \end{cases}$

Definition 3.25: Ein Körper K heißt *algebraisch abgeschlossen*, falls für jede algebraische Erweiterung L/K bereits $L = K$ gilt. $\bar{K}$ heißt *algebraischer Abschluß* des Körpers K, falls $\bar{K}/K$ algebraisch und $\bar{K}$ algebraisch abgeschlossen ist.

Satz 3.26: Ein Körper K besitzt einen algebraischen Abschluß $\bar{K}$, und je zwei algebraische Abschlüsse von K sind K-isomorph.

Beweis:

(1) Existenz
Betrachte die Menge M aller geordneten Paare $(f(t),\, n) \in K[t] \times \mathbb{N}$.
Identifiziere K mit den Paaren $(t-a,\, 1)$ für $a \in K$. Definiere $K_+ := \{(x,y,z) \in M^3 \mid x+y=z\}$ und $K_\cdot := \{(x,y,z) \in M^3 \mid xy = z\}$.
Folglich existiert eine nicht leere Famile $\mathfrak{F}$ von Tripeln $(A, A_+, A_*) \in 2^M \times (2^M)^3 \times (2^M)^3$ mit den Eigenschaften
  (a) A ist mit den Operationen $+ : A \times A \to A : (x,y) \mapsto z$ mit $(x,y,z) \in A_+$ und $* : A \times A \to A : (x,y) \mapsto z$ mit $(x,y,z) \in A_*$ ein Körper,
  (b) $x = (f,n) \in A$ hat das Minimalpolynom f.

Für Elemente A, B von $\mathfrak{F}$ schreiben wir $(A, A_+, A_*) \leq (B, B_+, B_*)$, falls B Oberkörper von A ist, d.h. $A \subseteq B$, $A_+ \subseteq B_+$ und $A_* \subseteq B_*$.
Damit wird $\mathfrak{F}$ partiell geordnet, und jede Kette in $\mathfrak{F}$ besitzt darin eine obere Schranke (Vereinigungsmenge!). Folglich enthält $\mathfrak{F}$ ein bzgl. $\leq$ maximales Element $(\Gamma, \Gamma_+, \Gamma_*)$. Gemäß (b) ist Γ/K algebraisch.
Annahme, Γ ist nicht algebraisch abgeschlossen. Dann existiert eine echte algebraische Erweiterung Δ von Γ. Jedes $\alpha \in \Delta$ ist hierbei über K algebraisch.
Es sei $f(t) = m_{\alpha/K}(t)$. $f(t)$ habe in Γ Wurzeln $\alpha_1, \ldots, \alpha_r$ sowie in $\Delta \setminus \Gamma$ die Wurzeln $\alpha_{r+1}, \ldots, \alpha_m$.
Die Elemente $\alpha_1, \ldots, \alpha_r$ entsprechen dabei Elementen $(f(t),\, n_i) \quad (1 \leq i \leq r)$ aus $K[t] \times \mathbb{N}$.
Wir bilden folglich $\alpha_{r+1}, \ldots, \alpha_m$ auf $(f(t),\, n_j)$ mit $\mathbb{N} \ni n_j \notin \{n_i, \ldots, n_{j-1}\}$ ab.
Damit entspricht Δ einer echten Obermenge in $\mathfrak{F}$, Widerspruch!

(2) Eindeutigkeit bis auf Isomorphie.
Wir nehmen an, daß $\bar{K}$ und $\hat{K}$ beides algebraische Abschlüsse von K sind.
Es bezeichne $\mathfrak{M}$ die Menge aller geordneten Tripel $(L,\, \tilde{L},\, \psi)$ mit $K \subseteq L \subseteq \bar{K}$, $K \subseteq \tilde{L} \subseteq \hat{K}$, $\psi : L \to \tilde{L}$ Isomorphismus.
Es ist $\emptyset \neq \mathfrak{M}$ wegen $(K,\, K_1\, id) \in \mathfrak{M}$.
Wir ordnen $\mathfrak{M}$ partiell gemäß $(L,\, \tilde{L},\, \psi) \leq (L_1,\, \tilde{L_1},\, \psi_1)$ für $L \subseteq L_1$, $\tilde{L} \subseteq \tilde{L_1}$, $\psi_1 \,|\, \tilde{L} = \psi$.
Es sei $(F,\, \tilde{F},\, \Phi)$ maximales Element in $\mathfrak{M}$ gemäß Zorn's Lemma.
Ist $F = \bar{K}$, so ist notwendig $\tilde{F} = \Phi(F)$ algebraisch abgeschlossen, also $\tilde{F} = \hat{K}$.
Existiert jedoch $x \in \bar{K} \setminus F$, so besitzt x ein Minimalpolynom $m_{x/F}(t)$.
Hierfür ist $\Phi(m_{x/F}(t)) \in \tilde{F}[t]$ irreduzibel, und Φ läßt sich fortsetzen zu einem Isomorphismus $\tilde{\Phi} : F(x) \to \tilde{F}(\tilde{x})$ im Widerspruch zur Maximalität von $(F,\, \tilde{F},\, \Phi)$.
Also muß $F = \bar{K},\ \tilde{F} = \hat{K}$ gelten.

□

KAPITEL 4

Galoistheorie

Satz 4.1: Es seien K, L zwei Körper und $\sigma_i : K \to L \quad (1 \leq i \leq n)$ verschiedene Isomorphismen.
Dann sind $\sigma_1, \ldots, \sigma_n$ im folgenden Sinn linear unabhängig: $\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0$ für feste $\alpha_1, \ldots, \alpha_n \in L$ und alle $\beta \in K$ impliziert $\alpha_i = 0 \qquad (1 \leq i \leq n)$.

Beweis: Mittels Induktion über n!

$n = 1$: trivial (speziell ist $\sigma_1(1) = 1$!).

$n-1 \Rightarrow n$: Es sei $\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0 \ \ \forall \beta \in K$ vorgegeben. Es sind σ_1 und σ_n verschieden, also existiert $\gamma \in K \backslash \{0, 1\}$ mit $\sigma_1(\gamma) \neq \sigma_n(\gamma)$. Hierfür gilt: $\sigma_n(\gamma^{-1}) \ \sum_{i=1}^{n} \alpha_i \sigma_i(\gamma\beta) = 0 \ \ \forall \beta \in K$, und wir subtrahieren hiervon $\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0 \ \ \forall \beta \in K$. Dies liefert $\sum_{i=1}^{n-1} \ \alpha_i \left(\sigma_n(\gamma^{-1})\, \sigma_i(\gamma) \ - 1\right) \sigma_i(\beta) \ = 0 \ \ \forall \beta \in K$. Nach Induktionsannahme gilt dann $\alpha_i \left(\sigma_n(\gamma^{-1})\, \sigma_i(\gamma) \ - 1\right) = 0 \qquad (1 \leq i \leq n-1)$, also $\alpha_1 = 0$. Wiederum nach Induktionsannahme folgt dann auch $\alpha_2 = \ldots = \alpha_n = 0$. □

Hilfssatz 4.2: Es seien K, L zwei Körper und $\sigma_i : \ K \to L \qquad (1 \leq i \leq n)$ verschiedene Isomorphismen.
Dann ist $F := \{\alpha \in K \mid \sigma_1(\alpha) = \ldots = \sigma_n(\alpha)\}$ ein Unterkörper von K mit $[K : F] \geq n$.

Beweis: F Teilkörper ist klar, es bleibt die Gradaussage zu zeigen. Indirekt! Wir nehmen $[K : F] = r < n$ an. Dann existiert eine F-Basis $\omega_1, \ldots, \omega_r$ von K/F. Danach hat das lineare Gleichungssystem $\sum\limits_{j=1}^{n} \sigma_j(\omega_i) X_j = 0 \ (1 \leq i \leq r)$ eine nicht triviale Lösung $X_1, \ldots, X_n$ in L.

Für beliebiges $\alpha \in K$, $\alpha = \sum_{i=1}^{r} \alpha_i \omega_i \ (\alpha_i \in F, \quad 1 \leq i \leq r)$, liefert dies

$$\sum_{j=1}^{n} \sigma_j(\alpha_i \omega_i) X_j = 0$$

$(1 \leq i \leq r)$ (mittels Multiplikation der i-ten Gleichung mit $\sigma_1(\alpha_i) = \sigma_2(\alpha_i) = \ldots = \sigma_n(\alpha_i)$). Addition aller Gleichungen ergibt $\sum_{j=1}^{n} \sigma_j(\alpha) X_j = 0 \ \ \forall \alpha \in K$, Widerspruch! □

Anwendung:

Es sei L eine endliche K-Erweiterung, $G(L/K)$ bezeichne die Gruppe aller K-Automorphismen von L. Ferner sei H eine Untergruppe von $G(L/K)$ und $\mathrm{Fix}(H) := \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \ \forall \sigma \in H\}$. Dann ist $\mathrm{Fix}(H)$ ein Teilkörper von L, der K enthält, und es gilt $[L : \mathrm{Fix}(H)] \geq (H : 1)$. $\mathrm{Fix}(H)$ heißt *Fixkörper* bzgl. H (Bezeichnung: $\mathrm{Fix}(H)$).

Beispiel: Es sei $L = K(t)$. L besitzt u.a. folgende 6 Automorphismen σ_i,

welche durch $\sigma_1(t) = t$, $\sigma_2(t) = 1-t$, $\sigma_3(t) = \frac{1}{t}$, $\sigma_4(t) = 1-\frac{1}{t}$, $\sigma_5(t) = \frac{1}{1-t}$, $\sigma_6(t) = \frac{t}{1-t}$ festgelegt sind.

Es sei F derjenige Teilkörper von L, der von allen 6 Automorphismen elementweise invariant gelassen wird. Hierfür gilt $[L : F] \geq 6$. Es steht sogar das Gleichheitszeichen: Denn $g(t) := \dfrac{(t^2-t+1)^3}{t^2(t-1)^2}$ liegt in F.

Also ist $F_1 := K(g(t))$ ein Teilkörper von F, d.h. $[L : F_1] \geq 6$. Wegen $(t^2-t+1)^3 - g(t)t^2(t-1)^2 = 0$ in $F_1[t]$ ist t Wurzel eines Polynoms vom Grad 6 aus $F_1[t]$, also $[F_1[t] : F_1] \leq 6$ und damit $F = K(g(t))$.

SATZ 4.3: Es sei G eine endliche Gruppe von Automorphismen eines Körpers L und $F = \mathrm{Fix}(G)$ der zugehörige Fixkörper. Dann gilt $[L : F] = (G : 1)$.

Beweis:

Gemäß 4.2 ist F Teilkörper von L mit $[L : F] \geq (G : 1) =: n$. Wir nehmen an, daß L über F $n+1$ linear unabhängige Elemente $\omega_1, \ldots, \omega_{n+1}$ enthält. Für $G = \{\sigma_1, \ldots, \sigma_n\}$ betrachten wir das homogene lineare Gleichungssystem

$$\sum_{j=1}^{n+1} \sigma_i(\omega_j) X_j = 0 \qquad (1 \leq i \leq n).$$

Hierfür sei $X_1, \ldots, X_{n+1}$ eine nicht triviale Lösung in L. Unter allen Lösungen des Gleichungssystems wählen wir nun eine aus, bei der minimal viele X_i von Null verschieden sind. Durch Umordnung der Basis erreichen wir also etwa

$$\sum_{j=1}^{r} \sigma_i(\omega_j) X_j = 0 \qquad (1 \leq i \leq n,\ r \leq n+1,\ X_1 \cdot \ldots \cdot X_r \neq 0).$$

Offenbar muß $r \geq 2$ sein. Außerdem normieren wir X_r zu 1 und nehmen noch $X_1 \notin F$ an (alle $X_i \in F \Rightarrow \omega_1, \ldots, \omega_r$ linear abhängig), d.h. es existiert $h \in \{1, \ldots, n\}$ mit $\sigma_h(X_1) \neq X_1$. Anwendung von σ_h auf alle n Gleichungen ergibt

$$\begin{aligned} \sum_{j=1}^{r} \sigma_h(X_j)\sigma_h\sigma_i(\omega_j) &= 0 \quad (1 \leq i \leq n), \text{ also} \\ \sum_{j=1}^{r} \sigma_h(X_j)\sigma_k(\omega_j) &= 0 \quad (1 \leq k \leq n). \end{aligned}$$

Subtraktion vom Ausgangssystem liefert:

$$\sum_{j=1}^{r-1} \sigma_k(\omega_j)(X_j - \sigma_h(X_j)) = 0 \quad (1 \leq k \leq n).$$

Wegen $X_1 \neq \sigma_h(X_1)$ steht dies jedoch im Widerspruch zur Minimalität von r. □

Es sei Γ/K normal, endlich, und F sei der Fixkörper von $G(\Gamma/K)$. Wir haben gesehen, daß F/K rein inseparabel ist 3.18.

Offenbar ist $G(\Gamma/F) = G(\Gamma/K)$, also nach 4.3:

$$[\Gamma : F] = \sharp G(\Gamma/F) \overset{3.17}{=} [\Gamma : F]_{sep}.$$

Folglich ist Γ/F separabel. Wir merken noch $[\Gamma : F] = \sharp G(\Gamma/K) = [\Gamma : K]_s$ an, so daß $[F : K] = [\Gamma : K]_i$ folgt.

DEFINITION 4.4: Eine algebraische Erweiterung L/K heißt *Galoiserweiterung*, falls K der Fixkörper von $G(L/K)$ ist. In diesem Fall heißt $G = G(L/K)$ *Galoisgruppe* von L/K.

SATZ 4.5: L/K endlich: L/K galoissch $\iff$ L/K normal und separabel.

Beweis: „$\Leftarrow$“ Es sei $F := \mathrm{Fix}(G(L/K))$ der Fixkörper zu $G(L/K)$. Hierfür ist $[F : K] = [L : K]_i = 1$, also $F = K$.

„$\Rightarrow$“ Es sei $\alpha \in L$. Betrachte $\alpha_j := \sigma_j(\alpha)$ für $G(L/K) = \{\sigma_1, \dots, \sigma_n\}$, hierunter seien - evtl. Umnummerieren - $\alpha_1, \dots, \alpha_r$ paarweise verschieden. G permutiert $\{\alpha_1, \dots, \alpha_r\}$. Alle symmetrischen Funktionen in $\alpha_1, \dots, \alpha_r$ bleiben demnach G-invariant, speziell ist $g_\alpha(t) := \prod_{i=1}^{r}(t - \alpha_i)$ demnach aus $K = \mathrm{Fix}(G)$.

Ein irreduzibler Teiler $\tilde{g}(t)$ von $g(t)$ in $K[t]$ hat dann mit einer Nullstelle α_j alle α_i als Nullstellen, also ist $g_\alpha(t) = m_\alpha(t)$. □

Bemerkung: L/K galoissch und $K \subset E \subset L \Rightarrow L/E$ galoissch.

SATZ 4.6 (Hauptsatz der Galoistheorie): Es sei L/K eine endliche Galoiserweiterung. Dann gibt es eine Bijektion zwischen den Zwischenkörpern $K \subset F \subset L$ und den Untergruppen von $G(L/K)$ mittels

$$F \leftrightarrow G(L/F).$$

Dabei ist F/K genau dann galoissch, wenn $G(L/F)$ Normalteiler in $G(L/K)$ ist. In diesem Fall gilt:

$$G(F/K) \cong G(L/K)/G(L/F).$$

Beweis:

(1) Zunächst ist $F \to G(L/F)$ eine injektive Abbildung: denn für Zwischenkörper $E \neq F$ sei $x \in E \setminus F$ beliebig. Da L/F separabel ist, existiert nach 3.18 ein $\sigma \in G(L/F)$ mit $\sigma(x) \neq x$, also $\sigma \notin G(L/E)$.
Es bleibt die Surjektivität zu zeigen. Dazu sei H eine Untergruppe von $G(L/K)$ und $\mathrm{Fix}(H)$ der zugehörige Fixkörper. Dann ist $L/\mathrm{Fix}(H)$ normal und separabel, also galoissch mit Galoisgruppe $G(L/\mathrm{Fix}(H))$. Also gilt $H < G(L/\mathrm{Fix}(H))$. Gemäß 4.3 ist $[L : \mathrm{Fix}(H)] = (H : 1)$ und nach 3.17:

$$[L : \mathrm{Fix}(H)] = (G(L/\mathrm{Fix}(H)) : 1),$$

also $H = G(L/\mathrm{Fix}(H))$.

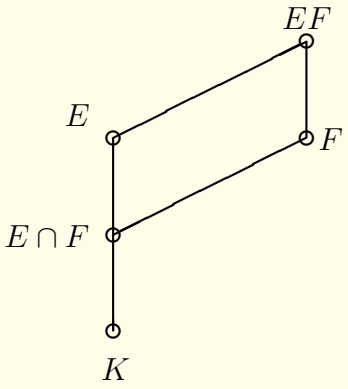
(2) Sei nun $K \subset E \subset L$.
Wir nehmen zunächst E/K als galoissch, d.h. normal und separabel, an. Ferner seien $\sigma \in G(L/K)$ und $\tau \in G(L/E)$. Für $\alpha \in E$ ist $\sigma(\alpha) \in E$, also $\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}\sigma(\alpha) = \alpha$, und damit $\sigma^{-1}\tau\sigma \in G(L/E)$. Damit ist $G(L/E)$ Normalteiler.
Umgekehrt sei $G(L/E) \triangleleft G(L/K)$. Trivialerweise ist E/K separabel, es bleibt E/K normal zu zeigen. Dazu sei $f \in K[t]$ irreduzibel mit Nullstelle $\alpha \in E$. In $L[t]$ zerfällt f in Linearfaktoren, alle Nullstellen sind dabei von der Form $\sigma(\alpha)$ ($\sigma \in G(L/K)$). Für alle $\tau \in G(L/E)$ existiert nun $\rho \in G(L/E)$ mit $\tau = \sigma\rho\sigma^{-1}$, d.h. $\tau(\sigma(\alpha)) = \sigma\rho\sigma^{-1}(\sigma(\alpha)) = \sigma\rho(\alpha) = \sigma(\alpha)$. Damit folgt $\sigma(\alpha) \in \mathrm{Fix}(G(L/E)) = E$. Also zerfällt f bereits in $E[t]$ in Linearfaktoren, und E/K ist normal.

(3) Definiere $\phi : G(L/K) \to G(E/K) : \sigma \mapsto \sigma\mid_E$. ϕ ist Homomorphismus wegen $\sigma\mid_E$ Automorphismus und gemäß Algebra 1, 3.29 surjektiv. $\ker\phi = \{\sigma \in G(L/K) \mid \sigma\mid_E = \mathrm{id}_E\} = G(L/E)$. Damit folgt die behauptete Isomorphie aus dem Homomorphiesatz für Gruppen.

□

Korollar 4.7: Es sei L/K galoissch, E, F seien Zwischenkörper. Dann gilt: $E \subseteq F \Leftrightarrow G(L/E) \supseteq G(L/F)$.

Satz 4.8: Es sei L/K eine Körpererweiterung mit Zwischenkörpern E, F. Ist dann E/K eine endliche Galoiserweiterung, so ist EF eine Galoiserweiterung von F mit $G(EF/F) \cong G(E/E \cap F)$ speziell gilt daher $G(EF/F) \cong U \leq G(E/K)$.



Beweis: E/K ist Zerfällungskörper eines Polynoms $f \in K[t]$, dessen Faktoren lauter einfache Nullstellen besitzen. Dann ist auch EF Zerfällungskörper von $f \in F[t]$, d.h. EF/F ist normal und separabel, also galoissch. Es seien nun $\sigma \in G(EF/F)$ und $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f. Dann induziert σ eine Permutation dieser Nullstellen, die einem Element $\tilde{\sigma} \in G(E/K)$ entspricht. Verschiedene σ induzieren so verschiedene $\tilde{\sigma}$, die Zuordnung $\sigma \mapsto \tilde{\sigma}$ liefert einen Isomorphismus von $G(EF/F)$ auf eine Untergruppe von $G(E/K)$. σ (und damit $\tilde{\sigma}$) läßt jedes Element von $F \cap E$ invariant, d. h. $\tilde{\sigma} \in G(E/E \cap F)$.

Jedes Element $\tilde{\sigma} \in G(E/E \cap F)$ permutiert $\alpha_1, \ldots, \alpha_n$ und ist daher als Bild eines $\sigma \in G(EF/F)$ erhältlich. Also folgt die behauptete Isomorphie. □

Definition 4.9: Es sei L/K galoissch.
Ist dann $G(L/K)$ abelsch, zyklisch etc., so heißt auch die Erweiterung L/K *abelsch*, *zyklisch* etc..

Beispiel:

Für $f(t) = t^3 - 2 \in \mathbb{Q}[t]$ ist der Zerfällungskörper $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

Demnach ist $[K : \mathbb{Q}] = 6$ und $K/\mathbb{Q}$ normal und separabel, also galoissch.

Alle 6 $\mathbb{Q}$-Automorphismen von K sind durch ihre Wirkung auf $\sqrt[3]{2}$ und $\sqrt{-3}$ eindeutig bestimmt.

Wir setzen $\xi := \dfrac{-1+\sqrt{-3}}{2}$ $(\Rightarrow \xi^3 = 1!)$ und

$$\begin{aligned} \sigma &: K \to K \text{ mittels } \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \sqrt{-3} \mapsto -\sqrt{-3} \qquad (\xi \mapsto \xi^2), \\ \tau &: K \to K \text{ mittels } \sqrt[3]{2} \mapsto \xi\sqrt[3]{2},\ \sqrt{-3} \mapsto +\sqrt{-3} \qquad (\xi \mapsto \xi) \end{aligned}$$

und erhalten folgende Tabelle:

	id	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\xi\sqrt[3]{2}$	$\xi^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\xi^2\sqrt[3]{2}$	$\xi\sqrt[3]{2}$
$\sqrt{-3}$	$\sqrt{-3}$	$\sqrt{-3}$	$\sqrt{-3}$	$-\sqrt{-3}$	$-\sqrt{-3}$	$-\sqrt{-3}$

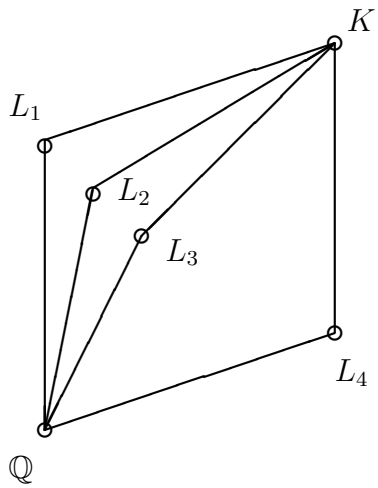
Die Untergruppen von $G(K/\mathbb{Q}) \cong S_3$ sind:

$$H_1 = \{\mathrm{id},\ \sigma\},\ H_2 = \{\mathrm{id},\ \sigma\tau\},\ H_3 = \{\mathrm{id},\ \sigma\tau^2\},\ H_4 = \{\mathrm{id},\ \tau,\ \tau^2\}.$$

Diesen entsprechen die Fixkörper

$$L_1 = \mathbb{Q}(\sqrt[3]{2}),\ L_2 = \mathbb{Q}(\xi\sqrt[3]{2}),\ L_3 = \mathbb{Q}(\xi^2\sqrt[3]{2}), L_4 = \mathbb{Q}(\sqrt{-3}).$$

Also ist $L_4/\mathbb{Q}$ galoissch, jedoch $L_i/\mathbb{Q}$ nicht normal $(1 \le i \le 3)$.



Endliche Körper

Satz 4.10: Es sei K eine endliche Erweiterung von $\mathbb{F}_p$ vom Grad n. Dann ist $K/\mathbb{F}_p$ galoissch mit $G(K/\mathbb{F}_p) = \langle\sigma\rangle$, wobei σ der Frobenius-Automorphismus von K ist, $\sharp\langle\sigma\rangle = n$.
Ist L eine Erweiterung von K vom Grad m, so ist auch L/K galoissch mit Galoisgruppe $G(L/K) = \langle\psi\rangle$, wobei ψ durch $x \mapsto x^{p^n}$ gegeben ist, $\sharp\langle\psi\rangle = m$.

Beweis:

(1) Die Erweiterung $K/\mathbb{F}_p$ ist normal als Zerfällungskörper von $t^{p^n} - t$; sie ist separabel, weil $\mathbb{F}_p$ vollkommen ist. Die Abbildung $\sigma : K \to K : x \mapsto x^p$ ist - wie früher gezeigt - ein Monomorphismus, der wegen $\sharp K < \infty$ surjektiv ist. Da für $x \in \mathbb{F}_p$ zudem $x^p = x$ gilt, ist $\sigma \in G(K/\mathbb{F}_p)$. Wir betrachten die zyklische Untergruppe $\langle\sigma\rangle =: U$ von $G = G(K/\mathbb{F}_p)$. Es gilt: $\sigma^v : K \to K : x \mapsto x^{p^v}$, d.h. $\sigma^v = \mathrm{id}_k$ erstmalig für $v = n$. Also ist $\sharp U = n = \sharp G$ und damit $U = G$.
(2) L/K ist galoissch (vgl. (1)). Wegen 4.3 gilt: $\sharp G(L/K) = [L : K] = m$.
Als Untergruppe von $G(L/\mathbb{F}_p)$ ist $G(L/K)$ zyklisch. Die Gruppe wird erzeugt durch $\psi : L \to L : x \mapsto x^{p^n}$.

□

Kreisteilung

Definition 4.11: Es sei K ein Primkörper. Jede Wurzel des Polynoms $t^n - 1 \in K[t]$ heißt *n-te Einheitswurzel* über K. Der Zerfällungskörper K_n von $t^n - 1$ heißt *n-ter Kreisteilungskörper* (Kreiskörper, engl. Cyclotomic Field) über K.

Im folgenden seien stets die Voraussetzungen von 4.11 gegeben.

In K_n zerfällt $t^n - 1$ in Linearfaktoren. Für die Nullstellenmenge E_n von $t^n - 1$ in K_n gilt dabei:

Satz 4.12: Es sei $t^n - 1 \in K[t]$, K Primkörper. Im Zerfällungskörper K_n von $t^n - 1$ bezeichne E_n die Nullstellenmenge von $t^n - 1$ ($\sharp E_n \leq n$). Dann gilt:
(1) E_n ist zyklische Untergruppe von $K_n^\times$.
(2) Für $\chi(K) = p$ mit $p|n$ gilt $E_n = E_{n/p}$.
(3) Für $\chi(K) \nmid n$ gilt $\sharp E_n = n$.
(4) $\forall m \in \mathbb{N}$ gilt $E_n \subseteq E_{mn}$, also $K_n \subseteq K_{mn}$.

Beweis:

(1) Gemäß 2.10, denn mit $x, y \in K_n$ und $x^n = y^n = 1$ folgt $(xy)^n = (xy^{-1})^n = 1$, also $E_n < K^\times$.
(2) Es sei $n = pm$; es folgt $t^n - 1 = (t^m)^p - 1 = (t^m - 1)^p$.
(3) $t^n - 1$ besitzt n Nullstellen in K_n, die wegen $\mathrm{ggT}(t^n - 1, (t^n - 1)') = \mathrm{ggT}(t^n - 1, nt^{n-1}) = 1$ alle verschieden sind. (Beachte: $n \neq 0$ in K_n).
(4) $x^n = 1 \Rightarrow x^{nm} = 1 \forall m \in \mathbb{N}$.

□

Wegen 4.12.(2) können wir im weiteren stets $\chi(K) \nmid n$ annehmen! Dann gilt $E_n = \langle \xi \rangle$, $\sharp E_n = n$, also $E_n = \{1, \xi, \ldots, \xi^{n-1}\}$.

Jedes erzeugende Element der zyklischen Gruppe E_n heißt dann *primitive n-te Einheitswurzel*.

Ist $E_n = \langle \xi \rangle$, so gilt $K_n = K[\xi]$. Wegen $\mathrm{ord}(\xi^m) = \frac{n}{\mathrm{ggT}(m,n)}$ gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln. Hierbei mißt die Eulersche Funktion φ die Anzahl der zu n teilerfremden Zahlen in $\{1, 2, \ldots, n\}$. Es bezeichne F_n die Menge der primitiven n-ten Einheitswurzeln, dann gilt $F_n \subseteq E_n$, $\sharp F_n = \varphi(n)$.

Hilfssatz 4.13: (1) Für $m \neq n, m, n \in \mathbb{N}$ ist $F_m \cap F_n = \emptyset$.
(2) $E_n = \dot{\bigcup}_{d|n} F_d$.
(3) $n = \sum_{d|n} \varphi(d)$.

Beweis:

(1) Trivial.
(2) Klar ist zunächst $E_n \supseteq \bigcup_{d|n} F_d$. Die Vereinigung ist wegen (1) zudem disjunkt. Ist andererseits $\xi \in E_n$, so existiert ein minimaler Exponent $m \in N$ mit $\xi^m = 1$ und $m|n$. Hierfür ist ξ eine primitive m-te Einheitswurzel.
(3) Folgt sofort aus (2).

□

Definition 4.14: $\Phi_n(t) := \prod_{\xi \in F_n}(t-\xi) \in K_n[t]$ heißt *n-tes Kreisteilungspolynom* über K.

Bemerkungen:

Offensichtlich ist $\deg(\Phi_n) = \varphi(n)$.

Ist ξ irgendeine primitive n-te Einheitswurzel, so gilt $\Phi_n(t) = \prod\limits_{\substack{i=1 \\ \mathrm{ggT}(i,n)=1}}^{n} (t-\xi^i)$. Damit folgt aus 4.13.(2) unmittelbar $t^n - 1 = \prod_{d|n} \Phi_d(t)$ in $K_n[t]$.

Satz 4.15: Es ist $\Phi_n(t) \in K[t]$; speziell für $K = \mathbb{Q}$ gilt sogar $\Phi_n(t) \in \mathbb{Z}[t]$.

Beweis: Mittels Induktion nach n!

$n = 1 : \Phi_1(t) = t - 1$

$1, \ldots, n-1 \to n$: Wegen

$$t^n - 1 = \prod_{d|n} \Phi_d(t) \text{ ist } \Phi_n(t) = (t^n - 1)/ \underbrace{\Big(\prod_{\substack{d|n \\ d<n}} (\Phi_d(t))\Big)}_{=:g_n(t) \in K[t] \text{ bzw. } \mathbb{Z}[t]} \quad \text{in } K_n(t)$$

nach Induktionsannahme.

Also existieren Polynome $h_n(t), r_n(t)$ aus $K[t]$ bzw. $\mathbb{Z}[t]$ mit $t^n - 1 = h_n(t)g_n(t) + r_n(t)$ und $\deg(r_n) < n - \varphi(n)$. Da diese Zerlegung auch in $K_n(t)$ Gültigkeit besitzt, folgt $r_n(t) = 0$ und $h_n(t) = \Phi_n(t)$. □

Satz 4.16: Es gilt $[K_n : K] = \varphi(n)$ für $K = \mathbb{Q}$; speziell ist $\Phi_n(t)$ in $\mathbb{Z}[t]$ irreduzibel, $K_n/\mathbb{Q}$ galoissch.

Beweis: Offenbar ist $[K_n : K] \leq \varphi(n)$, da $\Phi_n(t)$ in K_n in Linearfaktoren zerfällt und $K_n = K(\xi)$ mit ξ Nullstelle von Φ_n ist. Wir zeigen also noch $[K_n : K] \geq \varphi(n)$. Dazu sei ξ eine Nullstelle von $\Phi_n(t)$ mit Minimalpolynom $m_\xi(t) \in K[t]$. Hierfür gilt $m_\xi(t) | \Phi_n(t)$, d.h. es existiert $h(t) \in K[t]$ (nominiert!) mit $\Phi_n = m_\xi h$.

Wir zeigen: Ist nun x Nullstelle von m_ξ, so auch x^p für alle Primzahlen p, die n nicht teilen. Daraus folgt dann sofort, daß jede primitive n-te Einheitswurzel Nullstelle von m_ξ ist, also $m_\xi(t) = \Phi_n(t)$ gilt.

Annahme: x^p ist keine Nullstelle von m_ξ. Dies bedeutet wegen $\Phi_n(x^p) = 0$ jedoch $h(x^p) = 0$, d.h. x Nullstelle von $h(t^p)$ bzw. $m_\xi(t) | h(t^p)$ oder $h(t^p) = m_\xi(t)g(t)$ in $\mathbb{Z}[t]$. Also folgt wegen $h(t^p) \equiv h(t)^p \ mod\, p\mathbb{Z}[t]$ auch $h(t)^p \equiv m_\xi(t)g(t) \ mod\ p\mathbb{Z}[t]$, d.h. in $\mathbb{F}_p[t]$ gilt: $\mathrm{ggT}(\bar{h}, \bar{m}_\xi) \neq 1$, was dann bedingt, daß $t^n - 1$ mehrfache Nullstellen in $\mathbb{F}_p[t]$ besitzt. Dies ist jedoch ein Widerspruch zu $p \nmid n$. □

Beispiel:

Über $\mathbb{F}_5$ gilt:

$\Phi_{12}(t) = t^4 - t^2 + 1 = (t^2 - 2t - 1)(t^2 + 2t - 1) = (t - \xi)(t - \xi^5) \cdot (t - \xi^7)(t - \xi^{11})$
4.16 wird falsch!

Bemerkung:

Über $\mathbb{F}_p$ mit $p \nmid n$ ist $[K_n : K] = \min\{m \in \mathbb{N} | p^m - 1 \equiv 0 \bmod n\}$.

Satz 4.17: Für $n \in \mathbb{N}$ ist $G(K_n/\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z})$.

Beweis: Es seien ξ eine (feste) primitive n-te Einheitswurzel, $K_n = \mathbb{Q}(\xi)$, und $h \in \mathbb{N}$ mit $1 \leq h \leq n$, $\mathrm{ggT}(h, n) = 1$. Dann sind ξ und ξ^h beide Nullstellen des irreduziblen Polynoms $\Phi_n(t) \in \mathbb{Z}[t]$, welches in $K_n[t]$ in Linearfaktoren zerfällt, und es gilt $K_n(\xi) = K_n(\xi^h)$.

Wir definieren $\varphi : U(\mathbb{Z}/n\mathbb{Z}) \to G(K_n/\mathbb{Q}) : h + n\,\mathbb{Z} \mapsto \sigma_h$, wobei $\sigma_h : K_n \to K_n$ mittels $\xi \mapsto \xi^h$ gegeben ist. Offensichtlich ist σ_h ein Element aus $G(K_n/\mathbb{Q})$, φ ist wohldefiniert wegen $\xi^n = 1$, injektiv (und damit surjektiv).

Zur Homomorphie: $\varphi(hk + n\,\mathbb{Z}) = \sigma_{hk} = \sigma_h\sigma_k = \varphi(h + n\,\mathbb{Z})\varphi(k + n\,\mathbb{Z})$. □

Korollar 4.18: Der n-te Kreiskörper K_n ist abelsch über $\mathbb{Q}$. Alle Zwischenkörper F mit $\mathbb{Q} \subset F \subset K_n$ sind über $\mathbb{Q}$ abelsch.

Satz 4.19 (Kronecker-Weber): Jeder über $\mathbb{Q}$ abelsche Körper ist Teilkörper eines Kreisteilungskörpers.

Beweis. Wenn überhaupt, dann später. □

Zyklische Erweiterungen

Satz 4.20: Es sei K ein Körper, $n \in \mathbb{N}$ mit $\chi(K) \nmid n$, K enthalte eine primitive n-te Einheitswurzel ζ.

(1) Ist α Nullstelle von $t^n - a \in K[t]$, so ist $K(\alpha)$ zyklisch über K.
(2) Ist L/K zyklisch vom Grad n, so ist L Zerfällungskörper eines Polynoms $t^n - a \in K[t]$.

Beweis:

(1) Ist α Nullstelle von $t^n - a$ und ζ eine primitive n-te Einheitswurzel, so gilt $t^n - a = \prod^{n-1} i = 0(t - \alpha\zeta^i)$ in $K(\alpha)[t]$. $K(\alpha)$ ist also Zerfällungskörper eines separablen Polynoms über K also separabel nach . Also ist $K(\alpha)/K$ galoissch. Gemäß Algebra 1, 3.18 enthält $G(K(\alpha)/K)$ Automorphismen σ_i gegeben durch $\alpha \mapsto \alpha\zeta^i$ (für $\alpha\zeta^i$ Nullstelle von $m_\alpha(t)$).
Analog zum Beweis von 4.17 erhält man einen Gruppenepimorphismus

$$\psi : (\mathbb{Z}/n\mathbb{Z}, +) \to G(K(\alpha)/K) : k + n\mathbb{Z} \mapsto \sigma_k,$$

also ist $G(K(\alpha)/K)$ isomorph zu einer Faktorgruppe von $(\mathbb{Z}/n\mathbb{Z}, +)$, also zyklisch.
(2) Gemäß 4.1 sind die Automorphismen $\sigma_i := \sigma^i$ $(0 \leq i < n)$ für $G(L/K) = \langle\sigma\rangle$ linear unabhängig.
Mit $\zeta \in K$ bilden wir $\mu := \sigma_0 + \zeta\sigma_1 + \ldots + \zeta^{n-1}\sigma_{n-1}$. Hierzu exististiert dann $\gamma \in L$ mit $0 \neq \beta := \mu(\gamma) = \sum_{i=0}^{n-1} \zeta^i\sigma_i(\gamma)$. Also gilt auch $0 \neq \sigma(\beta) = \sum_{i=1}^{n} \zeta^{i-1}\sigma_i(\gamma) = \zeta^{-1}\mu(\gamma)$, sowie $\sigma(\beta^n) = \beta^n$, und damit $a := \beta^n \in K = \mathrm{Fix}(G(L/K)) = \mathrm{Fix}(<\sigma>)$. Folglich ist $\beta \in L$ Nullstelle von $t^n - a \in K[t]$. Mit β sind auch $\sigma^{-i}(\beta) = \beta\zeta^i$ $(0 \leq i < n)$ Nullstellen von $m_\beta(t) \in K[t]$, diese sind jedoch paarweise verschieden, also folgt $\deg(m_\beta) \geq n$. Wegen $m_\beta(t) | (t^n - a)$ folgt hier Gleichheit und wegen $G(L/K) = n = [L : K] = [K(\beta) : K]$ dann auch $L = K(\beta)$.

□

Auflösung algebraischer Gleichungen durch Radikale

Im folgenden sei K ein Körper der Charakteristik 0.

DEFINITION 4.21: Eine Körpererweiterung L/K heißt *Radikalerweiterung*, wenn es einen Körperturm

$$K = K_0 \subset K_1 \subset \ldots \subset K_m = L$$

gibt, bei dem K_i aus K_{i-1} durch Adjunktion einer Wurzel von $t^{n_i} - a_i \in K_{i-1}[t]$ entsteht.
Eine Gleichung $f(x) = 0$ mit $f(t) \in K[t]$ heißt *durch Radikale auflösbar*, falls es eine Radikalerweiterung L/K gibt, die einen Zerfällungskörper von f als Teilkörper enthält.

SATZ 4.22: Zu jeder Radikalerweiterung L/K existiert eine über K galoissche Radikalerweiterung $M/L/K$.

Beweis: Mittels Induktion nach $r = [L : K]$.

$r = 1$. Es ist $L = K$, also nichts zu zeigen.

Sei also $r > 1$ und L/K Radikalerweiterung mit Körperturm $K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m = L$.

1. Fall: $m = 1$. Dann ist $L = K(\alpha)$ mit $\alpha^n = a \in K$. Ist dann ζ eine primitive n-te Einheitswurzel, so setze $M := L(\zeta)$. Dann ist $K \subseteq L \subseteq M$ ebenfalls Radikalerweiterung. Hierin ist nun M als Zerfällungskörper von $(t^n - a)(t^n - 1)$ galoissch über K.

2. Fall: $m \geq 2$. Dann ist K_{m-1} Radikalerweiterung von K mit

$$[K_{m-1} : K] = \frac{[L : K]}{[L : K_{m-1}]} < [L : K] = r.$$

Nach Induktionsvoraussetzung exisitiert eine galoissche Radikalerweiterung N über K, die K_{m-1} umfaßt. Wegen 4.5, Algebra 1, 3.28 ist N Zerfällungskörper eines Polynoms $g \in K[t]$. Nach Induktionsvoraussetzung gilt $L = K_{m-1}(\gamma)$ mit $\gamma^n \in K_{m-1}$. Hiermit bilden wir das Polynom

$$f(t) := \prod_{\sigma \in G(N/K)} (t^n - \sigma(\gamma^n)) = \sum a_i t^i \in N[t].$$

Nach Konstruktion ist f invariant unter allen $\sigma \in G(N/K)$, d.h. $\sigma(a_i) = a_i \ \forall_i$, also $a_i \in \mathrm{Fix}(G(N/K)) = K$.

Es sei nun M der Zerfällungskörper von f über N. Nach Konstruktion von f ist M Radikalerweiterung von N, also auch von K. Wegen $f(\gamma) = 0$ gilt $\gamma \in M$, also $L \subseteq M$. Es bleibt zu zeigen, daß M/K galoissch ist. Offenbar ist M Zerfällungskörper von gf über K (beachte $f \in K[t]$!), also ist M/K normal (Algebra 1, 3.28) und separabel ($\chi(K) = 0$). □

SATZ 4.23: Es sei $f \in K[t]$ mit $deg(f) \geq 1$. Dann ist $f(x) = 0$ genau dann durch Radikale auflösbar, wenn für einen Zerfällungskörper L von f über K die Galoisgruppe $G(L/K)$ (Galoisgruppe von f) auflösbar ist.

Beweis:

(1) Es sei L Zerfällungskörper von $f \in K[t]$ und $G(L/K)$ auflösbar.
Wir setzen $n := [L : K]$. Zunächst nehmen wir an, daß K eine primitive n-te Einheitswurzel ζ enthält. Zu $G := G(L/K)$ gehöre die Kette $G =: G_0 \supset G_1 \supset \ldots \supset G_r = 1$ mit G_i/G_{i+1} zyklisch (vgl. 1.20.(2)) Ferner sei $F_i := \mathrm{Fix}(G_i)$, $(G_i := G(L/F_i))$ mit $F_0 = K \subset F_1 \subset \ldots \subset F_r = L$. Für $n_i := [F_i : F_{i-1}]$ gilt $n_i | n$, also enthält F_{i-1} eine primitive $n_i i$-te Einheitswurzel.
Wegen $G_i \triangleleft G_{i-1}$ ist F_i/F_{i-1} galoissch (vgl. 4.6 die betreffende Galoisgruppe ist isomorph zu G_{i-1}/G_i, also zyklisch. Nunmehr wenden wir 4.20.(2) an und erhalten $F_i = F_{i-1}(\alpha_i)$, mit α_i Wurzel eines Polynoms $t^{n_i} - \beta_i \in F_{i-1}[t]$. Also ist L/K Radikalerweiterung für f.
Enthält K dagegen keine primitive n-te Einheitswurzel, so bilden wir den Zerfällungskörper M von $t^n - 1 \in L[t]$, der dann eine primitive n-te Einheitswurzel ζ enthält. Damit setze $K_1 := K(\zeta)$ und $L_1 = K_1 L$. L_1 ist nun Zerfällungskörper von f über K_1 und $G(L_1/K_1)$ ist isomorph zu einer Untergruppe von $G = G(L/K)$ nach 4.6, 4.8.
Nach 1.21.(1) ist $G(L_1/K_1)$ auflösbar. Für $m := [L_1 : K_1]$ gilt $m | n$, also enthält K_1 auch eine primitive m-te Einheitswurzel ξ. Wie im ersten Teil des Beweises gezeigt, existiert ein Körperturm $K_1 =: F_0 \subset F_1 \subset \ldots \subset F_r := L_1$, also L_1/K_1 Radikalerweiterung. Wegen $K_1 = K(\zeta)$ ist auch L_1/K Radikalerweiterung mit $L_1 \supseteq L$, d.h. $f(x)$ ist durch Radikale auflösbar.

(2) Sei nun umgekehrt $f(x)$ durch Radikale auflösbar.
Nach 4.22 exististiert ein Körperturm $K =: K_0 \subset K_1 \subset \ldots \subset K_r =: M$, M/K Radikalerweiterung, M enthält Zerfällungskörper L von f über K, M/K galoissch.
Für $i = 1, \ldots, r$ ist dabei $K_i = K_{i-1}(\alpha_i), \alpha_i$ Wurzel von $t^{n_i} - \beta_i \in K_{i-1}[t]$. Setze $n := n_1 \cdot \ldots \cdot n_r$ und bestimme primitive n-te Einheitswurzel ζ in Erweiterung von M (Zerfällungskörper von $t^n - 1 \in M[t]$). Für $i = 1, \ldots, r$ setze $F_i := K_i(\zeta)$. Dann ist $K(\zeta) =: F_0 \subset F_1 \subset \ldots \subset F_r$ eine normale Radikalerweiterung von $K(\zeta)$. Hierbei ist jeweils $F_i = F_{i-1}(\alpha_i) = K_{i-1}(\alpha_i, \zeta)$, und F_{i-1} enthält eine primitive n_i-te Einheitswurzel. Nach 4.20.(1) ist F_i demnach über F_{i-1} zyklisch. Mit $H_i := G(F_r/F_i)$ $(0 \leq i \leq n\ )$ ist $H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_r = 1$ und dabei $H_i/H_{i+1} = G(F_r/F_i)/G(F_r/F_{i+1}) \cong G(F_{i+1}/F_i)$ zyklisch. Also ist $G(F_r/F_0)$ auflösbar.
Wegen $F_r = K_r K(\zeta) = K_r F_0$ erhalten wir mittles 4.8 $G(F_r/F_0) \cong G(K_r/K_r \cap F_0) =: \tilde{G}$, so daß auch $\tilde{G}$ auflösbar ist.
Schließlich ist F_0/K abelsch 4.18 also $K_r \cap F_0/K$ abelsch und insbesondere $G(K_r \cap F_0/K)$ auflösbar.
$K_r \cap F_0/K$ galoissch impliziert $G(K_r/K_r \cap F_0) \triangleleft G(K_r/K)$; die Faktorgruppe ist dabei isomorph zu $G(K_r \cap F_0/K)$, also abelsch. Damit ist dann auch $G(K_r/K)$ auflösbar nach 1.21.(2) $\Rightarrow G(L/K)$ auflösbar nach 1.21.(1).

□

KAPITEL 5

Moduln

1. Einführung

DEFINITION 5.1: Es sei R ein Ring. Ein (links) *R-Modul* M ist eine Abelsche Gruppe zusammen mit eine Verknüpfung: $\circ : R \times M \to M$ mit $(rs) \circ m = r \circ (s \circ m)$, $(r+s) \circ m = r \circ m + s \circ m$ und $r \circ (m+n) = r \circ m + r \circ n$
M heißt *unitär*, falls R ein Einselement $1 \neq 0$ besitzt und $1 \circ m = m$ für jedes $m \in M$ gilt.
Eine Teilmenge U eines R-Moduls M heißt *Untermodul* (*Teilmodul*) von M, falls gelten:
(1) U ist Untergruppe von M,
(2) $RU \subseteq U$.

(Ein Modul ist im Prinzip ein Vektorraum über einem Ring)

Ist M ein Modul, so ist der Durchschnitt von Teilmoduln von M wieder ein Teilmodul. Also existiert zu jeder Teilmenge $A \subseteq M$ ein kleinster Teilmodul von M der A enthält.

DEFINITION 5.2: Es sei M ein R-Modul. Für $A \subseteq M$ bezeichne $\langle A \rangle$ den kleinsten Teilmodul von M der A enthält.
M heißt *endlich erzeugt*, falls $A \subseteq M$ mit $\#A < \infty$ und $M = \langle A \rangle$ existiert.

Ist M ein unitärer Modul, so gilt

$$\langle A \rangle = \{ \sum_{\text{fin.}} r_a a \mid a \in A, r_a \in R \}$$

Für eine Familie $(M_i)_{i \in I}$ von Teilmoduln von M mit

$$M_j \cap \langle M_i \mid i \in I, i \neq j \rangle = \{0\}$$

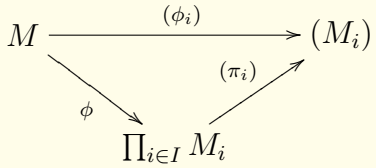
für jedes $j \in I$ heißt

$$\dot{+}_{i \in I} M_i := \langle M_i \mid i \in I \rangle$$

die *innere direkte Summe*. Für eine beliebige Familie von R-Moduln wird das direkte (äußere) Produkt $\prod_{i \in I} M_i$ und die äußere direkte Summe $\oplus_{i \in I} M_i$ wie üblich definiert. Sie haben die unviversellen Abbildungseigenschaften:

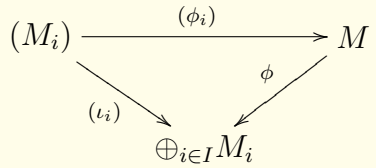
SATZ 5.3: Es sei $(M_i)_{i\in i}$ eine Familie von R-Moduln.

(1) Für jeden R-Modul M und jede Familie $\phi_i \in \mathrm{Hom}_R(M, M_i)$ von Abbildung gibt es genau eine Abbildung $\phi : M \to \prod_{i\in I} M_i$ so, daß das folgende Diagramm kommutiert.



Die $\pi_i : \prod_{i\in I} M_i \to M_i : (m_i)_i \mapsto m_i$ sind die kanonischen Projektionen.

(2) Für jeden R-Modul M und jede Familie $\phi_i \in \mathrm{Hom}_R(M_i, M)$ von Abbildung gibt es genau eine Abbildung $\phi : M \to \oplus_{i\in I} M_i$ so, daß das folgende Diagramm kommutiert.



Die $\iota : M_i \to \oplus_{i\in I} M_i : m_i \mapsto (m_j)_j$ mit $m_j = 0$ für $i \neq j$ sind die kanonischen Injektionen.

BEWEIS. Übung □

HILFSSATZ 5.4: Unter der Festsetzung $\alpha\circ(x+U) := \alpha\circ x+U$ wird die Faktorgruppe M/U eines R-Moduls M mit Untermodul U zu einem R-Modul (*Faktormodul*).

DEFINITION 5.5: Seien M, $\tilde{M}$ zwei R-Moduln und $\varphi : M \to \tilde{M}$ ein Gruppenhomomorphismus. Falls

$$\varphi(\alpha \circ m) = \alpha \circ \varphi(m) \quad \forall\, \alpha \in R\, \forall\, m \in M$$

gilt, so heißt φ *R-Modulhomomorphismus*, $\varphi \in \mathrm{Hom}_R(M, \tilde{M})$.

HILFSSATZ 5.6: Seien $M, \tilde{M}$ zwei R–Moduln und $\varphi : M \to \tilde{M}$ ein R-Modulhomomorphismus. Dann gelten:

(1) $\mathrm{bild}(\varphi) \cong M/\ker(\varphi)$,
(2) $(U + V)/U \cong V/(U \cap V)$ für Teilmoduln U,V von M,
(3) $M/V \cong (M/U)/(V/U)$ für U,V wie in (2) mit $U \subseteq V$.

BEWEIS. Wie für Gruppen, Ringe, Vektorräume. □

DEFINITION 5.7: Für $A \subseteq M$ ist $\mathrm{Ann}(A) := \{r \in R \mid \forall m \in A : rm = 0\}$ der *Annulator* von A. Falls $\mathrm{Ann}(M) = \{0\}$ gilt, so heißt M *treu* (eng. faithful). $m \in M$ heißt *Torsionselement*, falls $\mathrm{Ann}(m) \neq 0$. $\mathrm{Tor}\, M := \{m \in M \mid \mathrm{Ann}(m) \neq 0\}$. M heißt *Torsionsmodul*, falls $\mathrm{Tor}\, M = M$ gilt, M heißt *torsionsfrei*, falls $\mathrm{Tor}(M) = 0$ gilt.

HILFSSATZ 5.8: (1) Für $U \subseteq M$ ist $\mathrm{Ann}(U)$ ein Linksideal von R.
(2) Ist $M \neq \{0\}$ torsionsfrei, so hat R keine Nullteiler.

BEWEIS. Für $m \in M$ und $\phi_m : R \to M : r \mapsto rm$ gilt $\ker \phi_m = \mathrm{Ann}(m)$. Ferner: $\mathrm{Ann}(U) = \bigcap_{m\in U} \ker \phi_M$, daher ist Ann ein (Links-) Ideal. Es seien $r \neq 0 \neq s$ mit $sr = 0$ gegeben. Dann ist $s(rm) = (sr)m = 0$ und rm ein Torsionselement. □

BEMERKUNG 5.9: $\mathrm{Tor}(M)$ ist im allgemeinen kein Untermodul von M (etwa $M = R = \mathbb{Z}/6\mathbb{Z} \Rightarrow \mathrm{Tor}(M) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\} \Rightarrow \mathrm{Tor}(M)$ ist keine Untergruppe von $(M, +)$, also auch kein Untermodul).

HILFSSATZ 5.10: Es sei R ein Integritätsring und M ein R-Modul. Dann ist $\mathrm{Tor}\, M$ ein Teilmodul und $M/\mathrm{Tor}\, M$ ist torsionsfrei.

BEWEIS. Setze $\tilde{M} := \mathrm{Tor}(M)$. Seien $x, y \in \tilde{M}$ mit $\alpha, \beta \in R, \alpha \neq 0 \neq \beta$, so daß $\alpha \circ x = \beta \circ y = 0$ gilt $\Rightarrow$

$$\alpha\beta \circ (x - y) = \alpha\beta \circ x - \alpha\beta \circ y = \beta \circ (\alpha \circ x) - \alpha \circ (\beta \circ y) = 0$$

$\Rightarrow x - y \in \tilde{M}$ wegen $\alpha\beta \neq 0 \Rightarrow (\tilde{M}, +)$ ist Untergruppe von $(M, +)$. Für x, α wie oben folgt weiter

$$\alpha \circ (\beta \circ x) = (\alpha\beta) \circ x = \beta \circ (\alpha \circ x) = 0 \qquad \forall \beta \in R$$

$\Rightarrow \beta \circ x \in \tilde{M} \Rightarrow R \circ \tilde{M} \subseteq \tilde{M}$. Also ist $\mathrm{Tor}(M)$ Untermodul von M.

Seien nun $x + \tilde{M} \in M/\tilde{M}$ und $\alpha \in R$ mit $\alpha \circ (x + \tilde{M}) = \alpha \circ x + \tilde{M} = \tilde{M}$. Dies impliziert $\alpha \circ x \in \tilde{M} \Rightarrow \exists\, \beta \in R, \beta \neq 0$ mit $\beta\alpha \circ x = 0$. Für $\alpha \neq 0$ ist dann $\beta\alpha \neq 0 \Rightarrow x \in \tilde{M} \Rightarrow x + \tilde{M} = \tilde{M}$. Also ist $M/\mathrm{Tor}(M)$ torsionsfrei. □

2. Freie Moduln

DEFINITION 5.11: Eine endliche Teilmenge $\{x_1, \ldots, x_n\}$ eines R-Moduls M heißt *über R frei* (unabhängig), falls aus $\sum_{i=1}^{r} \alpha_i \cdot x_i = 0$ für $\alpha_1, \ldots, \alpha_r \in R$ bereits $\alpha_1 = \ldots = \alpha_r = 0$ folgt. Eine beliebige Teilmenge S von M heißt frei, falls jede endliche Teilmenge von S frei ist.
$S \subseteq M$ heißt Basis von M, falls S frei ist und $\langle S \rangle = M$ gilt. Ein Modul mit Basis heißt freier Modul.

BEMERKUNG 5.12: $\emptyset$ ist frei

M frei $\Rightarrow M$ torsionsfrei. Die Umkehrung ist i. allg. falsch.

SATZ 5.13: Es sei $X \subset M$, M ein unitärer R-Modul. Dann sind äquivalent:

(1) Für jeden R-Modul N und jede Abbildung $\phi : X \to N$ existiert genau ein Homomorphismus $\Phi : M \to N$ der ϕ fortsetzt.
(2) Für jedes $x \in X$ ist die Abbildung $rx \mapsto r$ ein R-Modul-Isomorphismus zwischen Rx und R. Ferner gilt $M = \dot{+}_{x\in X} Rx$
(3) M ist frei mit Basis X
(4) Jedes $m \in M$ besitzt eine eindeutige Darstellung $m = \sum_{\text{fin.}} r_x x$
(5) $M \cong \oplus_{x\in X} R$, wobei die Isomorphie durch $(r_x)_x \mapsto \sum r_x x$ gegeben ist.

BEWEIS. „(1)⇒(2)“: Sei $x_0 \in X$ fixiert. Nach Vorrausstzung gibt es genau eine Fortsetzung von $x \to \begin{cases} 1 & \text{für } x = x_0 \\ 0 & \text{sonst.} \end{cases}$. Diese leistet $s \circ x_0 \mapsto s$ und ist daher bijektiv.

Definiere $N := \langle X \rangle$ und $\phi : X \to N : x \mapsto x$. Nach Voraussetzung gibt es genau eine Fortsetzung $\Phi : M \to N$. Ferner sei $\psi : N \to M : m \mapsto m$ die triviale Einbettung. Dann gilt $\psi\phi(x) = x$ für $x \in X$ und daher $\psi\Phi = \mathrm{id}$. Offenbar folgt damit $\Phi = \mathrm{id}$ und $N = M$. Es sei nun $0 = \sum_{\text{fin.}} r_x x$ gegeben. Definiere $\phi : X \to \oplus_{x \in X} Rx : x \mapsto (\begin{cases} x & \text{für } y = x \\ 0 & \text{sonst.} \end{cases})_{y \in X}$ Für die Fortsetzung $\Phi : M \to \oplus_{x \in X} Rx$ gilt nun $0 = \Phi(0) = \Phi(\sum_{\text{fin.}} r_x x) = \sum_{\text{fin.}} r_x \Phi(x) = (r_x)_x$ und daher $r_x = 0$ für jedes $x \in X$. Damit folgt $M = \dot{+}_{x \in X} Rx$.

„(2)⇒(3)“: $M = \dot{+}_{x \in X} Rx \Rightarrow M = \langle X \rangle$. X ist frei, da anderfalls die Summe nicht direkt ist.

„(3)⇒(4)“: Jedes $m \in M$ hat eine Darstellung in der Form $\sum_{\text{fin.}} r_x x$ (Definition der Basis). Es sei $\sum_{\text{fin.}} r_x x = \sum_{\text{fin.}} s_x x$. Dann folgt $\sum_{\text{fin.}} (r_x - s_x)x = 0$ und daher $r_s = s_x$ da X frei ist.

„(4)⇒(5)“: Da sich jedes $m \in M$ eindeutig in der Form $m = \sum r_x x$ darstellen lässt ist, sind die Abbildungen $\phi_x : M \to R : m = \sum r_y y \mapsto r_x$ für jedes $x \in X$ R-linear. Offenbar ist $\Phi : M \to \oplus_{x \in X} m \mapsto (\phi_x(m))_x$ daher linear und wohldefiniert. Φ ist injektiv, da die Darstellung eindeutig ist und surjektiv, da $\Psi : \oplus_{x \in X} Rx \to M : (r_x)_x \mapsto \sum r_x x$ nach Voraussetzung surjektiv ist und offenbar invers zu Φ.

„(5)⇒(1)“: Es sei $\phi : X \to N$ beliebig gegeben. Mittels $\Phi : \oplus_{x \in X} R \to N : (r_x)_x \mapsto \sum r_x \phi(x)$ erhalten wir eine Fortsetzung auf $\oplus_{x \in X} Rx$ und mit $\oplus_{x \in X} Rx \cong M$ eine auf M. □

BEISPIEL 5.14: Vektorräume (diese sind stets frei), Ringe über sich selbst.

Es sei K ein Körper, V ein K-Vektorraum. Dann ist V ein $\mathrm{End}(V)$-Modul mittels $(\phi, v) \mapsto \phi(v)$.

Gruppen sind $\mathbb{Z}$-Moduln ($\mathbb{Z}G$, Gruppenringe)

In einem kommutativem Ring R gilt: Ein Ideal $\mathfrak{a} \subseteq R$ ist ein freier R-Modul $\iff$ $\mathfrak{a} = (a)$. Beweis: Es sei X eine Basis von $\mathfrak{a}$. Ang. $\{a, b\} \subseteq X$ mit $a \neq b$. Dann gilt $0 = ab - ba$ und X ist nicht frei. Der Rest ist klar.

Es sei $R \subseteq S$ eine unitäre Ringerweiterung. Dann ist S ein unitärer R-Modul.

SATZ 5.15: Es sei R kommutativ und unitär, M endlich erzeugter unitärer R-Modul $\mathfrak{a}$ ein Ideal in R, $\phi \in \mathrm{End}_R(M)$ mit $\phi(M) \subseteq \mathfrak{a}M$. Dann gibt es $a_i \in \mathfrak{a}$ mit

$$\phi^n + \sum_{i=0}^{n-1} a_i \phi^i = 0.$$

BEWEIS. Es sei $\langle x_i \mid 1 \leq i \leq n \rangle = M$. Dann gilt $\phi(x_i) \in \mathfrak{a}M$, daher gibt es $a_{i,j} \in \mathfrak{a}$ mit $\phi(x_i) = \sum_{j=1}^{n} a_{i,j}x_j$ (die $a_{i,j}$ sind nicht eindeutig!). $f := \det((a_{i,j})_{i,j} - x\,\mathrm{id}) = x^n + \sum_{i=0}^{n-1} a_i x^i \in x^n + \mathfrak{a}[x]$ erfüllt $f(\phi) = 0$. Denn:

Wir betrachten $A := (a_{i,j} - \phi\delta_{i,j})_{i,j} \in R[\phi]^{n\times n}$. Hierfür gilt:

$$A(x_1, \ldots, x_n)^t = (\sum_{j=1}^{n} a_{i,j}x_j - \phi(x_i))_i = 0.$$

Es sei nun B die adjungierte Matrix: $B := (b_{i,j})_{i,j}$ mit $b_{i,j} := (-1)^{i+j} \det((a_{l,m})_{i\neq l, j\neq m})$. Dann gilt $BA = \det(A)\,\mathrm{id}$, also

$$BA(x_1, \ldots, x_n)^t = 0 = \det(A)(x_1, \ldots, x_n)^t$$

und daher $f(\phi) = \det(A) = 0 \in \mathrm{End}_R(M)$. □

KOROLLAR 5.16: (1) Es seien R, $\mathfrak{a}$, M wie in 5.15. Gilt $\mathfrak{a}M = M$, so gibt es ein $x \in 1 + \mathfrak{a}$ mit $xM = 0$
(2) *Lemma von Nakayama:* Ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, M endlich erzeugter unitärer R-Modul mit $M = \mathfrak{m}M$, so folgt $M = 0$.
(3) Ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, M endlich erzeugter unitärer R-Modul, $N \subseteq M$ ein Teilmodul mit $M = N + \mathfrak{m}M$, so folgt $M = N$

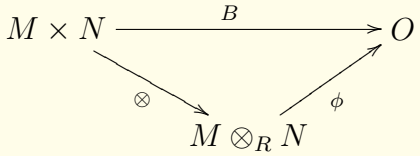
BEWEIS. (1) Wende 5.15 mit $\phi = \mathrm{id}$ an. Dann gibt es $f \in t^n + \mathfrak{a}[t]$ mit $f(\mathrm{id})[m] = 0$ für jedes $m \in M$. Setze $x := f(1) \in R$, hierfür gilt $x \equiv 1 \pmod{\mathfrak{a}}$ und $xM = f(\mathrm{id})M = 0$.
(2) Es gibt ein $x \equiv 1 \pmod{\mathfrak{m}}$. Da R lokal ist, ist x eine Einheit. $xM = 0$ liefert dann $M = 0$.
(3) Betrachte die Faktormoduln nach N.

□

3. Tensorprodukt

DEFINITION 5.17: Es seien M, N, O R-Moduln. Eine Abbildung $B : M \times N \to O$ heißt *bilinear*, wenn $B(., n) : M \to O$ und $B(m, .) : N \to O$ linear (homomorphismen) sind.

SATZ 5.18 (Tensorprodukt): Es seien M, N R-Moduln. Dann gibt es bis auf Isomorphie genau einen R-Modul $M \otimes_R N := M \otimes N$ und eine bilineare Abbildung $. \otimes . : M \times N \to M \otimes_R N : (m, n) \mapsto m \otimes n$ so, daß es zu jedem R-Modul O und jeder bilinearen Abbildung $B : M \times N \to O$ genau einen Homomorphismus $\phi : M \otimes N \to O$ gibt mit $B(m, n) = \phi(m \otimes n)$.



BEWEIS. (Analog zu LA 2) Eindeutigkeit: Übung

Existenz: F sei der freie R-Modul, der von $(m,n) \in M \times N$ erzeugt wird, $G \subseteq F$ sei der Teilmodul der von Ausdrücken der Form $(m_1+m_2,n)-(m_1,n)-(m_2,n)$ $(m_1,\, m_2 \in M,\, n \in N)$ $(am,n)-a(m,n)$, $(a \in R,\, m \in M,\, n \in N)$ $(m,n_1+n_2)-(m,n_1)-(m,n_2)$ $(m \in M,\, n_1,\, n_2 \in N)$ und $(m,an)-a(m,n)$ $(a \in R,\, m \in M,\, n \in N)$ erzeugt wird. Wir definieren $M \otimes_R N := F/G$, $m \otimes N := (m,n)G \in F/G$. Nun gilt: $(m_1+m_2)\otimes n = (m_1 \otimes n)+(m_2 \otimes n)$, $(am)\otimes n = a(m\otimes n) = m \otimes (an)$ und $m \otimes (n_1+n_2) = (m\otimes n_1)+(m\otimes n_2)$, daher ist $m \otimes n$ bilinear.

Es sei nun $B : M \times N \to O$ bilinear gegeben. Definiere $\bar{B} : F \to O$ mittels $(m,n) \mapsto B(x,y)$ und linearer Fortsetzung (5.13.(1)). Dann gilt $\bar{B}|_G = 0$, daher ist $\phi : M \otimes N : m \otimes n \mapsto \bar{B}(m,n)$ wohldefiniert und linear. □

SATZ 5.19: Es sei R kommutativ und unitär. Dann gilt
(1) $a \otimes 0 = 0$
(2) $(M_1 \otimes M_2)\otimes M_3 \cong M_1 \otimes (M_2 \otimes M_3) =: M_1 \otimes M_2 \otimes M_3$
(3) $M_1 \otimes M_2 \cong M_2 \otimes M_1$
(4) $M \otimes (\oplus_{i\in I} N_i) \cong \oplus_{i\in I}(M \otimes N_i)$
(5) $R \otimes M \cong M$

BEWEIS. Exemplarisch: nur (4): Wir definieren $f : M \times \oplus_{i\in I} M_i \to \oplus_{i\in I} M \otimes M_i$: $(x, \oplus_{i\in I} m_i) \mapsto \oplus_{i\in I}(x \otimes m_i)$ f ist bilinear, also existiert ein $g : M \otimes \oplus_{i\in I} M_i \to \oplus_{i\in I} M \otimes M_i$ mit $g(m \otimes \oplus_{i\in I} m_i) = \oplus_{i\in I} m \otimes m_i$. Wir zeigen: g ist injektiv und surjektiv. Es sei $x \in \oplus_{i\in I} M \otimes M_i$ beliebig. Dann hat x eine Darstellung mit $x = \oplus_{i\in I} \sum_{\text{fin.}} n_j \otimes m_{i,j} = \sum_{\text{fin.}} \oplus_{i\in I}(n_j \otimes m_{i,j})$. Für $y := \sum_{\text{fin.}} n_j \otimes \oplus_{i\in I} m_{i,j}$ gilt nun $g(y) = x$.

Um zu zeigen, daß g injektiv ist, geben wir eine Unkehrfunktion an. Definiere $h : \oplus_{i\in I} M \otimes M_i \to M \otimes \oplus_{i\in I} M_i$ als $h(\oplus_{i\in I} m \otimes m_i) := m \otimes \oplus_{i\in I} m_i$. Analog zu g folgt, daß h surjektiv ist. Offenbar gilt $g \circ h = \mathrm{id}$ also muß g injektiv sein. □

BEISPIEL 5.20: (1) Es seien V und W endlich dimensionale K-Vektorräume. Dann ist $V \otimes W$ ebenfalls endlich dimensional. Falls b_i eine Basis für V und c_j eine für W bilden, so ist $b_i \otimes c_j$ eine Basis für $V \otimes W$.
(2) $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$ $(3(a\otimes b) = (3a)\otimes b = a \otimes b = a \otimes (3b) = a \otimes 0 = 0)$
(3) In $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ gilt $2 \otimes 1 = 0$, aber in $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ ist $2 \otimes 1 \neq 0$!

BEMERKUNG 5.21 (Basiswechsel): Es sei $f : A \to B$ ein Ringhomomorphismus. Dann wird B zu einem A-Modul mittels $A \times B \to B : (a,b) \mapsto f(a)b$. Da B ein Ring ist, ist B somit eine *A-Algebra*.

(1) Ist N ein B-Modul, so wird N mittels
$$A \times N \to N : (a,n) \mapsto f(a)n$$
zu einem A-Modul. „*Einschränkung von Skalaren*“
(2) Ist M ein A-Modul, so setze $M_B := B \otimes_A M$. Durch
$$B \times M_B : (b, b' \otimes m) \mapsto (bb') \otimes m$$
wird M_B zu einem B-Modul. „*Erweitern von Skalaren*“

HILFSSATZ 5.22: Es sei R ein kommutativer unitärer Ring, $\mathfrak{a}$ ein Ideal und M ein R-Modul. Dann gilt $M/\mathfrak{a}M \cong R/\mathfrak{a} \otimes_R M$. Speziell für $M = R^n$ folgt: $R^n/\mathfrak{a}R^n \cong (R/\mathfrak{a})^n \cong R/\mathfrak{a} \otimes R^n$.

BEWEIS. Wir betrachten $f : R/\mathfrak{a} \times M/\mathfrak{a}M \to M/\mathfrak{a}M : (r+\mathfrak{a}, m) \mapsto rm + \mathfrak{a}M$. Dies ist wohldefiniert(!) und bilinear, also gibt es nach 5.18 ein $\phi : R/\mathfrak{a} \otimes M \to M/\mathfrak{a}M$ mit $f(r\mathfrak{a}, m) = \phi(r + \mathfrak{a} \otimes m) = rm + \mathfrak{a}M$. ϕ ist offensichtlich surjektiv. Es sei nun $x = \sum_{\text{fin.}} r_i + \mathfrak{a} \otimes m_i \in \ker \phi$. Wegen R (und M) unitär, folgt

$$x = \sum_{\text{fin.}} 1 + \mathfrak{a} \otimes (r_i m_i) = 1 + \mathfrak{a} \otimes \sum_{\text{fin.}} r_i m_i =: 1 + \mathfrak{a} \otimes m,$$

aus $\phi(x) = 0$ folgt nun $m + \mathfrak{a}M = 0$, also $m \in \mathfrak{a}M$. Daher gibt es $a_i \in \mathfrak{a}$, $n_i \in M$ mit $m = \sum_{\text{fin.}} a_i n_i$, also $x = 1 + \mathfrak{a} \otimes M = \sum_{\text{fin.}} a_i \mathfrak{a} \otimes n_i = 0$. Daher ist f injektiv und somit ein Isomorphismus. □

BEISPIEL 5.23: Es sei L/K und E/K Körpererweiterungen. Ferner gelte

$$L = K[t]/f(t)K[t]$$

mit $f \in K[t]$ separabel und irreduzibel. In $E[t]$ sei $f = \prod_{i=1}^n f_i$. Dann folgt: $L \otimes_K E \cong \prod_{i=1}^n E_i$ mit $E_i = E[t]/f_i(t)E[t]$.

Speziell folgt für $K/\mathbb{Q}$ endlich, algebraisch: $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2}$ wobei r_1 die Anzahl der reellen Nullstellen eines Minimalpolynoms für K angibt und $2r_2$ die Anzahl der komplexen Nulstellen ist.

Denn: $K[t] = \oplus_{n\in\mathbb{N}} K t^n$ impliziert (mit 5.19.(4)): $K[t] \otimes_K E \cong \oplus_{n\in\mathbb{N}}(K \otimes_K E)t^n \cong E[t]$. Nach 5.22 folgt für $\mathfrak{a} := f(t)K[t]$ $L \otimes_K E = K[t]/\mathfrak{a} \otimes_K E \cong E[t]/\mathfrak{a}E[t]$. Mit dem Chinesischen Restsatz folgt nun die Behauptung.

Über $\mathbb{R}$ gilt $f = \ell(f) \prod_{i=1}^{r_1}(t - x_i) \prod_{i=1}^{r_2}(t^2 + u_i t + v_i)$ mit $t^2 + u_i t + v$ irreduzibel.

SATZ 5.24: Es sei R ein kommutativer unitärer Ring und M ein freier R-Modul. Dann besitzen je zwei R-Basen von M die gleiche Mächtigkeit.

BEWEIS. Wähle ein maximales Ideal $\mathfrak{m}$ von R. Dann ist $M/\mathfrak{m}M$ nach 5.22 ein $R/\mathfrak{m}$-Modul. Da $R/\mathfrak{m}$ ein Körper ist, also ein Vektorraum. Es sei nun S eine Basis für M. Dann ist S eine Basis für $R/\mathfrak{m} \otimes M$. (Zu zeigen ist nur die Unabhängigkeit von S: Es sei $S' \subseteq S$ beliebig mit $\#S' < \infty$. Nach 5.22 folgt nun $\dim R/\mathfrak{m} \otimes (\oplus_{s\in S'} Rs) = \#S'$) Bei Vektorräumen ist die Dimension eine Invariante, also folgt die Behauptung. □

BEISPIEL 5.25: Im allgemeinen haben Modulbasen verschiedene Mächtigkeit: Es sei K ein Körper und $V := \oplus_{n\in\mathbb{N}} K$ ein Vektorraum mit abzählbar unendlicher Basis $B := \{e_i \mid i \in \mathbb{N}\}$. Nach dem Cantor'schen Diagonalfolgenargument gibt es eine Bijektion $\pi : B \to B \times B$. Mit linearer Fortsetzung erhalten wir eine lineare Abbildung $f : V \to V \oplus V : x \mapsto f(x) = f_1(x) \oplus f_2(x)$. Wir setzen $R := \text{End}_K(V)$ und zeigen: $R \oplus R \cong R$, mittels $\hat{f} : R \oplus R \to R : (u \oplus v)(x) := uf_1(x) + vf_2(x)$. Dies ist ein R-Homomorphismus zwischen den R-Moduln R und R^2. Es sei nun $u \oplus v \in \ker \hat{f}$. Dann gilt $uf_1(x) + vf_2(x) = 0$ für jedes x. Da $f : B \to B^2$ bijektiv ist, folgt $u(x) + v(y) = 0$ für jedes x, $y \in V$ also $u = v = 0$, also ist $\hat{f}$ injektv.

Für $r \in R$ definieren wir $g := rf^{-1} : V^2 \to V$ und $g_1 := g|_{V\oplus 0}$, $g_2 := g|_{0\oplus V}$. Hierfür gilt nun $\hat{f}(g_1 \oplus g_2)(x) = g_1 f_1(x) + g_2 f_2(x) = r(x)$, also ist $\hat{f}$ ein Isomorphismus.

Induktiv erhalten wir $R^n \cong R^m$ für n, $m \in \mathbb{N}$.

SATZ 5.26: Es sei F ein freier unitärer Modul mit Basis x_i $(i \in I)$. Dann gilt für jedes $a \in M \otimes F$: $a = \sum_{\text{fin.}} m_i \otimes x_i$. Diese Darstellung ist eindeutig.

BEWEIS. Für $f \in F$ gilt $f = \sum_{\text{fin.}} r_i x_i$, daher hat jedes $a = m \otimes f \in M \otimes F$ ein Darstellung in der Form $a = \sum_{\text{fin.}} m \otimes r_i x_i = \sum_{\text{fin.}} r_i m \otimes x_i$. Für ein beliebiges $a \in M \otimes F$ gilt $a = \sum_{\text{fin.}} a_i \otimes f_i$, also gilt auch $a = \sum_{\text{fin.}} a'_i \otimes x_i$. Um die Eindeutigkeit zu zeigen, nehmen wir ein $x = \sum_{\text{fin.}} a_i \otimes x_i$ mit $x = 0$ an. Für $j \in I$ betrachten wir $f_j : M \times F \to M : (m, \sum_{\text{fin.}} r_i x_i) \mapsto r_j m$. Da diese Abbildung bilinear ist, gibt es nach 5.18 ein $f'_j : M \otimes F \to M$ mit $f'_j(m \otimes \sum_{\text{fin.}} r_j x_j) = r_j m$. Wegen $x = 0$ folgt daher $0 = f'_j(x) = f'_j(\sum_{\text{fin.}} a_i \otimes x_i) = a_i$. □

SATZ 5.27: Es seien M, M', M'' und N R-Moduln und

$$M' \to M \to M'' \to 0$$

exakt. Dann ist auch

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

exakt.

BEWEIS. Es seien $f : M' \to M$ und $g : M \to M''$ gegeben. Damit erhalten wir Abbildungen $F : M' \otimes N \to M \otimes N : m' \otimes n \mapsto f(m') \otimes n$ und $G : M \otimes N \to M'' \otimes N : m \otimes n \mapsto g(m) \otimes n$. Offenbar ist G surjektiv und $G \circ F = 0$. Zu zeigen bleibt: $\operatorname{bild} F = \ker G$. Alternativ zeigen wir $G' : M \otimes N / F(M' \otimes N) \to M'' \otimes N$ ist injektiv. Dazu werden wir eine zu G' inverse Abbildung konstruieren: Definiere $h : M'' \times N \to M \otimes N / \operatorname{bild} F$ wie folgt. Es sei $(m'', n) \in M'' \times N$ beliebig. Dann gibt es ein $m \in M'$ mit $g(m) = m''$. $h(m'', n) := m \otimes n \operatorname{bild} F$. Dies ist wohldefiniert, da für $m_{1,2}$ mit $g(m_{1,2}) = m''$ offenbar $g(m_1 - m_2) = 0$ folgt, d.h. $m_1 - m_2 \in \ker g = \operatorname{bild} f$, also gibt es $m' \in M'$ mit $f(m') = m_1 - m_2$. Damit folgt $m_1 \otimes n = (m_2 + f(m')) \otimes n = m_2 \otimes n + f(m') \otimes n \in m_2 \otimes n + \operatorname{bild} F$. h ist bilinear, also existiert $H : M'' \otimes N \to M \otimes N / \operatorname{bild} F$ mit $H(m'' \otimes n) = h(m'', n)$. Für $H \circ G' : M \otimes N / \operatorname{bild} F \to M'' \otimes N \to M \otimes N / \operatorname{bild} F$ gilt $H \circ G' = \mathrm{id}$, also ist G' injektiv. □

4. Lokalisierung

Es sei R kommutativ und S eine multiplikative Teilmenge. Auf $M \times S$ haben wir eine Äquivalenzrelation:

$$\frac{m}{s} := (m, s) \sim (m', s') \iff \exists t \in S : t(s'm - sm') = 0.$$

Die Menge der Äquivalenzklassen wird (wie bei Ringen) mit $S^{-1}M$ bezeichnet. Durch $\frac{a}{s} \circ \frac{M}{t} := \frac{a \circ M}{st}$ und $\frac{m}{s} + \frac{n}{t} := \frac{tm+sn}{st}$ wird $S^{-1}M$ zu einem $S^{-1}R$-Modul. Ist $\mathfrak{p}$ ein Primideal und $S := R \setminus \mathfrak{p}$, so schreiben wir $M_\mathfrak{p}$ statt $S^{-1}M$. $M_\mathfrak{p}$ heißt die *Lokalisierung* nach $\mathfrak{p}$.

BEMERKUNG 5.28: Es sei R kommutativ, S eine multiplikative Teilmenge, M und N zwei R Moduln und $f \in \operatorname{Hom}_R(M, N)$. Dann ist $S^{-1}f : S^{-1}M \to S^{-1}N : \frac{m}{s} \mapsto \frac{f(m)}{s}$ in $\operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \neq S^{-1} \operatorname{Hom}_R(M, N)$.

SATZ 5.29: Es sei R kommutativ und unitär, S eine multiplikative Teilmenge und M ein R-Modul. Dann gilt (als $S^{-1}R$-Moduln):

$$S^{-1}R \otimes_R M \cong S^{-1}M$$

BEWEIS. Die Abbildung: $f : S^{-1}R \times M \to S^{-1}M : (\frac{r}{s}, m) \mapsto \frac{rm}{s}$ ist R-bilinear und wohldefiniert. Nach 5.18 gibt es daher eine R-lineare Abbildung $g : S^{-1}R \otimes_R M \to S^{-1}M$ mit $g(\frac{r}{s} \otimes m) = \frac{rm}{s}$. g ist auch $S^{-1}R$-linear und offensichtlich surjektiv. Es seien nun $x = \sum_{\text{fin.}} \frac{r_i}{s_i} \otimes m_i \in \ker g$. Mit $s := \prod s_i$ können wir $x = \frac{1}{s} \otimes m$ erreichen. $x \in \ker g$ bedeutet $\frac{m}{s} = 0$ in $S^{-1}M$. Nach Definition heißt dies: $\exists t \in S$ mit $tm = 0$. Damit erhalten wir $x = \frac{1}{s} \otimes m = \frac{t}{ts} \otimes m = \frac{1}{ts} \otimes tm = \frac{1}{ts} \otimes 0 = 0$ □

SATZ 5.30: Es sei R kommutativ, S eine multiplikative Teilmenge von R und

$$M' \to M \to M''$$

eine exakte Sequenz von R-Moduln. Dann ist

$$S^{-1}M' \to S^{-1}M \to S^{-1}M''$$

ebenfalls exakt.

BEWEIS. Es sei $f : M' \to M$ und $g : M \to M''$. Für $\frac{m}{s} \in S^{-1}M$ gilt:

$$\begin{aligned}
\frac{m}{s} \in \ker S^{-1}g &\iff \frac{g(m)}{s} = 0 \\
&\iff \exists t \in S : 0 = t(g(m) = g(tm) \\
&\iff \exists t \in S, m' \in M' : tm = f(m') \\
&\iff \frac{m}{s} = \frac{f(m')}{st} \in \operatorname{bild} S^{-1}f
\end{aligned}$$

□

KOROLLAR 5.31: Es sei R kommutativ und M ein torsionsfreier R-Modul. Dann läst sich M in einen Vektorraum V über $Q(R)$ einbetten. Die Vektorraumdimension von V heißt *Rationalrang* $r(M)$ von M.

5. Moduln über Hauptidealringen

Ab jetzt sei R ein kommutativer unitärer Hauptidealring.

SATZ 5.32: Sei M ein freier R-Modul vom Rang n über einem Hauptidealring R. Dann ist jeder Untermodul U von M frei vom Rang $m \leq n$.

BEWEIS. Der Induktionsanfang ($n = 0$) ist trivial.

Sei nun $n \geq 1$ und $M = \bigoplus_{i=1}^{n} R \circ x_i$. Setze

$$\tilde{M} := \bigoplus_{i=1}^{n-1} R \circ x_i \subseteq M.$$

Nach Induktionsannahme ist dann $\tilde{U} := U \cap \tilde{M}$ frei vom Rang $\leq n-1$. Also ist man für $U = \tilde{U}$ fertig. Sonst bilde

$$\mathfrak{a} := \left\{ \alpha \in R \mid \exists\, \alpha_1, \ldots, \alpha_{n-1} \in R : \sum_{i=1}^{n-1} \alpha_i \circ x_i + \alpha \cdot x_n \in U \right\}.$$

$\mathfrak{a}$ ist Ideal $\neq \{0\}$ von $R \Rightarrow \mathfrak{a} = R \circ \alpha_n$ (R ist Hauptidealring nach Voraussetzung). Sei nun $y \in U$ mit $y = \sum_{i=1}^{n} \alpha_i \circ x_i$ für $\alpha_1, \dots, \alpha_{n-1} \in R$. Zeige $U = \tilde{U} \oplus R \circ y$. Sei dazu $x \in \tilde{U} \cap R \cdot y \Rightarrow x$ hat eine eindeutige Darstellung $x = \sum_{i=1}^{n-1} \tilde{\alpha}_i \circ x_i$. Ferner besitzt x eine Darstellung $x = \alpha \circ y$ mit $\alpha \in R \Rightarrow x = \sum_{i=1}^{n} \alpha\alpha_i \cdot x_i \Rightarrow \alpha\alpha_n = 0 \Rightarrow \alpha = 0$, da $\alpha_n \neq 0$ und R Integritätsring $\Rightarrow x = 0$. Also gilt $\tilde{U} \cap R \circ y = \{0\}$. Sei nun $u \in U$ beliebig vorgegeben, etwa $u = \sum_{i=1}^{n} \beta_i \circ x_i$. Hierzu existiert $\tilde{\beta} \in R$ mit $\beta_n = \tilde{\beta}\alpha_n \Rightarrow$

$$u - \tilde{\beta} \circ y = \sum_{i=1}^{n} (\beta_i - \tilde{\beta}\alpha_i) \circ x_i = \sum_{i=1}^{n-1} (\beta_i - \tilde{\beta}\alpha_i) \cdot x_i \in \tilde{M}$$

$\Rightarrow u - \tilde{\beta} \circ y \in \tilde{U}$ wegen $u, y \in U \Rightarrow u \in \tilde{U} + R \circ y \Rightarrow U \subseteq \tilde{U} + R \circ y$. Trivialerweise gilt $\tilde{U} + R \circ y \subseteq U$. □

Satz 5.33: Endlich erzeugte, torsionsfreie Moduln über Hauptidealringen sind frei.

Beweis. Nach Voraussetzung gilt

$$M = \sum_{i=1}^{n} Rx_i.$$

Unter den Teilmengen von $\{x_1, \dots, x_n\}$ wähle eine freie mit maximal vielen Elementen. Nach eventueller Umnumerierung sei dies $\{x_1, \dots, x_s\}$. Für $n = s$ ist man fertig. Sei also $s < n$. Für jedes $j \in \{s+1, \dots, n\}$ existieren dann $\alpha_j, \alpha_{ji} \in R$ $(1 \leq i \leq s), \alpha_j \neq 0$ mit

$$\alpha_j x_j = \sum_{i=1}^{s} \alpha_{j,i} x_i$$

$\Rightarrow \alpha_j x_j \in F$ für $F = \sum_{i=1}^{s} Rx_i$.

Bilde $\alpha = \prod_{i=s+1}^{n} \alpha_i \Rightarrow \alpha \neq 0 \Rightarrow \alpha x \in F \ \forall\, x \in M$ bzw. $\alpha M \subseteq F \subseteq M$. Gemäß Satz 5.32 ist αM frei vom Rang $\leq s$. Dann ist $\varphi : M \to \alpha \cdot M : x \mapsto \alpha \cdot x$ ein Modulhomomorphismus, welcher trivialerweise surjektiv und injektiv aufgrund der Torsionsfreiheit von M ist $\Rightarrow M \simeq \alpha \cdot M \Rightarrow M$ ist frei vom Rang s. □

Bemerkung 5.34: $\mathbb{Q}$ ist ein torsionsfreier $\mathbb{Z}$-Modul, aber nicht frei.

Satz 5.35: Seien R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gilt $M = \mathrm{Tor}(M) \oplus F$ mit einem freien Untermodul $F \simeq M/\mathrm{Tor}(M)$.

Beweis. Nach 5.10 und 5.33 ist $M/\mathrm{Tor}(M)$ frei, etwa mit Basis B. Betrachte nun den kanonischen Epimorphismus

$$\varphi : M \to M/\mathrm{Tor}(M) : x \mapsto x + \mathrm{Tor}(M).$$

Zu jedem $b \in B$ wähle ein festes $m_b \in M$ mit $\varphi(m_b) = b$. Bilde $F := \sum_{b \in B} Rm_b \Rightarrow F$ ist Untermodul vom M. Offensichtlich ist $\{m_b \mid b \in B\}$ eine Basis von F. Zeige nun $M = \mathrm{Tor}(M) \oplus F$. Wir haben $F = \tau(M/\mathrm{Tor}(M))$ mit einem Isomorphismus

$$\tau : M/\mathrm{Tor}(M) \to F : \sum_{b \in B} \alpha_b b + \mathrm{Tor}(M) \mapsto \sum_{b \in B} \alpha_b m_b.$$

Für $m \in M$ gilt $m = \tau(\varphi(m)) + (m - \tau(\varphi(m))) \in F + \mathrm{Tor}(M)$. Ist andererseits $x \in F \cap \mathrm{Tor}(M)$, so gilt $x = \tau(\tilde{m})$ mit $\tilde{m} \in M/\mathrm{Tor}(M/R) \Rightarrow$

$$0 = \varphi(x) = \varphi(\tau(\tilde{m})) = \tilde{m} \Rightarrow x = \tau(\tilde{m}) = 0$$

$\Rightarrow F \cap \mathrm{Tor}(M) = \{0\}$. □

Definition 5.36: Seien R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Die invertierbaren Matrizen $U \in R^{n\times n}$ heißen *unimodular*. $\mathrm{GL}(n, R)$ ist die Menge aller invertierbaren Matrizen.

Hilfssatz 5.37: (1) Die unimodularen $(n \times n)$–Matrizen über R bilden eine Gruppe $\mathrm{GL}(n, R)$.
(2) $A \in R^{n\times n}$ ist genau dann unimodular, falls $\det(A) \in R^*$.

Beweis. Übung? Trivial? □

Hilfssatz 5.38: Seien R ein kommutativer Ring mit Eins und M ein freier R–Modul vom Rang n. Für zwei Basen $b_1, \dots, b_n$ und $c_1, \dots, c_n$ von M existiert $U \in \mathrm{GL}(n, R)$ mit

$$(b_1, \dots, b_n) = (c_1, \dots, c_n) \cdot U.$$

Hilfssatz 5.39: Seien R ein Hauptidealring und $a_1, \dots, a_n \in R$. Dann existiert eine Matrix $A \in R^{n\times n}$ mit erster Zeile $a_1, \dots, a_n$ und $\det(A) = \mathrm{ggT}(a_1, \dots, a_n)$.

Beweis. Der Induktionsanfang $(n = 1)$ ist trivial. Für $n > 1$ existiert nach Induktionsannahme $\tilde{A} = (\tilde{a}_{i,j}) \in R^{(n-1)\times(n-1)}$ mit $\tilde{a}_{1,j} = a_j$ $(1 \le j \le n-1)$ und $\det(\tilde{A}) = \mathrm{ggT}(a_1, \dots, a_{n-1})$. Sei $c := \mathrm{ggT}(\det(\tilde{A}), a_n)$. Dann existieren $u, v \in R$ mit $c = u \det(\tilde{A}) + v a_n$. Setze

$$A := \left(\begin{array}{ccc|c} & & & a_n \\ & \tilde{A} & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline b_1 & \cdots & b_{n-1} & u \end{array}\right)$$

mit $b_i = \frac{-v a_i}{\det(\tilde{A})}$ $(1 \le i \le n-1) \Rightarrow \det(A) = u \det(\tilde{A}) + a_n v = c$. □

Hilfssatz 5.40: Seien R ein Hauptidealring und $a_1, \dots, a_n \in R$. Dann existiert $U \in \mathrm{GL}(n, R)$ mit $(a_1, \dots, a_n) \cdot U = (c, 0, \dots, 0)$ für $c := \mathrm{ggT}(a_1, \dots, a_n)$.

Beweis. Bilde $A = (a_{ij}) \in R^{n\times n}$ mit $\det(A) = c$ wie in 5.39. Setze $\tilde{A} = (\tilde{a}_{ij}) \in R^{n\times n}$ mittels $\tilde{a}_{ij} := a_{ij}$ $(2 \le i \le n, 1 \le j \le n)$ und $\tilde{a}_{1j} := \frac{a_{1j}}{c}$ $(1 \le j \le n)$. $\tilde{A}$ ist dann unimodular wegen $\det(\tilde{A}) = 1$ und es gilt $(c, 0, \dots, 0)\tilde{A} = (a_1, \dots, a_n)$. Also erfüllt $\tilde{A}^{-1}$ die Behauptung. □

Für einen kommutativen Ring R mit Eins ist

$$a \sim b : \Longleftrightarrow \exists u \in R^* : a = ub$$

eine Äquivalenzrelation auf R. Im folgenden sei $\mathcal{R} \subseteq R$ ein Vertretersystem für die Äquivalenzklassen (für $R = \mathbb{Z}$ etwa $\mathcal{R} = \mathbb{Z}^{\ge 0}$).

Satz 5.41 (Hermite Normalform): Sei R ein Hauptidealring. Zu jeder Matrix $A \in R^{m\times n}$ existiert $U \in \mathrm{GL}(n, R)$, so daß $A \cdot U$ eine untere Dreiecksmatrix ist, deren Diagonalelemente in $\mathcal{R}$ liegen. $A \cdot U$ heißt eine *Hermite-Normalform* von A.

BEWEIS. Der Induktionsanfang ($n = 1$) ist trivial.

Sei nun $n > 1$. Zu $c = \mathrm{ggT}(a_{11}, \ldots, a_{1n}) \in \mathcal{R}$ existiert nach 5.40 $U_1 \in \mathrm{GL}(n, R)$ mit

$$A \cdot U_1 = \left(\begin{array}{c|ccc} c & 0 & \ldots & 0 \\ \hline * & & \tilde{A} & \end{array}\right).$$

Durch Anwendung der Induktionsannahme auf $\tilde{A}$ erhält man eine Matrix der gewünschten Gestalt. □

BEMERKUNG 5.42: Es sei G eine Abelsche Gruppe die mit Erzeugern und Relationen definiert ist: $G := \langle x_1, \ldots, x_n \mid \sum_{i=1}^{n} a_{i,j} x_i = 0, 1 \leq j \leq m \rangle$. Dann kann mit Hilfe der HNF die Anzahl der Relationen auf n beschränkt werden. Ferner liefert dies ein Verfahren um die Endlichkeit von G nachzuweisen.

SATZ 5.43 (Smith Normalform): Seien R ein Hauptidealring und $A = (a_{ij}) \in R^{m \times n}$ sowie $r = \min(m, n)$. Dann existieren $V \in \mathrm{GL}(m, R)$ und $U \in \mathrm{GL}(n, R)$, so daß für $S(A) := (s_{i,j}) := V \cdot A \cdot U$ gelten:
(1) $s_{i,j} = 0$ $(1 \leq i \leq m, 1 \leq j \leq n, i \neq j)$,
(2) $s_{i,i} | s_{j,j}$ $(1 \leq i \leq j \leq r)$,
(3) $s_{i,i} \in \mathcal{R}$ $(1 \leq i \leq r)$.
$S(A)$ ist eindeutig bestimmt und heißt *Smith–Normalform* von A.

BEWEIS. Wir bestimmen zunächst $\tilde{V} \in \mathrm{GL}(m, R)$ und $\tilde{U} \in \mathrm{GL}(n, R)$, so daß $\tilde{V} \cdot A \cdot \tilde{U}$ die Bedingung (1) erfüllt. Der Induktionsanfang ($n = 1$) folgt aus 5.40. Sei nun $n > 1$. Durch Anwenden von 5.41 erreicht man

$$A \cdot \tilde{U}_1 = \left(\begin{array}{c|c} c_1 & 0 \\ \hline * & A_1 \end{array}\right),$$

und weiter

$$\tilde{V}_2 \cdot A \cdot \tilde{U}_1 = \left(\begin{array}{c|c} c_2 & * \\ \hline 0 & A_2 \end{array}\right), \quad \tilde{V}_2 \cdot A \cdot \tilde{U}_1 \cdot \tilde{U}_2 = \left(\begin{array}{c|c} c_3 & 0 \\ \hline * & A_3 \end{array}\right), \quad \ldots$$

Wegen $c_{i+1} | c_i$ und $c_1 | a_{11}$ terminiert dieser Prozeß, weil a_{11} nur endlich viele Primteiler besitzt. Subtraktionen passender Vielfacher der ersten Zeile oder Spalte liefern dann

$$\left(\begin{array}{c|c} c_k & 0 \\ \hline 0 & A_k \end{array}\right).$$

Durch Anwendung der Induktionsannahme auf A_k erhält man eine Matrix, welche die Bedingung (1) erfüllt.

Um nun $s_{ii} | s_{jj}$ $(1 \leq i < j \leq r)$ zu erreichen, ersetzt man durch passende Spalten– und Zeilenoperationen s_{ii} durch $\mathrm{ggT}(s_{ii}, s_{jj}) \in \mathcal{R}$ und s_{jj} durch $\mathrm{kgV}(s_{ii}, s_{jj}) \in \mathcal{R}$:

Es sei $g := \mathrm{ggT}(s_{ii}, s_{jj}) = rs_{ii} + ts_{jj}$ und $l := s_{ii}s_{jj}/g = \mathrm{kgV}\,(s_{ii}, s_{jj})$. Dann gilt:

$$\begin{pmatrix} s_{ii} & 0 \\ 0 & s_{jj} \end{pmatrix} \overset{\cdot\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)}{\longrightarrow} \begin{pmatrix} s_{ii} & 0 \\ ts_{jj} & s_{jj} \end{pmatrix}$$

$$\overset{\left(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix}\right)\cdot}{\longrightarrow} \begin{pmatrix} s_{ii} & 0 \\ g & s_{jj} \end{pmatrix}$$

$$\overset{\left(\begin{smallmatrix} 1 & -s_{ii}/g \\ 0 & 1 \end{smallmatrix}\right)\cdot}{\longrightarrow} \begin{pmatrix} 0 & -s_{ii}s_{jj}/g \\ g & s_{jj} \end{pmatrix}$$

$$\overset{\cdot\left(\begin{smallmatrix} 1 & l/s_{ii} \\ 0 & 1 \end{smallmatrix}\right)}{\longrightarrow} \begin{pmatrix} 0 & -l \\ g & 0 \end{pmatrix}$$

Zum Beweis der Eindeutigkeit sei $d_i(A)$ der ggT aller (i,i)–Minoren von A $(1 \leq i \leq r) \Rightarrow d_{i-1}(A)|d_i(A)$ $(2 \leq i \leq r)$. Ferner folgt $d_i(A)|d_i(A \cdot B)$ für $B \in R^{n\times n}$, denn die Spalten von $A \cdot B$ sind Linearkombinationen der Spalten von A, so daß jeder Minor von $A \cdot B$ Produkt eines Minors von A ist. Analog folgt $d_i(A)|d_i(C \cdot A)$ für $C \in R^{m\times m}$. Damit erhält man

$$d_i(A)|d_i(A \cdot U)|d_i(V \cdot A \cdot U) = d_i(S(A))|d_i(V^{-1} \cdot S(A) \cdot U^{-1}) = d_i(A).$$

Also gilt

$$d_i(A) = d_i(S(A)) = \prod_{j=1}^{i} s_{jj} \qquad (1 \leq i \leq r).$$

Wegen $s_{ii} = \frac{d_i(A)}{d_{i-1}(A)}$ $(1 \leq i \leq r, d_0(A) := 1)$ ist man fertig. □

Die Diagonalelemente in der Smith Normalform heißen *Elementarteiler* .

BEMERKUNG 5.44: Aus der SNF folgt unmittelbar der Hauptsatz über endlich erzeugte Abelsche Gruppen: $G \cong C_{n_1} \times \cdots \times C_{n_n} \times \mathbb{Z}^r$ mit $n_1| \ldots |n_n$ und $r \geq 0$. Unter diesen Bedingungen sind die n_i und das r eindeutig bestimmt.

KOROLLAR 5.45 (Jordan-Normalform): Sei sei K ein Körper, $\phi \in \mathrm{End}(V^n)$. Dann exisiert die Jordan-Normalform: Es gibt $V_i \subseteq V$ mit

(1) $V_i = K[\phi]x_i$ (V_i ist ϕ-zyklisch)
(2) $V = \dot{+} V_i$
(3) Das Minimalpolynom von $\phi|_{V_i} = f_i^{n_i}$ mit f_i irreduzibel.
(4) Es gibt eine Basis von V_i so, daß die zu $\phi|_{V_i}$ gehörige Matrix die folgende Form hat:

$$\begin{pmatrix} B & \bar{1} & 0 & \dots & 0 \\ 0 & B & \bar{1} & 0\dots & 0 \\ \vdots & & & & \\ 0 & \dots & 0 & B & \bar{1} \\ 0 & \dots & & 0 & B \end{pmatrix}$$

B ist die Begleitmatrix zu $f_i = t^n + \sum_{i=0}^{n-1} a_{i,j}t^j$, d.h.

$$B = \begin{pmatrix} 0 & \dots & & 0 & -a_{i,0} \\ 1 & 0 & \dots & 0 & -a_{i,1} \\ 0 & 1 & \dots & 0 & -a_{i,2} \\ \vdots & & & & \\ 0 & \dots & 0 & 1 & -a_{i,n-2} \\ 0 & \dots & & 0 & -a_{i,n-1} \end{pmatrix}$$

und

$$\bar{1} = \begin{pmatrix} 0 & & \dots & 0 \\ 0 & & \dots & 0 \\ \vdots & & & \\ 0 & & \dots & 0 \\ 1 & 0\dots & 0 & \end{pmatrix}$$

BEWEIS. Wir defieren auf $V := K^n$ eine $K[x]$ Modulstruktur mittels $(f, v) \mapsto f(\phi)[v]$. Damit ist V ein (Torsions-) Modul über einem Hauptidealring. Es sei $R := \langle \phi(e_i) - (x\delta_{i,j})_i \mid 1 \le i \le n \rangle \le K[x]^n$. Dann gilt (als $K[x]$-Modul): $V \cong K[x]^n/R$. Auf die Matrix $A := \phi - \mathrm{id}\, x \in K[x]^{n\times n}$ wenden wir nun 5.43 an und erhalten eine Basis E_i von $K[x]^n$ bzgl. der $A = \mathrm{diag}(f_1, \dots, f_n)$ mit $f_1|f_2|\dots|f_n$ gilt. $A \bmod R$ induziert nun eine Basis von V mit den gewünschten Eigenschaften. □

HILFSSATZ 5.46: Es seien $N \subseteq M$ freie Moduln mit $\mathrm{rg}(N) =: n \le \mathrm{rg}(M) =: m$. (o.B.d.A.: $N \subseteq R^n$, $M \subseteq R^m$)

(1) Für jede Basis a_i ($1 \le i \le n$) von M existiert eine Basis b_j ($1 \le j \le m$) von N und eine obere Dreiecksmatrix A mit $(b_1, \dots, b_n) = (a_1, \dots, a_m)A$. Die Zeilen von A sind modulo $a_{i,i}$ eindeutig.
(2) Zu jeder Basis b_i ($1 \le i \le n$) von N existiert eine Basis a_j ($1 \le j \le m$) vom M und eine obere Dreiecksmatrix A mit $(b_1, \dots, b_n) = A(a_1, \dots, a_m)$. Die Spalten von A sind modulo $a_{i,i}$ eindeutig.
(3) In N und M existieren Basen a_i ($1 \le i \le n$) und b_j ($1 \le j \le m$) mit $b_i = \epsilon_i a_i$ ($1 \le i \le n$) $\epsilon_i|\epsilon_{i+1}$ ($1 \le i < n$), $\epsilon_0 := 1$ und die ϵ_i sind durch N und M eindeutig bestimmt.

BEWEIS. Übung. □

HILFSSATZ 5.47: M sei sein freier Modul mit Basis b_i $(1 \leq i \leq n)$. Ferner sei $i \in \{1, \dots, n\}$ und $c_i := \sum_{j=1}^{n} \gamma_j b_j \in M$. Dann ist $b_1, \dots, b_{i-1}, c_i$ genau dann zu einer Basis von M ergänzbar, wenn $\mathrm{ggT}(\gamma_i, \dots, \gamma_n) = 1$ ist.

BEWEIS. Übung. □

6. Projektive Moduln I und Auflösungen

SATZ 5.48: Es seien A, B, C R-Moduln, F ein freier R-Modul, das folgende Diagram exakt und $C = 0$ oder $\beta f = 0$:

$$\begin{array}{ccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \\ & & \uparrow{\scriptstyle f} & & \\ & & F & & \end{array}$$

Dann gibt es einen Homomorphismus $g : F \to A$ mit $\alpha g = f$.

BEWEIS. Es sei F frei von X erzeugt. Nach Voraussetzung gilt: $\beta f(x) = 0$, $f(x) \in \ker \beta = \mathrm{bild}\, \alpha$. Also gibt es ein $a_x \in A$ mit $\alpha(a_x) = f(x)$ Nach 5.13.(1) gibt es eine Fortsetzung $g : F \to A$ mit $g(x) = a_x$. Diese erfüllt $\alpha g(x) = f(x)$ für $x \in X$. Nach 5.13.(2) gilt dies dann auch für F. □

BEMERKUNG 5.49: Ein Modul F für den 5.48 gilt, heißt *projektiv*

DEFINITION 5.50: Eine Familie von freien (projektiven) R-Moduln M_i, $i \in \mathbb{N}$ zusammen mit einer Familie von Homomorphismen $d_i : M_i \to M_{i-1}$ heißt freie Auflösung (projektive Auflösung) von $\mathbb{Z}$, falls

$$\text{(5-1)} \quad \dots \to M_n \xrightarrow{d_n} M_{n-1} \to \dots \to M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} \mathbb{Z} \to 0$$

eine exakt ist.

BEMERKUNG 5.51: Es sei $\alpha : M \to M'$ ein R-Modulhomomorphismus, und N ein weiterer R-Modul. Dann ist $\alpha^* : \mathrm{Hom}(M', N) \to \mathrm{Hom}(M, N) : \alpha^*(\phi)[m] := \phi\alpha(m)$ ebenfalls ein Modulhomomorphismus. (analog zu dualen Abbildungen)

Es gilt $(\alpha\beta)^* = \beta^*\alpha^*$ und $(\alpha + \beta)^* = \alpha^* + \beta^*$. (Übung)

SATZ 5.52: Es sei

$$0 \xleftarrow{\alpha} A \xleftarrow{\beta} B \xleftarrow{\gamma} C$$

eine exakte Sequenz von R-Moduln. Dann ist

$$0 \xrightarrow{\alpha^*} \mathrm{Hom}(A, M) \xrightarrow{\beta^*} \mathrm{Hom}(B, M) \xrightarrow{\gamma^*} \mathrm{Hom}(C, M)$$

exakt (für jeden R-Modul M).

BEWEIS. Wegen $\alpha\beta = 0$ folgt auch $\beta^*\alpha^* = 0$, d.h. $\mathrm{bild}\, \alpha^* \subseteq \ker \beta^*$, analog $\mathrm{bild}\, \beta^* \subseteq \ker \gamma^*$.

Zeige: $\mathrm{bild}\, \alpha^* = \ker \beta^*$, d.h. β^* injektiv: Es sei $f \in \mathrm{Hom}(A, M)$ mit $\beta^*(f) = 0$. $\Rightarrow$ $\beta^*(f)[b] = f\beta(b) = 0$. Da β surjektiv ist, folgt $f = 0$.

Zeige $\mathrm{bild}\, \beta^* = \ker \gamma^*$: Es sei $f \in \mathrm{Hom}(B, M)$ mit $\gamma^*(f) = 0$. Dann gilt $\gamma^*(f)[c] = f\gamma(c) = 0$. Wegen $\mathrm{bild}\, \gamma = \ker \beta$, folgt $f|_{\ker \beta} = 0$. $f' : A \to M : a \mapsto f(\beta^{-1}(a))$

ist daher wohldefiniert (wegen β surjektiv gilt $\beta^{-1}(a) \neq \emptyset$). $\beta^*(f')[b] = f'\beta(b) = f(b)$. □

BEISPIEL 5.53:

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

ist exakt, aber

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0 \\ & & \| \downarrow & & \| \downarrow & & \| \downarrow \\ 0 & \longrightarrow & C_2 & \longrightarrow & C_2 & \longrightarrow & C_2 \to 0 \end{array}$$

ist rechts nicht exakt!.

DEFINITION 5.54: Ein *Komplex* ist eine Sequenz

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

mit $\beta\alpha = 0$.

KOROLLAR 5.55: Es sei R ein Ring, und

$$\cdots \to M_n \xrightarrow{d_n} M_{n-1} \to \cdots \to M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} \mathbb{Z} \to 0$$

eine freie Auflösung.
Dann erhalten wir für jeden R-Modul M den folgenden Komplex:

$$0 \to \mathrm{Hom}(\mathbb{Z}, M) \xrightarrow{d_0^*} \mathrm{Hom}(M_0, M) \xrightarrow{d_1^*} \mathrm{Hom}(M_1, M) \to \cdots \to \mathrm{Hom}(M_{n-1}, M) \xrightarrow{d_n^*} \mathrm{Hom}(M_n, M) \to \cdots \tag{5-2}$$

Dieser ist bei M_0 und $\mathbb{Z}$ exakt.

HILFSSATZ 5.56: Es seien A, B, C, A', B', C' projektive R-Moduln, α, β, α', β', f, g Homomorphismen so, daß

$$\begin{array}{ccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \\ & & f \downarrow & & g \downarrow \\ A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' \end{array}$$

ein kommutatives Diagramm mit exakten Zeilen ist. Dann gibt es ein $h : A \to A'$ so, daß das gesamte Diagramm kommutiert.

BEWEIS. Wir definieren $h' := f\alpha$. Dann gilt $\beta' h' = \beta' f\alpha = g\beta\alpha = 0$ (Exaktheit der 1. Zeile). Mit 5.48 folgt die Existenz von $h : A \to A'$ mit $\alpha' h = h'$. Damit gilt: $\alpha' h = h' = f\alpha$, das Diagramm kommutiert. □

HILFSSATZ 5.57: (1) Gegeben seien zwei freie Auflösungen (M_n, d_n) und (M'_n, d'_n) von $\mathbb{Z}$. Dann gibt es Homomorphismen $f_i : M_i \to M'_i$ so, dass das Diagramm kommutiert:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\cdots & \longrightarrow & M'_2 & \longrightarrow & M'_1 & \longrightarrow & M'_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

(2) Wenn nun f'_i eine weitere Familie von Homomorphismen die das Diagramm kommutativ machen. Dann sind $(f_i)_i$ und $(f'_i)_i$ *homotop*, d.h. es gibt eine Familie von Homomorphismen $h_i : M_i \to M'_{i+1}$ mit $f_i - f'_i = d'_{i+1}h_i + h_{i-1}d_i$.

$$\begin{array}{ccccccc}
M_{i+1} & \longrightarrow & M_i & \xrightarrow{d_i} & M_{i-1} & & \\
 & \swarrow{\scriptstyle h_i} & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f'_i} & \searrow{\scriptstyle h_{i-1}} & \\
M'_{i+1} & \xrightarrow{d'_{i+1}} & M'_i & \longrightarrow & M'_{i-1} & &
\end{array}$$

BEWEIS. Die Existenz der f_i wird per Induktion gezeigt. Für $i = -1, -2$ ist die Behauptung klar ($f_{-1} := \mathrm{id}_{\mathbb{Z}}$, $f_{-2} := \mathrm{id}_0$). Es gelte daher

$$\begin{array}{ccccccccc}
M_{i+1} & \xrightarrow{d_{i+1}} & M_i & \xrightarrow{d_i} & M_{i-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i-1}} & & \\
M'_{i+1} & \xrightarrow{d'_{i+1}} & M'_i & \xrightarrow{d'_i} & M'_{i-1} & \longrightarrow & \cdots
\end{array}$$

Mit 5.56 erhalten wir f_{i+1} mit den gewünschten Eigenschaften.

Homotopie: per Induktion. $i = 0$ ist klar. Es sei also h_{i-1} mit

$$f_{i-1} - f'_{i-1} = d'_i h_{i-1} + h'_{i-2} d_{i-1} \tag{5-3}$$

bereits gefunden. Wir setzen $f := f_i - f'_i - h_{i-1}d_i$. Dann gilt

$$\begin{aligned}
d'_i f &= d'_i(f_i - f'_i - h_{i-1}d_i) = d'_i(f_i - f'_i) - d'_i h_{i-1} d_i \\
&= d'_i f_i - d'_i f'_i - d'_i h_{i-1} d_i \\
&= f_{i-1}d_i - f'_{i-1}d_i - d'_i h_{i-1} d_i \\
&= (f_{i-1} - f_{i-1})d_i - d'_i h_{i-1} d_i \\
&= (d'_i h_{i-1} + h_{i-2}d_{i-1})d_i - d'_i h_{i-1} d_i \\
&= 0
\end{aligned}$$

Mit 5.48 gibt es dann $h_i : M_i \to M'_{i+1}$ mit $f_i - f'_i - h_{i-1}d_i = f = d'_{i+1}h_i$. □

KAPITEL 6

Kohomologie

Kohomologie (Homologische Algebra) spielt eine wichtige Rolle in vielen modernen Zweigen der Mathematik. Wir werden hier nur die einfachsten Grundlagen einführen.

1. Gruppenerweiterungen

Motivation: Sei $M/L/K$ ein normaler Körperturm: M/K und L/K seien normal. $G(L/K) := N$, $G(M/L) := G$ $G(M/K) := E$. Was können wir über die drei Gruppen aussagen?

(1) $N \triangleleft E$,
(2) $G \cong E/N$

Beispiel 6.1: Es sei $K := \mathbb{Q}$, $L := \mathbb{Q}(\sqrt{2})$, $M_1 := L(\sqrt{3})$, $M_2 := L(\sqrt{\sqrt{2}})$ und $M_3 := L(\sqrt{2+\sqrt{2}})$ Dann gilt $G(L/\mathbb{Q}) \cong G(M_i/L) \cong C_2$ aber $G(M_1/K) \cong V_4$, $G(M_2/K) \cong D_4$ und $G(M_3/K) \cong C_4$ Denn:

$M_1 = \mathbb{Q}(\sqrt{2},\sqrt{3})$ hat Grad 4 über $\mathbb{Q}$. Wir haben die nichttrivialen Automorphismen: $(\sqrt{2},\sqrt{3}) \mapsto \begin{cases}(-\sqrt{2},\sqrt{3})\\(\sqrt{2},-\sqrt{3})\\(-\sqrt{2},-\sqrt{3})\end{cases}$ Offensichtlich haben alle Automorphismen die Ordnung 2.

Es gilt $M_2 = \mathbb{Q}(\sqrt[4]{2})$, M_2 ist nicht normal über $\mathbb{Q}$: $f := t^4 - 2$ hat in $\mathbb{C}$ die Nullstellen $\alpha_l := i^l \sqrt[4]{2}$ mit $1 \le l \le 4$. M_2 normal $\Rightarrow \alpha_2/\alpha_1 = i \in M_3$. Offensichtlich gilt jedoch $M_2 \subseteq \mathbb{R}$. (Und daher ist M_2 auch kein Beispiel für die Gruppenerweiterung!) In $M_2' := M_2(i) = \mathbb{Q}(\sqrt[4]{2}, i)$ gibt es nun 8 Automorphismen:

$$(\sqrt[4]{2}, i) \mapsto \begin{cases}(\pm\sqrt[4]{2}, \pm i)\\(\pm i\sqrt[4]{2}, \pm i)\end{cases}$$

Es gilt $G(M_2'/\mathbb{Q}) \cong D_4$.

Für M_3 benötgen wir noch einen Hilfssatz:

Hilfssatz 6.2: Es sei $\chi(K) \neq 2$, $a \neq K^2$ und $L := K(\sqrt{a})$. Dann gibt es genau dann ein $M/L/K$ mit $G(M/K) \cong C_4$, wenn $a \in K^2 + K^2$ gilt.

BEWEIS. Es gilt $K(\sqrt{a}) = K(\sqrt{b})$ genau dann, wenn $a/b \in K^2$ gilt. Sei nun $[M : L] = 2$. Dann können wir $M = L(\sqrt{s+t\sqrt{a}})$ annehmen. Ferner gilt $t \neq 0$, da andernfalls sofort $G(M/K) \cong V_4$ folgt. Also ist $(t^2-(s+t\sqrt{a}))(t^2-(s-t\sqrt{a})) \in K[t]$ vom Grad 4 irreduzibel mit einer Nullstelle $\alpha := \sqrt{s+t\sqrt{a}} \in M$. Wenn nun M normal ist, muß daher auch $t^2 - (s - t\sqrt{a}) \in L[t]$ eine Nullstelle β haben. Aus $M = L(\alpha) = L(\beta)$ folgt nun $\alpha^2/\beta^2 = c$ mit $c \in L^2$. Also $\tilde{c}^2 := c\beta^4 = (a\alpha\beta)^2 \in L^2$. Mit $\tilde{c} = u + v\sqrt{a}$ erhalten wir

$$\tilde{c}^2 = u^2 + av^2 + 2uv\sqrt{a} = (\alpha\beta)^2 = \mathrm{N}_{K/\mathbb{Q}}(\alpha^2) = s^2 - at^2$$

Mittels Koeffizientenvergleich folgt $u = 0$ oder $v = 0$. Aus $v = 0$ erhalten wir $\tilde{c} \in K$. Der Automorphismus

$$\rho : \sqrt{s+t\sqrt{a}} \mapsto c\sqrt{s-t\sqrt{a}} = \tilde{c}\sqrt{\frac{1}{s+t\sqrt{a}}} = u\sqrt{\dots}$$

hat dann nur Ordnung 2. Damit haben dann alle Automorphismen Ordnung 2 (Warum?) und die $G(M/K) \cong V_4$.

Mit $u = 0$ folgt $a = s^2/(v^2+t^2) = ((sv)/(v^2+t^2))^2 + ((st)/(v^2+t^2))^2$, der Automorphismus hat nun Ordnung 4. □

Mit $s = 2$, $t = 1$, $v = 1$ erhalten wir nun unser Beispiel.

DEFINITION 6.3: Es seien drei Gruppen $N \triangleleft G$, $E \cong G/N$ gegeben. Dann nennen wir G eine *Gruppenerweiterung* von N mit E.

Gruppenerweiterungen entsprechen kurzen exakten Sequenzen:

$$1 \to N \to G \to E \to 1 \tag{6-1}$$

Im folgenden seien N und E beliebige Gruppen. Wir werden untersuchen wann es Gruppen G gibt (und welche), so daß (6-1) gilt.

LEMMA 6.4: Es sei

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\kappa} & B & \xrightarrow{\lambda} & C & \longrightarrow & 1 \\ & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & & \\ 1 & \longrightarrow & A' & \xrightarrow{\sigma} & B' & \xrightarrow{\rho} & C' & \longrightarrow & 1 \end{array}$$

ein kommutatives Diagramm mit exakten Zeilen. Wenn α und γ $\begin{cases}\text{injektiv}\\ \text{surjektiv}\end{cases}$ sind, so auch β.

BEWEIS. α und γ seinen injektiv. Gilt nun $\beta(b) = 1$ für ein $b \in B$, so folgt $1 = \rho\beta(b) = \gamma\lambda(b)$. Da γ injektiv ist, folgt $\lambda(b) = 1$, d.h. $b \in \ker\lambda = \mathrm{bild}\,\kappa$. Daher gibt es ein $a \in A$ mit $\kappa(a) = b$. Hierfür folgt $1 = \beta(b) = \beta\kappa(a)$. Aus der Kommutativität folgt nun $1 = \sigma\alpha(a)$. Da σ injektiv ist (exakte Sequenz!), gilt $\alpha(a) = 1$. Aus der Injektivität von α folgt nun $a = 1$ und damit $b = 1$. Daher ist β injektiv.

Die Surjektivität ist für die Übung. □

DEFINITION 6.5: Es seien N und E zwei Gruppen. Zwei Erweiterungen G und G' von N mit E heißen *äquivalent*, falls es einen Homomorphismus $\phi : G \to G'$ gibt, so daß das folgende Diagramm kommutativ wird:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & E & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & E & \longrightarrow & 1 \end{array}$$

BEMERKUNG 6.6: Äquivalente Erweiterungen G und G' sind stets isomorph. (Die Umkehrung ist i.allg. falsch)

Wie fixieren nun eine Gruppenerweiterung

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} E \longrightarrow 1\cdot$$

$M := \alpha(N) = \operatorname{bild}\alpha = \ker\beta$, $\tau : E \cong G/M \to G$ sei eine *Linksnebenklassenvertreterfunktion* (engl. *transversal*), d.h. wir fixieren in jeder Nebenklasse ein Element. Beachte: τ ist i.allg. *kein* Homomorphismus, es gilt jedoch immer:

$$\beta\tau = \mathrm{id} \tag{6-2}$$

WARNUNG 6.7: In Algebra 1 wurden innere Automorphismen eingeführt. Wir werden hier eine etwas andere Definition verwenden: Es sei G eine Gruppe und $a \in G$ ein Element.

$$\phi_a : G \to G : g \mapsto a^{-1}ga$$

ist ein innerer Automorphismus. Ferner gilt:

$$\phi_a \circ \phi_b(g) := \phi_a(\phi_b(g)) = \phi_{ba}(x)$$

In der Literatur ist es üblich $g^a := \phi_a(g)$ zu setzen. Dann gilt:

$$(g^a)^b = \phi_b \circ \phi_a(g) = \phi_{ab}(g) = g^{ab}.$$

Erinnerung: $I(G) := \{\phi_n | n \in G\} \lhd \mathrm{Aut}(G)$ Falls $N \lhd G$ gilt, setzen wir $\phi_g(n) := g^{-1}ng$, obwohl dies kein innerer Automorphismus ist.

HILFSSATZ 6.8: Sei

$$\lambda : E \to \mathrm{Aut}\, N : \lambda(g)[n] := \alpha^{-1}[(\tau(g))^{-1}\alpha(n)\tau(g)] = \alpha^{-1}\phi_{\tau(g)}\alpha[n]. \tag{6-3}$$

Es sei nun τ' eine weitere Linksnebenklassenvertreterfunktion und λ' analog definiert. Dann gilt für jedes $g \in E$:

$$\lambda(g) = \phi(g)\lambda'(g)$$

mit einem inneren Automorphismus $\phi(g) : N \to N$

BEWEIS. λ ist wohldefiniert, da α injektiv ist und $\alpha(N) \lhd G$ gilt.

Wenn wir in (6-3) τ durch τ' ersetzen, benutzen wir lediglich andere Nebenklassenrepräsentanten: $\tau(g) = \tau'(g)m$ mit $m \in M = \operatorname{bild}\alpha$. α ist injektiv, daher gibt es ein

$m' \in N$ mit $\alpha(m') = m$. Dann gilt:

$$\begin{aligned}
\lambda'(g)[n] &= \alpha^{-1}\phi_{\tau(g)}\alpha[n] \\
&= \alpha^{-1}\phi_{\tau'(g)m}\alpha[n] \\
&= \alpha^{-1}\phi_m\phi_{\tau'(g)}\alpha[n] \\
&= \alpha^{-1}[m^{-1}\phi_{\tau'(g)}[\alpha(n)]m] \\
&= \alpha^{-1}[m^{-1}]\alpha^{-1}\phi_{\tau'(g)}[\alpha(n)]\alpha^{-1}[m] \\
&= \phi_{m'}\alpha^{-1}\phi_{\tau'(g)}\alpha[n]
\end{aligned}$$

□

Satz 6.9: Die Abbildung:

$$\chi : E \to I(N) \setminus \mathrm{Aut}(N) : g \to I(N)\lambda(g)$$

ist ein Gruppenantihomorphismus. Sie ist unabhängig von der Wahl von τ.

Beweis. Die Unabhängigkeit ist klar mit 6.8.

Seien g_1, g_2 in E beliebig. Dann gilt (mit (6-2)): $\tau(g_1)\tau(g_2) = \tau(g_1g_2)m$ mit $m \in M$. Daher folgt:

$$\begin{aligned}
\lambda(g_2)\lambda(g_1)[n] &= \alpha^{-1}\phi_{\tau(g_2)}\alpha\alpha^{-1}\phi_{\tau(g_1)}\alpha[n] \\
&= \alpha^{-1}\phi_{\tau(g_2)}\phi_{\tau(g_1)}\alpha[n] \\
&= \alpha^{-1}\phi_{\tau(g_1)\tau(g_2)}\alpha[n] \\
&= \alpha^{-1}\phi_{\tau(g_1g_2)m}\alpha[n] \\
&= \alpha^{-1}\phi_m\phi_{\tau(g_1g_2)}\alpha[n] \\
&= \phi_m\lambda(g_1g_2)[n] \qquad \text{(6-4)}
\end{aligned}$$

□

Definition 6.10: Es seien E, N Gruppen. Ein Antihomomorphismus

$$\chi : G \to I(N) \setminus \mathrm{Aut}(N)$$

heißt *Paarung* (engl. *coupling*).

Satz 6.11: Äquivalente Gruppenerweiterungen haben die gleiche Paarung.

Beweis. Wir haben das folgende kommutative Diagramm:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & E & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle\theta} & & \| & & \\
1 & \longrightarrow & N & \xrightarrow{\alpha'} & G' & \xrightarrow{\beta'} & E & \longrightarrow & 1
\end{array}$$

Die Paarungen seien χ und χ'. Wenn wir eine Linksnebenklassenvertreterfunktion $\tau : E \to G$ fixieren, so erhalten wir mit $\tau' := \theta\tau$ eine für G' ($\beta'\tau' = \beta'\theta\tau = \beta\tau = \mathrm{id}$).

Damit erhalten wir:

$$\begin{aligned}\lambda(g)[n] &= \alpha^{-1}(\tau(g))^{-1}\alpha(n)\tau(g)\\ &= \alpha^{-1}(\theta^{-1}\tau'(g))^{-1}\alpha(n)\theta^{-1}\tau'(g)\\ &= \alpha^{-1}\theta^{-1}((\tau'(g))^{-1}\theta\alpha(n)\tau'(g))\\ &= \alpha'^{-1}(\tau'(g))^{-1}\alpha'(n)\tau'(n)\\ &= \alpha'\lambda'(g)[n]\end{aligned}$$

□

BEISPIEL 6.12: Es sei $G = NM$ ein (inneres) direktes Produkt. Dann ist G eine Erweiterung von N mit M und umgekehrt.

Es seien N, E beliebige Gruppen und $\alpha : E \to \operatorname{Aut} N$ ein Homomorphismus. $G := N \ltimes_\alpha E := \{(n, e) \in N \times E\}$ mit der Verknüpfung

$$(n_1, e_1)(n_2, e_2) := (\alpha(e_2)[n_1]n_2, e_1e_2).$$

Übung: G ist eine Gruppe, $N \to G : h \mapsto (n, 1)$ und $E \to G : e \mapsto (1, e)$ sind Monomorphismen. Wenn wir N und E mit ihren Bildern in G identifizieren gilt: $N \lhd G$, $E < G$, $N \cap E = \{1\}$, $G = NH$, $1 \to N \to G \to E \to 1$ ist exakt. G heißt *semidirektes Produkt* von N und E.

DEFINITION 6.13: Eine Erweiterung

$$1 \to N \to G \to E \to 1$$

heißt *zerfallend*, wenn es eine Linksnebenklassenvertreterfunktion $\tau : E \to G$ gibt, die gleichzeitig ein Gruppenhomorphismus ist.
Sie heißt *zerfallend mit abelschem Kern*, falls N abelsch ist.
Eine Erweiterung heißt *Zentral*, wenn $N < Z(G)$ gilt.

BEISPIEL 6.14: Semidirekte Produkte sind zerfallende Erweiterungen.

Jede zerfallende Erweiterung ist isomorph zu einem semidirekten Produkt.

Es sei L/K normal, $G := G(L/K)$ sei zerfallend, $G = N \ltimes_\alpha E$. Dann gilt $L = L_1L_2$ mit $L_1 = \operatorname{Fix}(N)$ und $L_2 = \operatorname{Fix}(E)$. $N \lhd G$, d.h. L_1/K ist normal.

$1 \to C_2 \to C_4 \to C_2 \to 1$ ist nicht zerfallend.

Faktorsysteme

Es sei τ eine Linksnebenklassenvertreterfunktion wie in (6-2). *Ab jetzt nehmen wir zusätlich $\tau(1) = 1$ an.* Wir identifizieren N mit $\alpha(N)$ und definieren

$$f : E \times E \to N : (x, y) \mapsto \tau(xy)^{-1}\tau(x)\tau(y)$$

d.h. es gilt

$$\tau(x)\tau(y) = \tau(xy)f(x, y). \tag{6-5}$$

Ferner gilt

$$f(x, 1) = f(1, y) = f(1, 1) = 1. \tag{6-6}$$

Ferner definieren wir $\bar\lambda(x) := \lambda(\tau(x))$.

SATZ 6.15: Für x, y, $z \in E$ gilt:

$$f(xy, z)\bar\lambda(z)[f(x, y)] = f(x, yz)f(y, z) \tag{6-7}$$

BEWEIS. Es gilt

$$\begin{aligned}\tau(xyz) &= \tau(xy)\tau(z)f(xy,z)^{-1} = \tau(x)\tau(y)f(x,y)^{-1}\tau(z)f(xy,z)^{-1}\\ &= \tau(x)\tau(yz)f(x,yz)^{-1} = \tau(x)\tau(y)\tau(z)f(y,z)^{-1}f(x,yz)^{-1}\end{aligned}$$

Und damit

$$f(x,y)^{-1}\tau(z)f(xy,z)^{-1} = \tau(z)f(y,z)^{-1}f(x,yz)^{-1}.$$

Mit Hilfe von λ wie in (6-3) (Beachte: $\alpha = \mathrm{id}$ hier!) folgt dann die Behauptung. □

Mit Hilfe der Funktion f können wir nun (6-4) präzisieren:

$$\bar\lambda(y)\bar\lambda(x) = \phi_{f(x,y)}\bar\lambda(xy) \tag{6-8}$$

DEFINITION 6.16: Ein Paar von Funktionen $f : E\times E \to N$ und $\bar\lambda : E \to \mathrm{Aut}(N)$ mit (6-7), (6-8) und $\bar\lambda(1) = \mathrm{id}$ heißt *Faktorsystem*.

SATZ 6.17: Es seien N und E Gruppen sowie f, λ ein Faktorsystem. Dann gibt es eine Gruppenerweiterung G von N mit E und eine Linksnebenklassenvertreterfunktion τ so, daß (6-5) gilt.

BEWEIS. Wir definieren $G := E \times N$ mit der Operation

$$\circ : (a,x)(b,y) := (ab, f(a,b)\lambda(b)[x]y) \tag{6-9}$$

Zeige: $\circ$ ist assoziativ: Es gilt:

$$\begin{aligned}((a,x)(b,y))(c,z) &= (ab, f(a,b)\lambda(b)[x]y)(c,z)\\ &= (abc, f(ab,c)\lambda(c)[f(a,b)\lambda(b)[x]y]z)\\ &= (abc, f(ab,c)\lambda(c)[f(a,b)]\lambda(c)[\lambda(b)[x]y]z)\\ &\overset{(6\text{-}8)}{=} (abc, f(ab,c)\lambda(c)[f(a,b)]\phi_{f(b,c)}\lambda(bc)[x]\lambda(c)[y]z)\\ &\overset{(6\text{-}7)}{=} (abc, f(a,bc)f(b,c)\phi_{f(b,c)}\lambda(bc)[x]\lambda(c)[y]z)\\ &= (abc, f(a,bc)\lambda(bc)[x]f(b,c)\lambda(c)[y]z). \qquad (6\text{-}10)\end{aligned}$$

Andererseits gilt aber auch:

$$\begin{aligned}(a,x)((b,y)(c,z)) &= (a,x)(bc, f(b,c)\lambda(c)[y]z)\\ &= (abc, f(a,bc)\lambda(bc)[x]f(b,c)\lambda(c)[y]z)\end{aligned}$$

Das Einselement ist $(1,1)$, wegen

$$(a,x)(a^{-1}, (f(a,a^{-1})\lambda(a^{-1})[x])^{-1})$$

$$\begin{aligned}&= (1, f(a,a^{-1})\lambda(a^{-1})[x](f(a,a^{-1})\lambda(a^{-1})[x])^{-1})\\ &= (1,1)\end{aligned}$$

ist $(a^{-1}, (f(a,a^{-1})\lambda(a^{-1})[x])^{-1})$ das Inverse zu (a,x).

Damit ist nun G als Gruppe Nachgewiesen.

Betrachte die Abbildung

$$\psi : G \to E : (a,x) \mapsto a.$$

Nach (6-9) ist dies ein Gruppenepimorphismus. Für $K := \ker \psi$ gilt $K = \{(1,x) \mid x \in E\}$ Wegen $(1,x)(1,y) = (1, f(1,1)\lambda(1)[x]y) = (1,xy)$ ist $(1,x) \mapsto x$ ein Isomorphismus von K auf N. Daher ist

$$1 \to N = K \to G \to E \to 1$$

exakt und G eine Erweiterung.

Eine passende Linksnebenklassenvertreterfunktion erhalten wir so:

$$\tau : E \to G : a \mapsto (a,1).$$

Hierfür gelten nun:

$$\tau(a)\tau(b) \mapsto (a,1)(b,1) = (ab, f(a,b)) = (ab,1)(1,f(a,b)) \mapsfrom \tau(ab)f(a,b)$$

und (mit (6-10)):

$$\begin{aligned}(a,1)^{-1}(1,x)(a,1) &= (a^{-1}, (f(a,a^{-1})\lambda(a^{-1}[1])^{-1})(a, f(1,a)\lambda(a)[x]1) = (a^{-1}, f(a,a^{-1})^{-1})(a,\lambda(a)[x]) \\ &= (1, f(a^{-1},a)\lambda(a)[f(a,a^{-1})^{-1}]\lambda(a)[x]) \\ &= (1, f(a^{-1},a)\lambda(a)[f(a,a^{-1})]^{-1}f(1,a)^{-1}\lambda(a)[x])\end{aligned}$$

mit $x = z = a$, $y = a^{-1}$ folgt aus (6-7):

$$= (1, f(a^{-1},a)f(a^{-1},a)^{-1}f(a,1)^{-1}\lambda(a)[x]) = (a,\lambda(a)[x])$$

□

Definition 6.18: Es seien f, λ und f', λ' zwei Faktorsysteme zu Gruppen N und E. Falls es eine Funktion $h : E \to N$ mit

(6-11) $$\lambda'(a) = \phi_{h(a)}\lambda(a)$$

und

(6-12) $$f'(a,b) = h(ab)^{-1}f(a,b)\lambda(b)[h(a)]h(b)$$

gibt, so heißen die Faktorsysteme assoziiert.

Bemerkung 6.19: Wenn wir die Linksnebenklassenvertreterfunktion wechseln erhalten wir ein assoziiertes Faktorsystem.

Beweis. (6-11) ist bereits in 6.8 gezeigt. Definiere $h := (\tau)^{-1}\tau'$. Dann gilt:

$$\begin{aligned}f'(a,b) &= \tau'(ab)^{-1}\tau'(a)\tau'(b) \\ &= h(ab)^{-1}\tau(ab)^{-1}\tau(a)h(a)\tau(b)h(b) \\ &= h(ab)^{-1}f(a,b)\tau(b)^{-1}h(a)\tau(b)h(b) \\ &= h(ab)^{-1}f(a,b)\lambda(b)[h(a)]h(b)\end{aligned}$$

Beachte ((6-5)): $f(a,b)\tau(b)^{-1} = \tau(ab)^{-1}\tau(a)$. □

Damit folgt, dass äquivalente Gruppenerweiterungen assoziierte Faktorsysteme haben, da wir im Beweis zu 6.11 gesehen haben, dass äquivalente Gruppenerweiterungen sich nur durch ihre Linksnebenklassenvertreterfunktion unterscheiden.

Satz 6.20: Assoziierte Faktorsysteme führen zu äquivalenten Gruppenerweiterungen.

BEWEIS. Es seien assoziierte Faktorsysteme f, λ und f', λ' gegeben. Die damit konstruierten Gruppen sind G und G'. Ferner sei h mit (6-11) und (6-12) gegeben. Wir definieren eine Abbildung $\psi : G \to G' : (a, x) \mapsto (a, h(a)^{-1}x)$. ψ ist offensichtlich eine Bijektion. ψ ist ein Homomorphismus:

$$\begin{aligned} \psi(gh) &= \psi((a,x)(b,y)) = \psi((ab, f(a,b)\lambda(b)[x]y)) \\ &= (ab, h(ab)^{-1}f(a,b)\lambda(b)[x]y). \end{aligned}$$

Andererseits gilt:

$$\begin{aligned} \psi(g)\psi(h) &= (a, h(a)^{-1}x)(b, h(b)^{-1}y) \\ &= (ab, f'(a,b)\lambda'(b)[h(a)^{-1}x]h(b)^{-1}y) \\ &\overset{(6\text{-}11)}{=} (ab, f'(a,b)\phi_{h(b)}\lambda(b)[h(a)^{-1}x]h(b)^{-1}y) \\ &\overset{(6\text{-}12)}{=} (ab, h(ab)^{-1}f(a,b)\lambda(b)[h(a)]h(b)\phi_{h(b)}\lambda(b)[h(a)^{-1}x]h(b)^{-1}y) \\ &= (ab, h(ab)^{-1}f(a,b)\lambda(b)[h(a)]\lambda(b)[h(a)^{-1}x]h(b)h(b)^{-1}y) \\ &= (ab, h(ab)^{-1}f(a,b)\lambda(b)[x]y) \end{aligned}$$

Es bleibt die Kommutativität des Diagramms zu zeigen, d.h. $\psi\alpha = \alpha'$ und $\beta = \beta'\psi$. Es gilt $h(1) = \tau(1)^{-1}\tau'(1)$, damit erhalten wir nun für α:

$$\alpha'(x) = (1, \tau'(1)^{-1}x) = (1, h(1)^{-1}\tau(1)^{-1}x) = \psi((1, \tau(1)^{-1}x) = \psi\alpha(x).$$

Analog für β:

$$\beta((a,x)) = a = \beta'((a,y)) = \psi((a,y'))$$

für beliebiges y und geeignetes y'. □

2. Kohomologie

Um nun weiterführende Aussagen über Gruppenerweiterungen treffen zu können, werden wir uns weiter einschränken. Ab jetzt sei $N =: A$ eine abelsche Gruppe.

Einführung

KOROLLAR 6.21: $\lambda : E \to \operatorname{Aut} A$ ist ein Gruppenantihomorphismus.

BEWEIS. Folge von 6.8, da $I(A) = \{\mathrm{id}\}$ gilt. □

Die Verknüpfung von A werden wir nun additiv schreiben $a+b$. Aus vereinfachungsgründen schreiben wir $ca := \lambda(c)[a]$.

(6-7) vereinfacht sich nun zu

$$f(a,bc) + f(b,c) = f(ab,c) + cf(a,b) \tag{6-13}$$

und (6-8) wird zu:

$$\lambda(a)\lambda(b) = \lambda(ba).$$

HILFSSATZ 6.22: Es sei A eine abelsche Gruppe, E beliebig, ferner sei ein Homomorphismus $\lambda : E \to \operatorname{Aut} A$ fixiert. Die Menge der Faktorsysteme f (mit (6-13) und $f(a,1) = f(1,b) = 0$) bildet eine (abelsche) Gruppe $Z^2(E, A)$ mit der Operation: $(f+g)(a,b) := f(a,b) + g(a,b)$.

BEWEIS. Übung. □

HILFSSATZ 6.23: Es sei $h : E \to A$ eine Abbildung mit $h(1) = 0$. Dann ist $f(a,b) := bh(a) + h(b) - h(ab) =: \delta h \in Z^2(E,A)$, mit $f(a,1) = f(b,1) = 0$. Ferner gilt $\delta(h+k) = \delta(h) + \delta(k)$.

BEWEIS. Übung. □

DEFINITION 6.24: Die Gruppe $B^2(E,A) := \{\delta h \mid h : E \to A, h(1) = 0\}$ heißt Gruppe der *2-Koränder*. Die Elemente von $Z^2(E,A)$ heißen *2-Kozykel*.
Die Gruppe $H^2(E,A) := Z^2(E,A)/B^2(E,A)$ ist die *2. Kohomologie Gruppe (von E mit Koeffizienten in A)*.

WARNUNG 6.25: Z, B und H hängen von λ ab!

SATZ 6.26: Es gibt eine Bijektion zwischen Gruppenerweiterungen (modulo Äquivalenz) und Elementen von $H^2(E,A)$.

BEWEIS. Übung. □

BEISPIEL 6.27: Es sei $\lambda : C_2 \to \mathrm{Aut}(C_2) : a \mapsto \mathrm{id}$, $H^2(C_2, C_2) = C_2$:

Gruppenringe und Moduln

In der Algebra 1 sind Gruppenringe eingeführt worden. Wir Setzen $R := \mathbb{Z}[E] = \{\sum_{\text{fin.}} x_a a \mid a \in E, x_a \in \mathbb{Z}\}$.

BEMERKUNG 6.28: Mit $\circ : R \times A \to A : (r,a) \mapsto \lambda(r)[a]$ ist A ein R-Modul.

BEISPIEL 6.29: Es sei G eine Gruppe, $R := \mathbb{Z}G$. Wir setzen $X_n := \{[x_1, \dots, x_n] \mid x_i \in G \setminus \{1\}\}$ und $\Lambda_n := RX_n$ der von X_n frei erzeugte R-Modul. Zusätzlich setzen wir $X_0 := \{[\,]\}$ und $\Lambda_0 := R$. Ferner vereinbaren wir, daß für jedes $x := [x_1, \dots, x_n] \in G^n \setminus X_n$ (d.h. min. ein $x_i = 1$) $x = 0$ in Λ_n gelten soll.

Jetzt ist $d_0 : \Lambda_0 \to \mathbb{Z} : \sum r_x x \mapsto \sum r_x$ ein R-Modulepimorphismus und (5-1) ist exakt bei $\mathbb{Z}$. Für $n > 0$ definieren wir:

$$\begin{aligned} d_n([x_1, \dots, x_n]) \;:=\; & x_1[x_2, \dots, x_n] \\ & + \sum_{i=1}^{n-1} (-1)^i [x_1, \dots, x_i x_{i+1}, \dots, x_n] \\ & + (-1)^n [x_1, \dots, x_{n-1}] \end{aligned}$$

Per linearer Fortsetzung erhalten wir $d_n : \Lambda_n \to \Lambda_{n-1}$. Um nun die Exaktheit von (5-1) an den anderen Stellen nachzuweisen, definieren wir noch eine weitere Familie von Abbildungen:

$$s_{-1} : \mathbb{Z} \to \Lambda_0 : n \mapsto n[\,]$$

und

$$s_n : \Lambda_n \to \Lambda_{n+1} : x[x_1, \dots, x_n] \mapsto [x, x_1, \dots, x_n].$$

Wir zeigen: $d_0 s_{-1} = \mathrm{id}$ (offensichtlich) und

$$d_{n+1} s_n + s_{n-1} d_n = \mathrm{id}\,. \tag{6-14}$$

(Damit gilt dann $\ker d_n \subseteq \operatorname{bild} d_{n+1}$)

$$\begin{aligned} x[x_1,\dots,x_n] &\overset{s_n}{\mapsto} [x,x_1,\dots,x_n] \\ &\overset{d_{n+1}}{\mapsto} x[x_1,\dots,x_n] - [xx_1,\dots,x_n] \\ &\quad + \sum_{j=1}^{n-1}(-1)^{j-1}[x,x_1,\dots,x_jx_{j+1},\dots,x_n] \\ &\quad +(-1)^{n+1}[x,x_1,\dots,x_{n-1}] \end{aligned}$$

und

$$\begin{aligned} &\overset{d_n}{\mapsto} xx_1[x_2,\dots,x_n] \\ &\quad + \sum_{j=1}^{n-1} x(-1)^j[x_1,\dots,x_jx_{j+1},\dots,x_n] \\ &\quad +x(-1)^n[x_1,\dots,x_{n-1}] \\ &\overset{s_{n-1}}{\mapsto} [xx_1,x_2,\dots,x_n] \\ &\quad + \sum_{j=1}^{n-1}(-1)^j[x,x_1,x_jx_{j+1},\dots,x_n] \\ &\quad +(-1)^n[x,x_1,\dots,x_n] \end{aligned}$$

Durch Vergleich der Vorzeichen folgt nun $\mathrm{id} = d_{n+1}s_n + s_{n-1}d_n$. Durch Multiplizieren von (6-14) von links mit d_n erhalten wir

$$d_n = d_nd_{n+1}s_n + d_ns_{n-1}d_n. \tag{6-15}$$

Wir zeigen per Induktion: $d_nd_{n+1} = 0$: Für $n = 0$ folgt $d_0 = d_0d_1s_0 + d_0s_{-1}d_0 = d_0d_1s_0 + d_0$ und daher $d_0d_1s_0 = 0$. Da $X_1 \subseteq \operatorname{bild} s_0$ gilt ($[x] = s_0(x[])$), folgt $d_0d_1 = 0$.

Multiplikation von (6-14) von rechts mit d_{n+1}: $d_{n+1} = d_{n+1}s_nd_{n+1} + s_{n-1}d_nd_{n+1}$ Nach Induktionsvoraussetzung gilt $d_nd_{n+1} = 0$ und daher $d_{n+1} = d_{n+1}s_nd_{n+1}$. Wenn wir dies mit (6-15) (für $n := n+1$) vergleichen folgt: $d_{n+1}s_nd_{n+1} = d_{n+1} = d_{n+1}d_{n+2}s_{n+1} + d_{n+1}s_nd_{n+1}$. Und $0 = d_{n+1}d_{n+2}s_{n+1}$. Da $X_{n+1} \subseteq \operatorname{bild} s_n$ gilt, folgt $d_{n+1}d_{n+2} = 0$. $\Rightarrow$: $\operatorname{bild} d_{n+1} \subseteq \ker d_n$, $\Rightarrow$: $\operatorname{bild} d_{n+1} = \ker d_n$ und (5-1) ist exakt.

Dies zeigt, daß freie Auflösungen immer existieren. Die so erhaltene Auflösung heißt auch *kanonische Auflösung* (*standard Auflösung*).

Definition 6.30: Es sei G eine Gruppe, A ein $\mathbb{Z}G$-Modul und M_i eine freie Auflösung. Die *n-te Kohomologiegruppe von G mit Koeffizienten in A* ist definiert als

$$H^n(G,A) := \ker d_{n+1}^* / \operatorname{bild} d_n^*.$$

Bemerkung 6.31: Wir haben die folgende exakte Sequenz:

$$0 = H^0(G,A) \to H^1(G,A) \to \cdots \to H^n(G,A) \to \cdots.$$

Beweis: Übung.

Satz 6.32: Die Kohomologiegruppen sind unabhängig von der gewählten Auflösung.

BEWEIS. Durch Anwenden von 5.57.(1) auf M und M' bzw. M' und M erhalten wir folgendes kommutative Diagramm:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & \searrow{\scriptstyle g_2f_2} & \downarrow{\scriptstyle f_1} & \searrow{\scriptstyle g_1f_1} & \downarrow{\scriptstyle f_0} & \searrow{\scriptstyle g_0f_0} & & & \\
\cdots & \longrightarrow & M_2' & \longrightarrow & M_1' & \longrightarrow & M_0' & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_0} & & & & \\
\cdots & \longrightarrow & M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Offensichtlich ist

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\cdots & \longrightarrow & M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

ebenfalls kommutativ. Nach 5.57.(2) existieren daher $h_i : M_i \to M_{i+1}$ mit

$$g_i f_i - 1 = d_{i+1}h_i + h_{i-1}d_i$$

($h_{-1} := 0$). Indem wir nun $\mathrm{Hom}(., M)$ anwenden erhalten wir ein neues kommutatives Diagramm:

$$\begin{array}{ccccc}
\mathrm{Hom}(M_{i+1}, M) & \xleftarrow{d_{i+1}^*} & \mathrm{Hom}(M_i, M) & \xleftarrow{d_i*} & \\
\downarrow{\scriptstyle g_{i+1}^*} & & \downarrow{\scriptstyle g_i^*} & & \\
\mathrm{Hom}(M_{i+1}', M) & \xleftarrow{(d_{i+1}')^*} & \mathrm{Hom}(M_i', M) & \xleftarrow{(d_i')^*} &
\end{array}$$

Damit: $g_i^* \ker d_{i+1}^* \subseteq \ker(d_{i+1}')^*$ und $g_i^* \operatorname{bild} d_i^* \subseteq \operatorname{bild}(d_i')^*$. $\Rightarrow$ wir können g_i^* als Abbildung von

$$g_i^* : \ker d_{i+1}^* / \operatorname{bild} d_i^* \to \ker(d_{i+1}')^* / \operatorname{bild}(d_i')^*$$

auffassen. Analog erhalten wir:

$$f_i^* : \ker(d_{i+1}')^* / \operatorname{bild}(d_i')^* \to \ker d_{i+1}^* / \operatorname{bild} d_i^*.$$

Aus der Homotopie von $(gf)_i$ und $(\mathrm{id})_i$ erhalten wir:

$$f_i^* g_i^* - \mathrm{id} = h_i^* d_{i+1}^* + d_i^* h_i^*$$

Und damit für $x \in \ker d_{i+1}^*$:

$$f_i^* g_i^*(x) - x = h_i^* d_{i+1}^*(x) + d_i^* h_i^*(x) \in 0 + \operatorname{bild} d_i^*$$

Also ist $f_i^* g_i^* = \mathrm{id}$ auf $\ker d_{i+1}^* / \operatorname{bild} d_i^* = H^i$ und $g_i^* f_i^* = \mathrm{id}$ auf $\ker {d_{i+1}'}^* / \operatorname{bild} {d_i'}^* = H'^i$ □

BEISPIEL 6.33: Wenn wir die standard Auflösung aus 6.29 nehmen, sehen wir

$$\mathrm{Hom}(\Lambda_n, A) \cong C^n(G, A) =: \{f : G^n \to A \mid f(x_1, \ldots, x_n) = 0 \text{ falls } x_i = 1\},$$

$\delta_n := d_n^*$. (Achtung: die f's sind keine Homomorphismen!)

Die Elemente von $C^n(G, A)$ heißen normalisierte Koketten. $Z^n(G, A) := \ker \delta_n$ sind die Kozykel, $B^n(G, A) := \operatorname{bild} \delta_{n-1}$ die Koränder.

$n = 1$: $(\delta_1 f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1)$ Damit:

$$\ker \delta_1 = \{f \mid f(xy) = xf(y) + f(x)\} \tag{6-16}$$

Diese Elemente heißen gekreuzte Homomorphismen.

$$(\delta_0 f)(x_1) = x_1 f - f. \tag{6-17}$$

Elemente aus $\operatorname{bild} \delta_0$ heißen zerfallend.

$n = 2$: $(\delta_2 f)(x_1, x_2, x_3) = x_1 f(x_2, x_3) - f(x_1 x_2, x_3) + f(x_1, x_2 x_3) - f(x_1, x_2)$. Also entsprehen Elemente aus $\ker \delta_2$ genau den Faktorsystemen. $\operatorname{bild} \delta_1$ entspricht der Bedingung für äquivalente Faktorsysteme.

Beispiel 6.34: Es sei $G := \langle g \rangle$ eine endliche zyklische Gruppe und $R := \mathbb{Z}G$. Wir definieren $M_n := R$ und $d_{2n}(x) := (1 - g)x =: Tx$, $d_{2n+1}(x) := \sum_{a \in G} ax =: Nx$. Es gilt $\ker N = \operatorname{bild} T$ und $\ker N = \operatorname{bild} T$. Also ist

$$M \xrightarrow{N} M \xrightarrow{T} \cdots \xrightarrow{N} M \xrightarrow{T} M \longrightarrow \mathbb{Z} \to 0$$

eine freie Auflösung von R. Wir erhalten: $\ker T^* = \{x \in M \mid gx = x\}$. Ferner gilt $H^{2n} = H^2$ und $H^{2n+1} = H^1$.

Satz 6.35 (Hilbert 90): Es sei K/k normal mit $G := G(K/k)$. Dann gelten

$$H^1(G, K^\times) = 1, \quad H^1(K, K^+) = 0.$$

Für $G = \langle g \rangle$ zyklisch folgt damit auch $x \in K$ hat $\mathrm{N}_{K/k}(x) = 1 \iff x = y/gy$ und $x \in K$ hat $\mathrm{Tr}_{K/k}(x) = 0 \iff x = y - gy$.

Beweis. Zu zeigen: $B^1 = Z^1$. Sei also $f \in Z^1(G, K^\times)$ beliebig gegeben, d.h. $f : G \to K^\times$, also $f(\sigma) \neq 0 \ \forall \sigma \in G$. Nach Unabhängigkeit der Automorphismen Algebra 1, 4.1 existiert ein $\beta \in K^\times$ mit

$$\alpha := \sum_{\tau \in G} f(\tau)\tau(\beta) \neq 0$$

Hierfür gilt nun:

$$\begin{aligned} \sigma(\alpha) &= \sum_{\tau \in G} \sigma f(\tau)\sigma\tau(\beta) \\ &\overset{(6\text{-}16)}{=} \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(\beta) \\ &= f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau(\beta) = f(\sigma)^{-1}\alpha \end{aligned}$$

Also $f(\sigma) = \alpha/\sigma(\alpha)$ also (nach (6-17)) $f \in B^1$.

Für zyklische Körper folgt aus 6.34:

$$H^1(G, K^\times) = \{x \in K^\times \mid \mathrm{N}(x) = 1\}/\{x/gx \mid x \in K^\times\} = 1$$

K^+: Übung. □

SATZ 6.36: Es sei

$$0 \to A \to B \to C \to 0$$

eine exakte Sequenz von $\mathbb{Z}G$-Moduln. Dann gibt es *Verbindungshomomorphismen* $\delta_i : H^i(G, C) \to H^{i+1}(G, A)$ so, daß

$$0 \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots$$

exakt ist.

BEWEIS. Fehlt □

KAPITEL 7

Gitter

1. Grundlagen

DEFINITION 7.1: Seien $b_1, \dots, b_k \in \mathbb{R}^n$ linear unabhängig über $\mathbb{R}$. Dann nennt man den $\mathbb{Z}$–Modul

$$\Lambda := \left\{ \sum_{i=1}^{k} \lambda_i b_i \;\mid\; \lambda_1, \dots, \lambda_k \in \mathbb{Z} \right\}$$

ein Gitter der Dimension k. $d(\Lambda) := \det(b_i^t \cdot b_j)_{1 \le i,j \le k}^{1/2}$ heißt Gitterdiskriminante von Λ, und

$$\Pi(\Lambda) := \left\{ x \in \mathbb{R}^n \;\mid\; x = \sum_{i=1}^{k} \xi b_i, 0 \le \xi_i < 1 \; (1 \le i \le k) \right\}$$

bezeichnet man als das Fundamentalparallelotop (Grundmasche) von Λ. $\Lambda' \subseteq \Lambda$ heißt Teilgitter von Λ, sofern Λ' selbst ein Gitter im $\mathbb{R}^n$ ist.

Im folgenden sei Λ ein k–dimensionales Gitter im $\mathbb{R}^n$ mit $\mathbb{Z}$–Basis $b_1, \dots, b_k \in \mathbb{R}^n$.

HILFSSATZ 7.2:

(1) $d(\Lambda) = \mathrm{Vol}_k(\Pi(\Lambda))$.

(2) Ist Λ' ein k–dimensionales Teilgitter von Λ mit einer Gitterbasis $c_1, \dots, c_k$, so gilt

$$d(\Lambda') = |\det(U)| \cdot d(\Lambda)$$

für $U \in \mathbb{Z}^{k \times k}$ mit $(c_1, \dots, c_k) = (b_1, \dots, b_k) \cdot U$.

BEWEIS. (1) Definiere $f : \mathbb{R}^k \to \mathbb{R}^n$ mittels $f(e_i) = b_i$ $(1 \le i \le k)$ und linearer Fortsetzung $\Rightarrow$ $(\mathbb{R}^k, [0,1]^k, f)$ ist eine Parameterdarstellung des k–dimensionalen Flächenstückes $\overline{\Pi(\Lambda)}$ $\Rightarrow$

$$\begin{aligned} \mathrm{Vol}_k(\overline{\Pi(\Lambda)}) &= \int_{[0,1]^k} \det(J_f^t \cdot J_f)^{1/2} \, dm_k \\ &= \int_{[0,1]^k} \det(b_i^t \cdot b_j)_{1 \le i,j \le k}^{1/2} \, dm_k = d(\Lambda). \end{aligned}$$

(2) Trivial.

□

HILFSSATZ 7.3: Ist Λ' ein k–dimensionales Teilgitter von Λ, so gilt

$$(\Lambda : \Lambda') = \frac{d(\Lambda')}{d(\Lambda)} \; .$$

BEWEIS. Sei $c_1, \dots, c_k$ eine $\mathbb{Z}$–Basis von Λ'. Nach Satz 5.41 können wir annehmen, daß die Transformationsmatrix $U = (u_{ij}) \in \mathbb{Z}^{k\times k}$ mit $(c_1, \dots, c_k) = (b_1, \dots, b_k) \cdot U$ eine untere Dreiecksmatrix ist. Da

$$\mathcal{V} := \{\sum_{i=1}^{k} m_i b_i + \Lambda' \mid 0 \le m_i < u_{ii}, m_i \in \mathbb{Z}\ (1 \le i \le k)\}$$

ein komplettes Vertretersystem von Λ/Λ' ist, folgt $\#\mathcal{V} = (\Lambda : \Lambda')$. Andererseits gilt nach Hilfssatz 7.2

$$\frac{d(\Lambda')}{d(\Lambda)} = |\det(U)| = \prod_{i=1}^{k} u_{ii} = \#\mathcal{V}.$$

□

ALGORITHMUS 7.4 (Quadratische Ergänzung): Zu $A \in \mathbb{R}^{k\times k}$ positiv definit berechnen wir eine obere Dreiecksmatrix $Q \in \mathbb{R}^{k\times k}$, so daß

$$x^t \cdot A \cdot x = \sum_{i=1}^{k} q_{ii} \left(x_i + \sum_{j=i+1}^{k} q_{ij} x_j \right)^2 .$$

(1) (Initialisierung) Setze $Q \leftarrow A$.
(2) Für $i = 1, \dots, k-1$ setze $q_{ji} \leftarrow q_{ij}, q_{ij} \leftarrow \frac{q_{ij}}{q_{ii}}$ $(i+1 \le j \le k)$ und weiter $q_{\mu\nu} \leftarrow q_{\mu\nu} - q_{\mu i} q_{i\nu}$ $(i+1 \le \mu \le \nu \le k)$.
(3) Setze $q_{ij} \leftarrow 0$ $(1 \le j < i \le k)$.

Sei $A \in \mathbb{R}^{k\times k}$ positiv definit mit zugehöriger quadratischer Form $f(x) = x^t \cdot A \cdot x$. Quadratische Ergänzung liefert dann

$$\begin{aligned} f(x) &= \sum_{i=1}^{k} q_{ii}(x_i + \sum_{j=i+1}^{k} q_{ij} x_j)^2 \\ &= q_{11}(x_1 + q_{12}x_2 + \cdots + q_{1k}x_k)^2 + \underbrace{\sum_{i=2}^{k} q_{ii} \left(x_i + \sum_{j=i+1}^{k} q_{ij} x_j \right)^2}_{=:g(x)} \end{aligned}$$

Betrachte nun die lineare Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ mit zugehöriger Matrix

$$U = \begin{pmatrix} 1 & -q_{12} & \dots & -q_{1n} \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}.$$

Offensichtlich gilt $\det(U) = 1$ und weiter

$$f(Ux) = q_{11}x_1^2 + g(x) = x^t(U^t \cdot A \cdot U)x.$$

g läßt sich als quadratische Form in $k-1$ Variablen (eben $x_2, \dots, x_k$) auffassen. Ist dann $B \in \mathbb{R}^{(k-1)\times(k-1)}$ die zugehörige Matrix, so gilt

$$\det(A) = \det(U^t \cdot A \cdot U) = \det \left(\begin{array}{c|ccc} q_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array} \right) = q_{11} \det(B).$$

Induktiv folgt daraus $\det(A) = \prod_{i=1}^{k} q_{ii}$.

ALGORITHMUS 7.5 (Auszählalgorithmus): Zu $A \in \mathbb{R}^{k\times k}$ und $C > 0$ bestimmen wir alle $x \in \mathbb{Z}^k$ mit $x^t \cdot A \cdot x \leq C$.

(1) Bestimme $Q \in \mathbb{R}^{k\times k}$ wie in Algorithmus 7.4.
(2) (Initialisierung) Setze $i \leftarrow k, T_i \leftarrow C, U_i \leftarrow 0$.
(3) (Schranken für x_i) Setze $Z \leftarrow \sqrt{\frac{T_i}{q_{ii}}}$, $B_i \leftarrow \lfloor Z - U_i \rfloor$ und weiter $x_i \leftarrow \lceil -Z - U_i \rceil - 1$.
(4) Setze $x_i \leftarrow x_i + 1$. Falls $x_i \leq B_i$, so gehe zu Schritt 6.
(5) Setze $i \leftarrow i + 1$ und gehe zu Schritt 4.
(6) Falls $i = 1$, so gehe zu Schritt 7, sonst setze $i \leftarrow i - 1, U_i \leftarrow \sum_{j=i+1}^{k} q_{ij}x_j, T_i \leftarrow T_{i+1} - q_{i+1,i+1}(x_{i+1} + U_{i+1})^2$ und gehe zu 2.
(7) Falls $x = 0$, so terminiere, sonst gebe x sowie $-x$ aus und gehe zu Schritt 4.

SATZ 7.6 (Diskretheit von Gittern): Zu $x \in \mathbb{R}^n$ und $C > 0$ gibt es nur endlich viele $y \in \Lambda$ mit $\|x - y\| \leq C$.

BEWEIS. Konsequenz aus dem Auszählalgorithmus. □

KOROLLAR 7.7: Es existiert $\delta > 0$ mit $\|x - y\| > \delta \; \forall \, x, y \in \Lambda, x \neq y$.

BEWEIS. Angenommen für alle $n \in \mathbb{N}$ existieren $x_n, y_n \in \Lambda, x_n \neq y_n$, mit $\|x_n - y_n\| \leq \frac{1}{n} \Rightarrow \#\{z \in \Lambda \mid \|z\| \leq 1\} = \infty \Rightarrow$ Widerspruch zu Satz 7.6. □

KOROLLAR 7.8: Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge in Λ. Konvergiert $(x_n)_{n\in\mathbb{N}}$ gegen $x \in \mathbb{R}^n$, so gilt $x \in \Lambda$.

BEWEIS. Λ ist nach Korollar 7.7 abgeschlossen in $\mathbb{R}^n$. □

SATZ 7.9: Sei $k = n$. Ist $C \subseteq \mathbb{R}^n$ konvex und ursprungssymmetrisch, so enthält C einen nicht–trivialen Gitterpunkt, falls eine der beiden folgenden Bedingungen erfüllt ist:
(1) $\mathrm{Vol}(C) > 2^n d(\Lambda)$.
(2) $\mathrm{Vol}(C) \geq 2^n d(\Lambda)$ und C kompakt.

BEWEIS. (1) Für das Fundamentalparallelotop $\Pi(\Lambda)$ gilt

$$\mathbb{R}^n = \bigcup_{y\in\Lambda} \Pi(\Lambda) + y.$$

Damit folgt

$$\frac{1}{2}C = \frac{1}{2}C \cap \mathbb{R}^n = \bigcup_{y\in\Lambda} \left(\frac{1}{2}C \cap (y + \Pi(\Lambda))\right)$$

und weiter

$$\begin{aligned}
\mathrm{Vol}(\Pi(\Lambda)) &= d(\Lambda) < \frac{1}{2^n}\,\mathrm{Vol}(C) = \mathrm{Vol}(\frac{1}{2}C) \\
&= \mathrm{Vol}\left(\bigcup_{y\in\Lambda} \left(\frac{1}{2}C \cap (y + \Pi(\Lambda))\right)\right) \\
&= \sum_{y\in\Lambda} \mathrm{Vol}\left(\frac{1}{2}C \cap (y + \Pi(\Lambda)\right) \\
&= \sum_{y\in\Lambda} \mathrm{Vol}\left(\left(\frac{1}{2}C - y\right) \cap \Pi(\Lambda)\right).
\end{aligned}$$

Angenommen $(\frac{1}{2}C - u) \cap (\frac{1}{2}C - v) = \emptyset \; \forall \, u, v \in \Lambda, u \neq v \Rightarrow$

$$\begin{aligned} \sum_{y \in \Lambda} \mathrm{Vol}\left(\left(\frac{1}{2}C - y\right) \cap \Pi(\Lambda)\right) &= \mathrm{Vol}\left(\left(\bigcup_{y \in \Lambda}\left(\frac{1}{2}C - y\right)\right) \cap \Pi(\Lambda)\right) \\ &\leq \mathrm{Vol}(\Pi(\Lambda)) \end{aligned}$$

$\Rightarrow$ Widerspruch. Also existieren $y, z \in \Lambda, y \neq z$, mit $(\frac{1}{2}C - y) \cap (\frac{1}{2}C - z) \neq \emptyset$. Für $c_1, c_2 \in C$ mit $\frac{1}{2}c_1 - y = \frac{1}{2}c_2 - z$ folgt dann

$$0 \neq y - z = \frac{1}{2}c_1 - \frac{1}{2}c_2 = \frac{1}{2}c_1 + \frac{1}{2}(-c_2) \; \in C.$$

(2) Wähle zunächst eine monotone Nullfolge $(e_n)_{n \in \mathbb{N}}$ in $\mathbb{R}^{>0}$ und bilde

$$C_n := (1 + e_n)C \qquad (n \in \mathbb{N}).$$

C_n ist offensichtlich für jedes $n \in \mathbb{N}$ konvex sowie ursprungssymmetrisch, und es gilt $\mathrm{Vol}(C_n) > 2^n d(\Lambda)$. Zu jedem $n \in \mathbb{N}$ existiert nach (a) also $x_n \in C_n \cap \Lambda \setminus \{0\}$. Da C_1 kompakt ist, besitzt $(x_n)_{n \in \mathbb{N}}$ eine konvergente Teilfolge $(x_{n_j})_{j \in \mathbb{N}}$ mit $x := \lim_{j \to \infty} x_{n_j} \; \in C \Rightarrow x \in \Lambda$ nach Korollar 7.8.

□

2. Sukzessive Minima

Definition 7.10: Für $i \in \{1, \ldots, k\}$ heißt

$M_i := \min\{\gamma > 0 \mid \exists x_1, \ldots, x_i \in \Lambda \;$ linear unabhängig mit $\|x_\nu\|^2 \leq \gamma \; (1 \leq \nu \leq i)\}$.

das i–te sukzessives Minimum.

Hilfssatz 7.11:

(1) Es existieren $y_1, \ldots, y_k \in \Lambda$ linear unabhängig mit $\|y_i\|^2 = M_i \; (1 \leq i \leq k)$.
(2) $v \in \Lambda$ mit $\|v\|^2 = M_1$ läßt sich zu einer Basis von Λ ergänzen.

Beweis. (1) Trivialerweise existiert $y_1 \in \Lambda$ mit $\|y_1\|^2 = M_1$. Sind nun $y_1, \ldots, y_{j-1} \in \Lambda$ gefunden mit $\|y_i\|^2 = M_i \; (1 \leq i < j)$, so existieren nach Definition $x_1, \ldots, x_j \in \Lambda$ linear unabhängig mit $\|x_i\|^2 \leq M_j \; (1 \leq i \leq j)$. Insbesondere existiert $m \in \{1, \ldots, j\}$, so daß $y_1, \ldots, y_{j-1}, x_m$ linear unabhängig sind. O.B.d.A. $m = j$ und $M_1 < M_j$. Angenommen $\|x_j\|^2 < M_j$. Gilt dann

$$M_{j-r-1} < M_{j-r} = \ldots = M_j$$

für ein $r \in \{0, \ldots, j-2\}$, so sind $y_1, \ldots, y_{j-r-1}, x_j$ linear unabhängig im Widerspruch zur Definition von M_{j-r}. Also folgt $\|x_j\|^2 = M_j$.

(2) Konsequenz aus Satz 5.18.

□

Satz 7.12: Es existiert eine nur von k abhängige Konstante $\gamma_k \in \mathbb{R}$ (Hermitesche–Konstante), welche

$$M_1^k \leq \gamma_k^k d(\Lambda)^2$$

leistet und minimal mit dieser Eigenschaft ist.

BEWEIS. Wir zeigen $M_1^k \leq C_k d(\Lambda)^2$ für

$$C_k := \frac{4}{3}^{\frac{1}{2}k(k-1)}.$$

Der Induktionsanfang ($k = 1$) ist trivial. Sei also nun $k > 1$. Nach Hilfssatz 7.11 können wir $\|b_1\|^2 = M_1$ annehmen. Bilde

$$f(x) = \sum_{i,j=1}^{k} x_i x_j b_i^t b_j \qquad (x = \sum_{\nu=1}^{k} x_\nu b_\nu).$$

Dann gilt

$$f(x) = M_1(x_1 + \sum_{j=2}^{k} q_{1j} x_j)^2 + g(x_2, \ldots, x_k)$$

mit $\det(A) = d(\Lambda)^2$ und

$$\det(B) = \frac{d(\Lambda)^2}{M_1},$$

sofern A bzw. B die zugehörigen Matrizen zu den quadratischen Formen f bzw. g sind. Seien nun $y_2, \ldots, y_k \in \mathbb{Z}$ mit

$$g(y_2, \ldots, y_k) = \min\{g(x_2, \ldots, x_k) \mid x_2, \ldots, x_k \in \mathbb{Z}, |x_2| + \cdots + |x_k| > 0\}.$$

Nach Induktionsannahme folgt

$$g(y_2, \ldots, y_n)^{k-1} \leq C_{k-1} \frac{d(\Lambda)^2}{M_1}.$$

Wähle $y_1 \in \mathbb{Z}$ mit

$$\left| y_1 + \sum_{j=2}^{k} q_{1j} y_j \right| \leq \frac{1}{2}.$$

Für $y := y_1 b_1 + \cdots + y_k b_k \in \Lambda \setminus \{0\}$ folgt dann

$$M_1 \leq f(y) \leq \frac{1}{4} M_1 + \left(C_{k-1} \frac{d(\Lambda)^2}{M_1} \right)^{\frac{1}{k-1}}.$$

Damit

$$M_1 \leq \frac{4}{3} \left(C_{k-1} \frac{d(\Lambda)^2}{M_1} \right)^{\frac{1}{k-1}},$$

und weiter

$$\begin{aligned} M_1^k &\leq \left(\frac{4}{3}\right)^{k-1} C_{k-1} d(\Lambda)^2 = \left(\frac{4}{3}\right)^{k-1} \left(\frac{4}{3}\right)^{\frac{1}{2}(k-2)(k-1)} d(\Lambda)^2 \\ &= \left(\frac{4}{3}\right)^{\frac{1}{2}k(k-1)} d(\Lambda)^2 = C_k d(\Lambda)^2. \end{aligned}$$

□

SATZ 7.13: Es gilt $M_1 \cdot \ldots \cdot M_k \leq \gamma_k^k d(\Lambda)^2$.

BEWEIS. Seien $y_1, \dots, y_k \in \Lambda$ linear unabhängig mit $\|y_i\|^2 = M_i$ $(1 \le i \le k)$. Ferner sei $Q \in \mathbb{Q}^{k\times k}$ mit

$$(b_1, \dots, b_k) = (y_1, \dots, y_k) \cdot Q.$$

Bilde $Y := (y_i^t y_j)_{1\le i,j\le k}$ sowie $B := (b_i^t b_j)_{1\le i,j\le k}$. Für $x \in \Lambda$ mit

$$x = \sum_{i=1}^{k} x_{b_i} b_i = \sum_{i=1}^{k} x_{y_i} y_i \qquad (x_{b_1}, \dots, x_{b_k} \in \mathbb{Z}, y_{b_1}, \dots, y_{b_k} \in \mathbb{Q})$$

gilt dann

$$\begin{aligned} \|x\|^2 &= (x_{b_1}, \dots, x_{b_k}) \cdot B \cdot (x_{b_1}, \dots, x_{b_k})^t \\ &= (x_{b_1}, \dots, x_{b_k}) \cdot Q^t \cdot Y \cdot Q \cdot (x_{b_1}, \dots, x_{b_k})^t \\ &= (x_{y_1}, \dots, x_{y_k}) \cdot Y \cdot (x_{y_1}, \dots, x_{y_k})^t. \end{aligned}$$

Sei f die zu Y gehörige quadratische Form. Quadratische Ergänzung liefert dann

$$\begin{aligned} (z_1, \dots, z_k) \cdot Y \cdot (z_1, \dots, z_k)^t &= f(z_1, \dots, z_k) \\ &= \sum_{i=1}^{k} \underbrace{q_{ii} \left(z_i + \sum_{j=i+1}^{k} q_{ij} z_j \right)^2}_{=:g_i(z_i, \dots, z_k)}. \end{aligned}$$

Damit bildet man eine neue quadratische Form

$$h(z_1, \dots, z_k) := \sum_{i=1}^{k} \frac{1}{M_i} g_i(z_i, \dots, z_k).$$

Ist C die zugehörige Matrix von h, so gilt

$$\det(Q^t \cdot C \cdot Q) = \det(Q)^2 \cdot \det(C) = \det(Q)^2 \frac{\det(Y)}{M_1 \cdot \ldots \cdot M_k} = \frac{d(\Lambda)^2}{M_1 \cdot \ldots \cdot M_k}.$$

Also erhält man aus Satz 7.12

$$\min\{(z_1, \dots, z_k) \cdot Q^t \cdot C \cdot Q \cdot (z_1, \dots, z_k)^t \mid z_1, \dots, z_k \in \mathbb{Z}, |z_1| + \cdots + |z_k| > 0\}^k$$

$$\le \gamma_k^k \frac{d(\Lambda)^2}{M_1 \cdot \ldots \cdot M_k}.$$

Sei nun $x \in \Lambda \setminus \{0\}$ beliebig. Ferner sei m maximal mit $x_{y_m} \ne 0 \Rightarrow$

$$\begin{aligned} &(x_{b_1}, \dots, x_{b_k}) \cdot Q^t \cdot C \cdot Q \cdot (x_{b_1}, \dots, x_{b_k})^t \\ &= h(x_{y_1}, \dots, x_{y_k}) \\ &= \sum_{i=1}^{m} \frac{1}{M_i} g_i(x_{y_i}, \dots, x_{y_k}) \ge \frac{1}{M_m} \sum_{i=1}^{m} g_i(x_{y_i}, \dots, x_{y_k}) \\ &= \frac{1}{M_m} f(x_{y_1}, \dots, x_{y_k}) = \frac{1}{M_m} \|x\|^2 \ge 1, \end{aligned}$$

denn x ist linear unabhängig von $y_1, \dots, y_{m-1}$, daher $\|x\|^2 \ge M_m$. □

Zu $b_1, \dots, b_k$ sei nun $b_1^*, \dots, b_k^* \in \mathbb{R}^n$ die Orthogonalbasis von $\mathbb{R} \cdot b_1 + \cdots + \mathbb{R} \cdot b_n$, welche man mit dem Verfahren von E. Schmidt berechnet, also

$$b_i^* := b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \qquad (1 \le i \le k),$$

$$\mu_{ij} := \frac{b_i^t b_j^*}{b_j^{*t} b_j^*} \qquad (1 \le j < i \le k).$$

SATZ 7.14 (Hadamard): Es gilt

$$d(\Lambda) \le \prod_{i=1}^{k} \|b_i\|.$$

BEWEIS. Nach Konstruktion gilt

$$(b_1^*, \ldots, b_k^*) = (b_1, \ldots, b_k) \cdot Q$$

für $Q \in \mathbb{R}^{k\times k}$ mit $\det(Q) = 1 \Rightarrow$

$$\det(b_i^t \cdot b_j)_{1\le i,j\le k}^{1/2} = \det(b_i^{*t} \cdot b_j^*)_{1\le i,j\le k}^{1/2}.$$

Ferner gilt $\|b_i^*\| \le \|b_i\|$ $(1 \le i \le k)$ wegen

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \|b_j^*\|^2 \ge \|b_i^*\|^2 \qquad (1 \le i \le k).$$

Damit folgt

$$d(\Lambda) = \det(b_i^{*t} \cdot b_j^*)_{1\le i,j\le k}^{1/2} = \prod_{i=1}^{k} \|b_i^*\| \le \prod_{i=1}^{k} \|b_i\|.$$

□

KOROLLAR 7.15: Es gilt $d(\Lambda)^2 \le M_1 \cdot \ldots \cdot M_k$.

BEWEIS. Seien $y_1, \ldots, y_k \in \Lambda$ linear unabhängig mit $\|y_i\|^2 = M_i$ $(1 \le i \le k)$. Dann ist $\Lambda' := \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_k$ ein Teilgitter von $\Lambda \Rightarrow$

$$d(\Lambda)^2 \le d(\Lambda')^2 \le \prod_{i=1}^{k} \|y_i\|^2 = M_1 \cdot \ldots \cdot M_k.$$

□

3. LLL–reduzierte Basen

DEFINITION 7.16: Wir nennen die Basis $b_1, \ldots, b_k$ LLL–reduziert, falls gelten:
(1) $|\mu_{ij}| \le \frac{1}{2}$ $(1 \le j < i \le k)$,
(2) $\|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \ge \frac{3}{4}\|b_{i-1}^*\|^2$ $(1 < i \le k)$.

SATZ 7.17: Sei $b_1, \ldots, b_k$ LLL–reduziert. Dann gelten:
(1) $\|b_j\|^2 \le 2^{i-1}\|b_i^*\|^2$ $(1 \le j < i \le k)$,
(2) $d(\Lambda) = \prod_{i=1}^{k} \|b_i^*\| \le \prod_{i=1}^{k} \|b_i\| \le 2^{\frac{1}{4}k(k-1)} d(\Lambda)$,
(3) $\|b_1\| \le 2^{\frac{1}{4}(k-1)} d(\Lambda)^{\frac{1}{k}}$,
(4) $\|b_1\|^2 \le 2^{k-1}\|x\|^2 \ \forall\, x \in \Lambda \setminus \{0\}$,
(5) Für $x_1, \ldots, x_t \in \Lambda$ linear unabhängig gilt

$$\|b_j\|^2 \le 2^{k-1} \max\{\|x_1\|^2, \ldots, \|x_t\|^2\} \qquad (1 \le j \le t).$$

BEWEIS. (1) Zunächst gilt

$$\|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 = \|b_i^*\|^2 + \mu_{i,i-1}^2 \|b_{i-1}^*\|^2 \qquad (1 < i \le k).$$

Also

$$\|b_i^*\|^2 \ge \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|b_{i-1}^*\|^2 \ge \frac{1}{2}\|b_{i-1}^*\|^2 \quad (1 < i \le k).$$

Daraus folgt induktiv zunächst

$$\|b_j^*\|^2 \le 2^{i-j}\|b_i^*\|^2 \qquad (1 \le j \le i \le k)$$

und für $i \in \{1, \dots, k\}$ hiermit

$$\begin{aligned}
\|b_i\|^2 &= \|b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*\|^2 \le \|b_i^*\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} \|b_j^*\|^2 \\
&\le \|b_i^*\|^2 + \frac{1}{4}\|b_i^*\|^2 \sum_{j=1}^{i-1} 2^{i-j} = \|b_i^*\|^2 + \frac{1}{4}\|b_i^*\|^2 \sum_{j=1}^{i-1} 2^j \\
&= \|b_i^*\|^2 + \frac{1}{4}\|b_i^*\|^2 (2^i - 2) = \|b_i^*\|^2 (1 + \frac{1}{2}(2^{i-1} - 1)) \\
&= \|b_i^*\|^2 (2^{i-2} + \frac{1}{2}) \le 2^{i-1}\|b_i^*\|^2.
\end{aligned}$$

Damit ergibt sich $\|b_j\|^2 \le 2^{j-1}\|b_j^*\|^2 \le 2^{i-1}\|b_i^*\|$ $(1 \le j < i \le k)$.

(2) Aus (a) folgt zunächst

$$\prod_{i=1}^{k} \|b_i\| \le \prod_{i=1}^{k} 2^{\frac{1}{2}(i-1)} \|b_i^*\| = d(\Lambda) \prod_{i=1}^{k} 2^{\frac{1}{2}(i-1)} = 2^{\frac{1}{4}k(k-1)} d(\Lambda).$$

Die restliche Behauptung erhält man aus dem Beweis zu Satz 7.14.

(3) Aus (a) folgt

$$\|b_1\|^{2k} = \prod_{i=1}^{k} \|b_1\|^2 \le \prod_{i=1}^{k} 2^{i-1}\|b_i^*\|^2 = 2^{\frac{1}{2}k(k-1)} d(\Lambda)^2.$$

(4) Sei $x \in \Lambda \setminus \{0\}$ mit Darstellungen

$$x = \sum_{i=1}^{k} x_i b_i = \sum_{i=1}^{k} x_i^* b_i^* \qquad (x_1, \dots, x_k \in \mathbb{Z}, x_1^*, \dots, x_k^* \in \mathbb{R}).$$

Ist m der größte Index mit $x_m \ne 0$, so gilt gemäß Konstruktion $x_m = x_m^* \Rightarrow$

$$\|x\|^2 \ge x_m^2 \|b_m^*\|^2 \ge \|b_m^*\|^2.$$

Damit folgt aus (a)

$$\|b_1\|^2 \le 2^{m-1}\|b_m^*\|^2 \le 2^{m-1}\|x\|^2.$$

(5) Für

$$x_j = \sum_{i=1}^{k} x_{ij} b_i \qquad (x_{ij} \in \mathbb{Z}, 1 \le i \le k, 1 \le j \le t).$$

sei jeweils i_j der maximale Index mit $x_{i_j,j} \ne 0$. Wie in (d) folgt dann

$$\|x_j\|^2 \ge x_{i_j,j}^2 \|b_{i_j}^*\|^2 \ge \|b_{i_j}^*\|^2 \qquad (1 \le j \le t).$$

O.B.d.A. gelte nun $i_1 \leq \ldots \leq i_t \Rightarrow i_1 < \ldots < i_t$, denn $x_1, \ldots, x_t$ sind linear unabhängig $\Rightarrow i_j \geq j$ $(1 \leq j \leq t)$. Also folgt aus (a)

$$\|b_j\|^2 \leq 2^{i_j - 1}\|b_{i_j}^*\|^2 \leq 2^{k-1}\|b_{i_j}^*\|^2 \leq 2^{k-1}\|x_j\|^2 \qquad (1 \leq j \leq t).$$

□

ALGORITHMUS 7.18 (LLL–Algorithmus): Aus der Basis $b_1, \ldots, b_k$ berechnen wir eine LLL–reduzierte Basis $c_1, \ldots, c_k$ von Λ.

(1) (Initialisierung) Setze $c_i \leftarrow b_i, C_i \leftarrow \|c_i^*\|^2$ $(1 \leq i \leq k)$ und $m \leftarrow 2$.
(2) Setze $l \leftarrow m - 1$.
(3) Falls $|\mu_{ml}| > \frac{1}{2}$, so setze

$$r \leftarrow \lfloor \mu_{ml} + \frac{1}{2} \rfloor, \quad c_m \leftarrow c_m - r c_l,$$

$$\mu_{mj} \leftarrow \mu_{mj} - r\mu_{lj} \quad (1 \leq j \leq l-1), \quad \mu_{ml} \leftarrow \mu_{ml} - r.$$

Falls $l < m - 1$, so gehe zu Schritt 5.
(4) Falls $C_m < (\frac{3}{4} - \mu_{m,m-1}^2)C_{m-1}$, so gehe zu Schritt 6.
(5) Setze $l \leftarrow l - 1$. Falls $l > 0$, so gehe zu Schritt 3. Falls $m = k$, so terminiere, sonst setze $m \leftarrow m + 1$ und gehe zu Schritt 2.
(6) (Vertausche c_{m-1} und c_m) Setze $\mu \leftarrow \mu_{m,m-1}, C \leftarrow C_m + \mu^2 C_{m-1}$ sowie $\mu_{m,m-1} \leftarrow \mu\frac{C_{m-1}}{C}, C_m \leftarrow \frac{C_{m-1}C_m}{C}, C_{m-1} \leftarrow C$. Dann setze

$$\begin{pmatrix} c_{m-1} \\ c_m \end{pmatrix} \leftarrow \begin{pmatrix} c_m \\ c_{m-1} \end{pmatrix}.$$

Ferner

$$\begin{pmatrix} \mu_{m-1,j} \\ \mu_{mj} \end{pmatrix} \leftarrow \begin{pmatrix} \mu_{mj} \\ \mu_{m-1,j} \end{pmatrix} \quad (1 \leq j \leq m-2),$$

und für $i = m+1, \ldots, k$ schließlich

$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \cdot \begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix}.$$

Falls $m > 2$, so setze $m \leftarrow m - 1$. Gehe zu Schritt 2.

Um zu zeigen, daß der obige Algorithmus terminiert, setze

$$\Lambda_i := \sum_{j=1}^{i} \mathbb{Z} \cdot c_j \qquad (1 \leq i \leq k).$$

Für $D_i := d(\Lambda_i)^2$ $(1 \leq i \leq k)$ gilt dann

$$D_i = \det(c_\mu^{*t} \cdot c_\nu^*)_{1 \leq \mu,\nu \leq i} = \prod_{\nu=1}^{i} C_\nu.$$

Nach Satz 7.12 folgt $M_1^i \leq \gamma_i^i \cdot D_i$ $(1 \leq i \leq k)$, wobei M_1 die Länge des kürzesten Gitters in Λ sei. Nach jedem Durchlauf von Schritt 6 des Algorithmus ist der neue Wert von C_{m-1} um einen Faktor $< \frac{3}{4}$ kleiner als der alte Wert von C_{m-1} und damit ebenso der neue Wert von D_{m-1}. Andererseits bleiben die übrigen D_i unverändert, weil die zugehörigen Gitter Λ_i sich nicht ändern. Also terminiert der Algorithmus.

ALGORITHMUS 7.19 (MLLL–Algorithmus): Es seien $c_1, \dots, c_k \in \Lambda$ linear unabhängig. Zu $c_{k+1} \in \Lambda$ beliebig berechnen wir $m_1, \dots, m_{k+1} \in \mathbb{Z}$ mit

$$\sum_{i=1}^{k+1} m_i b_i = 0 \qquad (|m_1| + \ldots + |m_{k+1}| > 0).$$

Ferner bestimmen wir $c'_1, \dots, c'_k \in \Lambda$, so daß

$$\sum_{i=1}^{k+1} \mathbb{Z} \cdot c_i = \sum_{i=1}^{k} \mathbb{Z} \cdot c'_i.$$

(1) (Initialisierung) Setze $C_i \leftarrow \|c_i^*\|^2, c'_i \leftarrow c_i$ $(1 \le i \le k+1)$. Ferner setze $H = (h_1, \dots, h_{k+1}) \leftarrow I_{k+1}$ und $m \leftarrow 2$.
(2) Setze $l \leftarrow m-1$.
(3) Falls $|\mu_{ml}| > \frac{1}{2}$, setze

$$r \leftarrow \lfloor \mu_{ml} + \frac{1}{2} \rfloor, \quad c'_m \leftarrow c'_m - r c'_l, h_m \leftarrow h_m - r h_l,$$

$$\mu_{mj} \leftarrow \mu_{mj} - r\mu_{lj} \quad (1 \le j \le l-1), \quad \mu_{ml} \leftarrow \mu_{ml} - r.$$

Falls $c'_m = 0$, so setze $c'_i \leftarrow c'_{i+1}$ $(m \le i \le k), (m_1, \dots, m_{k+1})^t \leftarrow h_m$ und terminiere. Falls $l < m-1$, so gehe zu Schritt 5.
(4) Falls $C_m < (\frac{3}{4} - \mu_{m,m-1}^2) C_{m-1}$, so gehe zu Schritt 6.
(5) Setze $l \leftarrow l-1$. Falls $l > 0$, so gehe zu Schritt 3, sonst setze $m \leftarrow m+1$ und gehe zu Schritt 2.
(6) Setze $\mu \leftarrow \mu_{m,m-1}, C \leftarrow C_m + \mu^2 C_{m-1}$. Falls $C = 0$, so gehe zu Schritt 7. Setze $\mu_{m,m-1} \leftarrow \mu \frac{C_{m-1}}{C}$ sowie $C_m \leftarrow \frac{C_{m-1} C_m}{C}$ und für $i = m+1, \dots, k$ ferner

$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \cdot \begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix}.$$

(7) (Vertausche c'_{m-1} und c'_m) Setze $C_{m-1} \leftarrow C$.

$$\begin{pmatrix} h_{m-1} \\ h_m \end{pmatrix} \leftarrow \begin{pmatrix} h_m \\ h_{m-1} \end{pmatrix}, \quad \begin{pmatrix} c'_{m-1} \\ c'_m \end{pmatrix} \leftarrow \begin{pmatrix} c'_m \\ c'_{m-1} \end{pmatrix},$$

$$\begin{pmatrix} \mu_{m-1,j} \\ \mu_{mj} \end{pmatrix} \leftarrow \begin{pmatrix} \mu_{mj} \\ \mu_{m-1,j} \end{pmatrix} \quad (1 \le j \le m-2).$$

Falls $m > 2$, so setze $m \leftarrow m-1$. Gehe zu Schritt 2.

Wir zeigen nun, daß der obige Algorithmus terminiert. Nach der Initialisierung gilt zunächst $C_{k+1} = 0$. Wie in Algorithmus 7.18 schließt man nun, daß in Schritt 6 der Wert C nur endlich oft $\neq 0$ sein kann, da in diesem Fall der neue Wert von C_{m-1} um einen Faktor $< \frac{1}{4}$ kleiner als der alte Wert von C_{m-1} ist. Also erreicht man nach endlich vielen Schritten $\mu_{k+1,k} = 0 \Rightarrow b_{k+1}$ ist linear abhängig von $b_1, \dots, b_{k-1}$ (†). Nach Voraussetzung existieren $m_1, \dots, m_{k+1} \in \mathbb{Z}, |m_1| + \cdots + |m_{k+1}| > 0$, mit

$$\sum_{i=1}^{k+1} m_i b_i = 0.$$

Aus (†) folgt dann $m_k = 0$. Also ist

$$\Lambda' := \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_{k-1} + \mathbb{Z}b_{k+1}$$

nach dem Beweis zu Satz 5.33 ein $(k-1)$–dimensionales Teilgitter von Λ. Der Algorithmus wird nun auf diesem Teilgitter fortgesetzt. Sofern er nicht vorher terminiert, liefert er schließlich zwei linear abhängige Vektoren $c_1', c_2' \in \Lambda$. Nach endlich vielen weiteren Schritten gilt dann $\mu_{12} = 0 \Rightarrow c_2' = 0$. Damit terminiert der Algorithmus.

KAPITEL 8

Dedekind Ringe

1. Projektive Moduln II

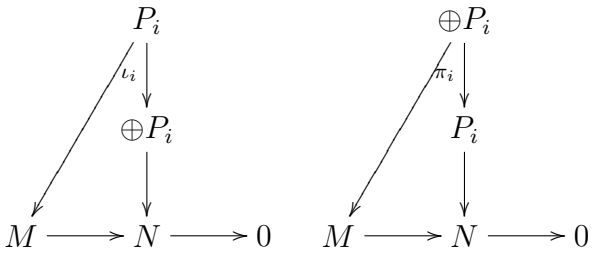
LEMMA 8.1: (1) Ein R-Modul P ist genau dann projektiv, wenn für jede exakte Sequenz $M \to N \to 0$ auch $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N) \to 0$ exakt ist.
(2) $\mathrm{Hom}_R(\oplus_{i\in I} M_i, M) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, M)$
(3) $\mathrm{Hom}_R(M, \prod_{i\in I} M_i) \cong \prod_{i\in I} \mathrm{Hom}_R(M, M_i)$
(4) Es sei $P = \oplus P_i$. Dann ist P genau dann projektiv, wenn jedes P_i projektiv ist.

BEWEIS. (1): Es sei $f \in \mathrm{Hom}_R(P, N)$ beliebig. P projektiv sichert die Existenz von $g : P \to M$ mit $hg = f$, also $h_*(g) = f$.

Die Rückrichtung ist trivial.

(2), (3): Übung.

(4): Wir betrachten folgende Diagramme:



Wir nehmen nun $\oplus P_i$ projektiv an. Es sei $f : P_i \to N$ beliebig. Dann ist $\tilde{f} := f\pi_i : \oplus P_i \to N$. Nach Voraussetzung existiert $\tilde{g} : \oplus P_i \to M$ mit $h\tilde{g} = \tilde{f}$. $g := \tilde{g}\iota_i : P_i \to N$ tut's.

Es sei nun P_i projektiv für jedes i und $f : \oplus P_i \to N$ beliebig. Zu $f_i := f\iota_i : P_i \to N$ existiert dann $g_i : P_i \to M$ mit $hg_i = f_i$. $g : \oplus P_i \to M : (x_i) \mapsto \sum g_i(x_i)$ tut's dann.

□

SATZ 8.2: Für einen R-Modul P sind äquivalent:
(1) P ist projektiv.
(2) Es seien M, N weitere R-Moduln. $M \xrightarrow{h} N \to 0$ exakt impliziert $\mathrm{Hom}_R(P, M) \xrightarrow{h_*} \mathrm{Hom}_R(P, N) \to 0$ exakt.
(3) Ist $h : M \to N$ surjektiv und $f : P \to N$ beliebig, so gibt es ein $g : P \to M$ mit $f = hg$.
(4) Für jede exakte Sequenz $M \xrightarrow{h} P \to 0$ existiert $g : P \to M$ mit $hg = \mathrm{id}_P$.
(5) Ist $0 \to M \xrightarrow{f} N \xrightarrow{h} P \to 0$ exakt, so folgt $N \cong M \oplus P$.
(6) Es gibt einen freien Modul F und $N < F$ mit $F = N \oplus P$

BEWEIS. (1)⇒(2):8.1.(1) Es sei $f \in \mathrm{Hom}(P,N)$ beliebig. P projektiv sichert die Existenz von $g : P \to M$ mit $hg = f$, also $h_*(g) = f$.

(2)⇒(3): f surjektiv bedeutet $M \to N \to 0$ ist exakt.

(3)⇒(4):trivial

(4)⇒(5): Mit (4) folgt die Existenz von $g : P \to N$ mit $\mathrm{id}_P = hg$. Da g injektiv ist, können wir P als Teilmodul von N auffassen. Da die Sequenz exakt ist, ist f injektiv und M ebenfalls ein Teilmodul von N. Zeige: $N = M \oplus P$. Wegen $a = a - gh(a) + gh(a)$ und $h(a - gh) = 0$ folgt $N = M + P$. Es sei nun $a \in M \cap P$. $\Rightarrow$ $h(a) = 0$ und $gh(a) = a$ also $a = 0$.

(5)⇒(6): Es sei x_i ein Erzeugendensystem für P und F der hier von frei erzeugte Modul. Die Abbildung $h : F \to P : 1x_i \to x_i$ ist surjektiv, so daß $F \to P \to 0$ exakt ist. Mit $R := \ker h$ erhalten wir eine kurze exakte Sequenz $0 \to R \to F \to P \to 0$. Mit (5) folgt die Behauptung.

(6)⇒(1): Da F frei ist und daher projektiv, ist dies eine Folge von 8.1.(4). □

DEFINITION 8.3: Es sei R ein unitärer Integritätsring. R heißt *Dedeking Ring*, wenn jedes Ideal $\mathfrak{a}$ von R als R-Modul projektiv ist.

Dies ist eine Verallgemeinerung von Hauptidealringen: Ein Ring ist PID genau dann, wenn jedes Ideal als R-Modul frei ist.

DEFINITION 8.4: Es sei R ein Integritätsring.

(1) Ein R-Modul $M \subseteq Q(R)$ heißt *gebrochenes Ideal* (engl. fractional ideal), wenn es ein $a \in R$ gibt mit $aM \subseteq R$
(2) Für gebrochene Ideale $\mathfrak{a}$, $\mathfrak{b}$ ist $[\mathfrak{a}/\mathfrak{b}] := \{x \in Q(R) \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$
(3) Für gebrochene Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R ist $\mathfrak{ab} := \{\sum_{\text{fin.}} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$
(4) Ein gebrochene Ideal $\mathfrak{a}$ heißt *invertierbar* wenn es ein Ideal $\mathfrak{b}$ mit $\mathfrak{ab} = R$ gibt, $\mathfrak{a}^{-1} := \mathfrak{b}$.

Ab jetzt können alle Ideale (wenn nichts anderes gefordert wird) ohne Vorwarnung gebrochen sein. Gewöhliche Ideale heißen auch ganze Ideale

BEMERKUNG 8.5: (1) Jedes ganze Ideal ist ein gebrochenes Ideal (mit $a := 1$).
(2) $\mathfrak{ab}$ ist ein Ideal: Es sei $a\mathfrak{a} \subseteq R$ und $b\mathfrak{b} \subseteq R$. Dann gilt $ab \sum_{\text{fin.}} a_i b_i = \sum_{\text{fin.}} (aa_i)(bb_i) \in R$, also $ab\mathfrak{ab} \subseteq R$. Offenbar ist $\mathfrak{ab}$ ein R-Modul und damit ein gebrochenes Ideal.
(3) $\mathfrak{a}R = R\mathfrak{a} = \mathfrak{a}$ ($1 \in R$!)
(4) $[R/\mathfrak{a}]$ ist ein Ideal: $a[R/\mathfrak{a}] \subseteq R$ für jedes $a \in \mathfrak{a}$ nach Definition.
(5) $\mathfrak{a}[R/\mathfrak{a}] \subseteq R$: Nach Definition.
(6) $\mathfrak{a}$ ist invertierbar, genau dann, wenn $\mathfrak{a}[R/\mathfrak{a}] = R$ gilt: $\mathfrak{a}$ invertierbar, also $\mathfrak{ab} = R$ mit $\mathfrak{b} := \mathfrak{a}^{-1}$. Wegen $b\mathfrak{a} \in \mathfrak{ab} \subseteq R$ für alle $b \in \mathfrak{b}$ folgt $\mathfrak{b} \subseteq [R/\mathfrak{a}]$, und damit $R = \mathfrak{ab} \subseteq \mathfrak{a}[R/\mathfrak{a}] \subseteq R$.
(7) $\mathfrak{a}^{-1}$ ist eindeutig (wenn existent): $\mathfrak{ab} = R$ impliziert $\mathfrak{b} \subseteq [R/\mathfrak{a}]$. Damit folgt $\mathfrak{b} = R\mathfrak{b} = [R/\mathfrak{a}]\mathfrak{ab} = [R/\mathfrak{a}]R = [R/\mathfrak{a}]$.

SATZ 8.6: Die Menge I_R der invertierbaren Ideale bildet eine (multiplikative) Gruppe, die Menge P_R der Hauptideale eine Untergruppe. $\mathrm{Cl}_R := I_R/P_R$ ist die *Klassengruppe* (Picard-Gruppe) von R.

BEWEIS. Klar. □

LEMMA 8.7: Es sei P ein R-Modul. P ist genau dann projektiv, wenn es Elemente $p_i \in P$ und $f_i \in \mathrm{Hom}_R(P,R)$ gibt so, daß für jedes $a \in P$ nur endlich viele $f_i(a) \neq 0$ sind und $a = \sum f_i(a)p_i$ gilt.

BEWEIS. Es sei P projektiv. Nach 8.2.(6) existiert ein (über X) freier R-Modul F, so daß $F = P \oplus M$ gilt und $F \xrightarrow{f} P \to 0$ exakt ist. Nach 5.13.(4) ist die Darstellung $x = \sum r_i(x)x_i$ ($x_i \in X$, $r_i(x) \in R$) eindeutig, so daß $x \mapsto r_i(x)$ ein R-Homomorphismus ist. Mit $a_i := f(x_i)$ und $f_i := f|_P$ erhalten wir die gewünschte Darstellung.

Es seien nun $f_i : P \to R$ und $a_i \in P$ gegeben. Wir definieren F als den von a_i frei erzeugten R-Modul und betrachten die Abbildungen $g : P \to F : x \mapsto x$ und $f : F \to P : x \mapsto x$. Offenbar gilt $fg = \mathrm{id}_P$ und daher $F = P \oplus M$ mit $M := \ker f$. Nach 8.2.(6) ist P daher projektiv. □

SATZ 8.8: Ein Ideal ist genau dann invertierbar, wenn es ein projektiver R-Modul ist.

BEWEIS. Es sei $\mathfrak{a}$ invertierbar, d.h. $\mathfrak{a}\mathfrak{a}^{-1} = R$. Also existieren $a_i \in \mathfrak{a}$ und $b_i \in \mathfrak{a}^{-1}$ mit $1 = \sum_{\text{fin.}} a_i b_i$. Definiere $f_i : \mathfrak{a} \to R : x \mapsto b_i x$. Dann gilt $x = 1x = \sum_{\text{fin.}} a_i b_i x = \sum_{\text{fin.}} a_i f_i(x)$ und $\mathfrak{a}$ ist projektiv nach 8.7.

Es sei nun $\mathfrak{a}$ projektiv. Nach 8.7 existieren $f_i : \mathfrak{a} \to R$ und $a_i \in \mathfrak{a}$ mit $x = \sum a_i f_i(x)$ für jedes $x \in \mathfrak{a}$.

Definiere $x_i := f(x)/x \in Q(R)$ für $0 \neq x \in \mathfrak{a}$. Dies ist unabhängig von der Wahl von x: $xf_i(y) = f_i(xy) = yf_i(x)$, also $f_i(x)/x = f_i(y)/y$.

Wegen $x_i a = f_i(x)/xa = f_i(ax)/x = f_i(a)x/x = f_i(a) \in R$ für jedes $a \in \mathfrak{a}$ folgt $x_i \in [R/\mathfrak{a}]$. Für $x \in \mathfrak{a}$ sind nur endlich viele $f_i(x) \neq 0$, also $x = \sum_{\text{fin.}} f_i(a)a_i = \sum_{\text{fin.}} xx_i a_i = x\sum_{\text{fin.}} x_i a_i$, also $1 = \sum_{\text{fin.}} x_i a_i$ und daher $R = \mathfrak{a}[R/\mathfrak{a}]$. □

LEMMA 8.9: Es sei R ein Integritätsring und M ein endlich erzeugter torsionsfreier R-Modul. Dann ist M Teilmodul eines freien Moduls.

BEWEIS. Es seien $x_1, \ldots, x_n$ Erzeuger von M. $M \otimes_R Q(R) =: V$ ist ein m-Dimensionaler $Q(R)$-Vektorraum ($m \leq n$) mit Basis $y_1, \ldots, y_m$. In dem wir $x \in M$ mit $x \otimes 1$ identifizieren gilt $M \subseteq V$ und $x_i = \sum_{j=1}^m r_{i,j} y_j$. Wähle nun ein $0 \neq d \in R$ mit $dr_{i,j} \in R$ für jedes i und jedes j. Damit gilt dann $M \subseteq 1/d \sum y_i R$. □

SATZ 8.10: Es sei R ein Dedekind Ring und M ein endlich erzeugter torsionsfreier R-Modul. Dann gibt es Ideale $\mathfrak{a}_i$ von R und Elemente $x_i \in M \otimes_R Q(R)$ mit $M = \sum_{i=1}^n \mathfrak{a}_i x_i$.

BEWEIS. Es sei F der in 8.9 konstruierte freie Modul. Der Beweis geht nun per Induktion über die Dimension n von F. $n = 0$: Klar

$n-1 \mapsto n$: Es sei $M \subseteq F$ wo F frei vom Rang n mit Basis $x_1, \ldots, x_n$ ist. F' sei der frei von $x_1, \ldots, x_{n-1}$ erzeugte Modul. Wir betrachten die Abbildung $f : F \to Q(R) : \sum_{i=1}^n x_i r_i \mapsto r_n$ bzw. die Einschränkung $f|_M : M \to R$. Da F frei ist, ist f wohldefiniert und linear. Die Sequenz:

$$0 \to \ker f \to M \to \mathrm{bild}\, f \to 0$$

ist exakt, bild f ist ein R-Teilmodul von R also ein Ideal, also ein projektiver Teilmodul. Mit 8.2.(5) folgt $M \cong \text{bild}\, f \oplus \ker f$. Damit ist $\ker f$ endlich erzeugt, es gilt $\ker f \subseteq F'$. Nach 8.2.(4) existiert $g : \text{bild}\, f \to M$, also (wegen $\dim \text{bild}_f \otimes Q(R) = 1$) existiert ein $y \in F$ mit $g(\alpha) = y\alpha$.

Nach Induktionsvoraussetzung folgt: $\ker f = \sum_{i-1}^{n-1} a_i \mathfrak{a}_i$ und $M = y\,\text{bild}\, f + \sum_{i=1}^{n-1} a_i \mathfrak{a}_i$.

(Wegen $ker f \subseteq F'$ folgt $a_i \in F'$) □

2. Dedekind Ringe

Nach dem wir gesehen habe, daß Dedekind Ringe nützlich sind, werden wir uns nun etwas mehr mit ihnen beschäftigen.

Insbesondere wollen wir ein paar Ringe als Dedekindsch nachweisen.

Satz 8.11: Es sei R ein Dedekind Ring. Dann ist R Noethersch und jedes Primideal $(0) \neq \mathfrak{p}$ ist maximal.

Beweis. Es sei $(0) \neq \mathfrak{a}$ ein Ideal. Da $\mathfrak{a}$ invertierbar ist, existieren $a_i \in \mathfrak{a}$ und $b_i \in \mathfrak{a}^{-1}$ mit $1 = \sum_{i=1}^{n} a_i b_i$. Damit folgt $x = 1x = \sum_{i=1}^{n} x b_i a_i$ mit $x_i b_i \in R$ für $x \in \mathfrak{a}$. Daher ist $a_1, \ldots, a_n$ ein erzeugenden System für $\mathfrak{a}$, $\mathfrak{a}$ ist endlich erzeugt und R Noethersch.

Es sei nun $(0) \neq \mathfrak{p}$ ein Primideal in R und $\mathfrak{m} \supseteq \mathfrak{p}$ maximal. Damit gilt $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = R$ und $\mathfrak{p}\mathfrak{m}^{-1}$ ist ein ganzes Ideal. Wegen $(\mathfrak{p}\mathfrak{m}^{-1})\mathfrak{m} = \mathfrak{p}$ folgt $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}$ oder $\mathfrak{m} \subseteq \mathfrak{p}$ da $\mathfrak{p}$ Primideal ist. Aus $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}$ folgt $\mathfrak{m}^{-1} \subseteq \mathfrak{p}^{-1}\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}^{-1}\mathfrak{p} = R$ und damit $\mathfrak{m} = R$. Also gilt $\mathfrak{m} \subseteq \mathfrak{p}$ und damit $\mathfrak{p} = \mathfrak{m}$, $\mathfrak{p}$ ist maximal. □

Definition 8.12: Es sei R ein Integritätsring und $K \supseteq R$ ein Körper. $a \in K$ heißt *ganz über R*, falls es ein normiertes Polynom $f \in R[x]$ mit $f(a) = 0$ gibt.

Offensichtlich sind ganze Elemente immer auch algebraisch über $Q(R)$.

Lemma 8.13: Es sei R ein Integritätsring und $K \supseteq R$ ein Körper sowie $a \in K$. Dann sind äquivalent:

(1) a ist ganz über R
(2) $R[a]$ ist endlich erzeugter R-Modul
(3) Es existiert ein endlich erzeugter R-Modul $0 \neq M \subseteq K$ mit $aM \subseteq M$

Beweis. Übung □

Korollar 8.14: Die Menge $\text{Cl}(R, L)$ aller R-ganzen Elemente in L bildet einen Ring, den *ganzen Abschluß von R in L*

In der Übung haben wir gesehen, daß die über $\mathbb{Z}$-ganzen Elemente einen endlich erzeugten (freien) $\mathbb{Z}$-Modul vom Rang $(L : \mathbb{Q})$ bilden.

Definition 8.15: Ein Ring R mit $\text{Cl}(R, Q(R)) = R$ heißt *ganz abgeschlossen*.

Satz 8.16: Es sei R Integritätsring, $R \subseteq K$ ein Körper, L/K eine Erweiterung von K. Dann gilt $\text{Cl}(R, L) = \text{Cl}(\text{Cl}(R, K), L)$.

BEWEIS. Wir setzen $S := \mathrm{Cl}(R,K)$, müssen also $\mathrm{Cl}(R,L) = \mathrm{Cl}(S,L)$ zeigen. Wegen $R \subseteq \mathrm{Cl}(R,K) = S$ ist $\mathrm{Cl}(R,L) \subseteq \mathrm{Cl}(S,L)$ klar. Sei nun also $x \in \mathrm{Cl}(S,L)$ und $a_i \in S$ mit $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ gegeben. Setze $R_1 := R[a_0, \ldots, a_{n-1}]$. R_1 ist als R-Modul endlich erzeugt (mit Induktion und 8.13). Ferner ist $x \in \mathrm{Cl}(R_1, L)$, also ist $R_1[x]$ nach 8.13 endlich erzeugter R_1 Modul und damit ebenfalls über R endlich erzeugt. Wegen $xR_1[x] \subseteq R_1[x]$ folgt dann mit 8.13 $x \in \mathrm{Cl}(R,L)$. □

KOROLLAR 8.17: Ganze Abschlüsse sind ganz abgeschlossen.

KOROLLAR 8.18: Dedekind Ringe sind ganz abgeschlossen.

BEWEIS. Es sei $x \in \mathrm{Cl}(R, Q(R))$ beliebig. Nach 8.13 ist $R[x]$ ein endlich erzeugter R-Modul, $R[x] := \langle a_1, \ldots, a_n \rangle$. (für $a_i \in Q(R)$ geeignet) Wähle $b \in R$ mit $ba_i \in R$ für alle i. Dann gilt $bR[x] \subseteq R$ und $R[x]$ ist ein Ideal, also invertierbar. Wegen $1 \in R[x]$ folgt $R[x]^2 = R[x]$. Damit gilt:

$$R[x] = RR[x] = R[x]R[x]^{-1}R[x] = R[x]^2R[x]^{-1} = R[x]R[x]^{-1} = R$$

also $x \in R$. □

LEMMA 8.19: Es sei R Noethersch und $(0) \neq \mathfrak{a} \neq R$ ein ganzes Ideal. Dann gibt es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.

BEWEIS. Es sei $\mathcal{M} := \{\mathfrak{a} \mid 8.19 \text{ gilt nicht}\}$. Angenommen $\mathcal{M} \neq \emptyset$. Dann gibt es in $\mathcal{M}$ ein maximales Element $\mathfrak{a}$. $\mathfrak{a}$ kann kein Primideal sei, da anderfalls 8.19 trival erfüllt ist: $\mathfrak{a} = \mathfrak{a} = \mathfrak{a}$.

Also gibt es $a, b \notin \mathfrak{a}$ mit $ab \in \mathfrak{a}$. Setze $\mathfrak{b} := \mathfrak{a} + (a)$ und $\mathfrak{c} := \mathfrak{a} + (b)$. Offenbar gilt $\mathfrak{a} \subseteq \mathfrak{b}, \mathfrak{c} \subseteq R$. Angenommen $\mathfrak{b} = R$, dann folgt $(b) = Rb = \mathfrak{b}b = \mathfrak{a}b + (ab) \subseteq \mathfrak{a}$. Also gilt $\mathfrak{b}$, $\mathfrak{c} \neq R$. Da $\mathfrak{a}$ maximal war gilt 8.19 für $\mathfrak{b}$ und $\mathfrak{c}$. Also gibt es $\mathfrak{p}_i$ und $\mathfrak{q}_j$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{b} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ und $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{c} \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$. Mit $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ erhalten wir 8.19 dann auch für $\mathfrak{a}$. (Beachte: $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ für alle Ideale). □

LEMMA 8.20: Es sei R ein Noetherscher Integritätsring, der ganz abgeschlossen ist und in dem jedes $(0) \neq \mathfrak{p}$ Primideal maximal ist. Dann ist jedes Primideal invertierbar.

BEWEIS. Es sei $(0) \neq \mathfrak{p}$ ein Primideal. Für $0 \neq a \in \mathfrak{p}$ gibt es nach 8.19 Primideale $\mathfrak{p}_i$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq (a)$. Fixiere nun a so, daß n möglichst klein ist. Wegen $a \in \mathfrak{p}$ und $\mathfrak{p}$ prim, gibt es daher ein i_0 (o.b.d.A. $i_0 = 1$) mit $\mathfrak{p}_1 \subseteq \mathfrak{p}$, also $\mathfrak{p}_1 = \mathfrak{p}$. Da n minimal war, gilt $\mathfrak{p}_2 \cdots \mathfrak{p}_n \not\subseteq (a)$, also gibt es ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \setminus (a)$. Wegen $b\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq (a)$ folgt $ba^{-1}\mathfrak{p} \subseteq R$ also $ba^{-1} \in [R/\mathfrak{p}]$. $b \notin (a)$ impliziert $ba^{-1} \notin R$ also $[R/\mathfrak{p}] \supset R$.

$\mathfrak{p}[R/\mathfrak{p}]$ ist ein Ideal. Wegen $\mathfrak{p} = \mathfrak{p}R \subseteq \mathfrak{p}[R/\mathfrak{p}] \subseteq R$ folgt also $\mathfrak{p}[R/\mathfrak{p}] = \mathfrak{p}$ oder $= R$. Angenommen, es gilt $\mathfrak{p}[R/\mathfrak{p}] = \mathfrak{p}$. Dann folgt $\mathfrak{p}[R/\mathfrak{p}]^n = \mathfrak{p}$ für alle $n \in \mathbb{N}$ und damit für $0 \neq x \in \mathfrak{p}$ und $y \in [R/\mathfrak{p}] \setminus R$ sogar $xy^n \in \mathfrak{p} \subseteq R$. Damit erhalten wir $xR[y] \subseteq R$, so daß $xR[y]$ ein ganzes Ideal ist. R ist Noethersch, also gibt es $a_1, \ldots, a_m$ mit $xR[y] = \langle a_1, \ldots, a_m \rangle$. Damit folgt auch $R[y] = \langle a_1 x^{-1}, \ldots, a_m x^{-1} \rangle$. Nach 8.13 ist daher $y \in \mathrm{Cl}(R, Q(R))$, also $y \in R$ nach Voraussetzung.

Also erhalten wir $\mathfrak{p}[R/\mathfrak{p}] = R$ und $\mathfrak{p}$ ist invertierbar. □

LEMMA 8.21: Die Voraussetzungen seien wie in 8.20. Dann ist jedes ganzes Ideal $R \neq \mathfrak{a}$ als Produkt von Primidealen darstellbar.

BEWEIS. Angenomen, 8.21 ist falsch. Dann gibt es ein Ideal $\mathfrak{a}$ welches sich nicht in Primideale faktorisieren lässt. Nach 8.19 existieren $\mathfrak{p}_i$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}$. Unter all diesen $\mathfrak{a}$ wähle eines wo n minimal ist. $n = 1$ impliziert $\mathfrak{a} = \mathfrak{p}$, also $n > 1$. Für $\mathfrak{p} := \mathfrak{p}_1$ folgt (wegen $\mathfrak{a} \subseteq \mathfrak{p}_1$) $\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$. Daher ist $\mathfrak{a}\mathfrak{p}^{-1}$ ein ganzes Ideal. Nach Wahl von $\mathfrak{a}$ gilt $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ und daher $\mathfrak{a} = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_m$. □

SATZ 8.22: Ein unitärer Integritätsring R ist Dedekind Ring genau dann, wenn
(1) er ganz abgeschlossen ist
(2) er Noethersch ist
(3) jedes Primideal maximal ist.

BEWEIS. 8.11 (2, 3), 8.18 (1) zeigen, daß die Bedingungen notwendig sind.

Es sei nun R ein unitärer Integritätsring mit 1-3 und $(0) \neq \mathfrak{a}$ ein Ideal. Dann gibt es $a \in R$ mit $a\mathfrak{a} \subseteq R$. Nach 8.21 gilt $a\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ und daher $\mathfrak{a} = (a^{-1})\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Also ist $\mathfrak{a}$ Produkt invertierbarer Ideale und daher invertierbar. Mit 8.8 ist $\mathfrak{a}$ projektiv. □

SATZ 8.23: In einem Dedekind Ring läßt sich jedes Ideal $0 \neq \mathfrak{a}$ (bis auf Reihenfolge) eindeutig als Produkt von Primidealen schreiben.

BEWEIS. Die Existenz folgt aus 8.21, es bleibt die Eindeutigkeit zu zeigen. Es sei $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ gebenen. Wir wählen $\mathfrak{a}$ so, daß $n \leq m$ minimal ist für alle Ideale die vercshiedene Faktorisierungen zulassen. Aus $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{p}_1$ folgt (o.b.d.A) $\mathfrak{q}_1 = \mathfrak{p}_1$ und $\mathfrak{q}_2 \cdots \mathfrak{q}_m = \mathfrak{p}_2 \cdots \mathfrak{p}_n$. Nach Wahl von $\mathfrak{a}$ sind nun die Restfaktorisierungen gleich. □

BEMERKUNG 8.24: Es sei R ein Dedekind Ring.

(1) Der ganze Abschluss von $\mathbb{Z}$ in einem beliebigem Zahlkörper ist Dedekindsch.
(2) Die Gruppe der von (0) verschiedenen Ideale ist frei erzeugt von den Primidealen.
(3) Ein ganzes Ideal $\mathfrak{a}$ kann nur endlich viele ganze Teiler haben.
(4) $\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{b}|\mathfrak{a} \iff \mathfrak{a} = \mathfrak{b}\mathfrak{c}$ mit einem ganzen Ideal $\mathfrak{c}$: Es sei $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ mit $\mathfrak{c}$ ganz. Dann gilt $\mathfrak{a} = \mathfrak{a}R \subseteq \mathfrak{a}\mathfrak{c}^{-1} = \mathfrak{b}$. Gilt nun andererseits $\mathfrak{a} \subseteq \mathfrak{b}$, so folgt $\mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = R$ und $\mathfrak{c} := \mathfrak{a}\mathfrak{b}^{-1} \subseteq R$.
(5) Es sei $\mathfrak{a}$ ein Ideal. Dann existiert ein Hauptideal (a) mit $(a)\mathfrak{a}^{-1} \subseteq R$.
(6) Es gilt $\mathfrak{a} + \mathfrak{b} = \mathrm{ggT}(\mathfrak{a}, \mathfrak{b})$ für ganze Ideale: Wegen $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ folgt aus $\mathfrak{a} + \mathfrak{b}| \mathrm{ggT}(\mathfrak{a}, \mathfrak{b})$. Da $\mathfrak{a} + \mathfrak{b}$ minimal ist mit $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{c}$, folgt die Behauptung.
(7) Es gilt $\mathfrak{a} \cap \mathfrak{b} = \mathrm{kgV}(\mathfrak{a}, \mathfrak{b})$ für ganze Ideale.

BEMERKUNG 8.25: Es sei R Dedekind Ring und $(0) \neq \mathfrak{p}$ ein Primideal. Nach 8.24.(2) ist die Funktion $v_\mathfrak{p} : I_R \to \mathbb{Z} : \mathfrak{a} \mapsto z$ mit $\mathfrak{p}^z \| \mathfrak{a}$ wohldefiniert. Für $0 \neq x \in Q(R)$ setzten wir $v_\mathfrak{p}(x) := v_\mathfrak{a}(xR)$. Dann gelten:

(1) $v_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})$
(2) $R = \{a \in Q(R) \mid v_\mathfrak{p}(a) \geq 0 \forall \mathfrak{p}\}$
(3) $v_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$
(4) $v_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = \max(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$
(5) $v_\mathfrak{p}(x + y) \geq \min(v_\mathfrak{p}(x), v_\mathfrak{p}(y))$ wobei $>$ höchstens dann auftreten kann, wenn $v_\mathfrak{p}(x) = v_\mathfrak{p}(y)$ gilt.
(6) $\mathfrak{a}^{-1} \cap \mathfrak{b}^{-1} = (\mathfrak{a} + \mathfrak{b})^{-1}$

Es $x \in Q(R)$ mit $v_\mathfrak{p}(x) \geq 0$ heißt auch $\mathfrak{p}$-ganz.

SATZ 8.26 (Schwacher Approximationssatz): Es seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ Primideale, $l_i \in \mathbb{Z}$ beliebig. Dann gibt es ein $x \in Q(R)$ mit $v_{\mathfrak{p}_i}(x) = l_i$ und $v_\mathfrak{p}(x) \geq 0$ ür jedes weitere Primideal.

BEWEIS. Wähle $x_i \in \mathfrak{p}_i^{l_i} \setminus \mathfrak{p}_i^{l_i+1}$ beliebig und ein $a \in R$ mit $ax_i \in R$ für alle i. Für jedes $\mathfrak{p}_{n+1}, \ldots, \mathfrak{p}_m$ mit $\mathfrak{p}_j|(a)$ wähle ein $x_i \in \mathfrak{p}_i^{v_{\mathfrak{p}_i}(a)} \setminus \mathfrak{p}_i^{v_{\mathfrak{p}_i}(a)+1}$. Mit dem Chinesischem Restsatz erhalten wir ein $\tilde{x} \in R$ mit $x \cong \begin{cases} ax_i \bmod \mathfrak{p}_i^{l_i+v_{\mathfrak{p}_i}(a)} & 1 \leq i \leq n \\ a_i \bmod \mathfrak{p}_i^{v_\mathfrak{p}(a)} & \text{sonst.} \end{cases}$ $x := x/a$ erfüllt dann alles. □

LEMMA 8.27: Es seien $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Ideale. Dann gibt es $x, y \in Q(R)$ mit $x\mathfrak{a} + y\mathfrak{b} = \mathfrak{c}$. Speziell kann jedes Ideal mit maximal zwei Elementen erzeugt werden.

BEWEIS. Wähle $\beta \in \mathfrak{b}^{-1}\mathfrak{c}$ beliebig, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ seien alle Primideale die in der Faktorisierung von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ und (β) auftauchen (dies sind nur endlich viele!). Mit 8.26 finde ein $x \in Q(R)$ mit $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(\mathfrak{c}\mathfrak{a}^{-1})$ und $v_\mathfrak{p}(x) \geq 0$ sonst. Dann folgt $v_\mathfrak{p}(x\mathfrak{a} + \beta\mathfrak{b}) = \min(v_\mathfrak{p}(x\mathfrak{a}), v_\mathfrak{p}(\beta\mathfrak{b})) = v_\mathfrak{p}(\mathfrak{c})$. □

DEFINITION 8.28: Es sei M ein endlich erzeugter R-Modul, R ein Dedekind Ring, $V := M \otimes Q(R)$. Ideale $\mathfrak{a}_i$ und Elemente $\alpha_i \in V$ mit $M = \sum_{i=1}^n \alpha_i\mathfrak{a}_i$ heißen *Pseudobasis* für M.
Es sei $0 \neq \alpha \in V$ beliebig. $\mathfrak{a}_\alpha := \{x \in Q(R) \mid x\alpha \in M\}$ heißt das *Koeffizientenideal* zu α.

BEMERKUNG 8.29: (1) In 8.10 haben wir gesehen, daß Pseudobasen immer existieren.
(2) Für jedes $\alpha \in V$ gilt $\mathfrak{a}_\alpha \neq (0)$. Ferner ist $\mathfrak{a}_\alpha$ immer ein Ideal.
(3) Für eine Pseudobasis $(\mathfrak{a}_i, \alpha_i)$ gilt stets $\mathfrak{a}_{\alpha_i} = \mathfrak{a}_i$.

LEMMA 8.30: Es sei $M = \sum_{i=1}^n \mathfrak{a}_i\alpha_i$ ein R-Modul und $\alpha = \sum_{i=1}^n r_i\alpha_i \in V$ beliebig. Dann gilt

$$\mathfrak{a}_\alpha = \bigcap_{i=1}^n \frac{\mathfrak{a}_i}{r_i}$$

wobei wir formal $\mathfrak{a}_i/0 = Q(R)$ setzen.

BEWEIS. Es gilt $x\alpha = \sum_{i=1}^n (xr_i)\alpha_i$ und $x\alpha \in M$ genau dann, wenn $xr_i \in \mathfrak{a}_i$ für jedes i gilt. Also $x \in \mathfrak{a}_i/r_i$. □

KOROLLAR 8.31: Es sei $x_1, \ldots, x_n$ eine Basis von $V := M \otimes Q(R)$. Dann gibt es eine *adaptierte Pseudobasis*, d.h. $M = \sum_{i=1}^n \mathfrak{a}_i\alpha_i$ mit $\alpha_i \in \langle x_1, \ldots, x_i \rangle$.

BEWEIS. Folgt direkt aus dem Beweis von 8.10. Eigentlich wollte ich es als Korollar anhängen, daß hätte aber die ganze Numerierung durcheinander gebracht. □

SATZ 8.32: Es seien $M = \sum_{i=1}^n \mathfrak{a}_i\alpha_i$ und $N = \sum_{i=1}^n \mathfrak{b}_i\beta_i$ zwei Moduln (von vollem Rang) (α_i, $\beta_i \in V$, $\mathfrak{a}_i$, $\mathfrak{b}_i$ Ideale in R, $M \otimes Q(R) = V$, $N \otimes Q(R) = V$) und $U = (u_{i,j}) \in Q(R)^{n\times n}$ mit $\sum_{i=1}^n u_{i,j}\beta_i = \alpha_j$.
Dann gilt $M \subseteq N$ genau dann, wenn $u_{i,j} \in \mathfrak{a}_i^{-1}\mathfrak{b}_j$, $M = N$ falls zusätzlich $\det U \prod_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{b}_i$ gilt.

BEWEIS. Es gilt $\mathfrak{a}_i\alpha_i \in M$ und $\sum_{j=1}^n u_{i,j}\mathfrak{a}_i\beta_j = \mathfrak{a}_i\alpha_i \subseteq M \subseteq N$, also $u_{i,j}\mathfrak{a}_i \subseteq \mathfrak{b}_j$. Aus der Definition der Determiante ($\det U = \sum_{\pi\in\mathfrak{S}_n} \operatorname{sign}(\pi) \prod_{i=1}^n u_{i,\pi(i)}$) folgt dann $\det U \prod_{i=1}^n \mathfrak{a}_i \subseteq \prod_{i=1}^n \mathfrak{b}_i$. Indem wir $N \subseteq M$ benutzen, folgt $=$.

Es gelte nun $\det U \prod_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{b}_i$ und $M \subseteq N$. Aus dem gezeigten folgt $u_{i,j} \in \mathfrak{b}_j\mathfrak{a}_i^{-1}$. Nach der Cramerschen Regel gilt $U^{-1} = (v_{i,j})_{i,j}$ mit $v_{i,j} = \det U_{i,j}/\det U$ wobei $U_{i,j}$ die Adjunkte ist (wir streichen in U die $j$te Zeile und die $i$te Spalte). Aus der Definition der Determinante folgt dann $\det U_{i,j} \in \prod_{l\neq j} \mathfrak{a}_l^{-1} \prod_{l\neq i} \mathfrak{b}_l$ und $v_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$. Damit erhalten wir $N \subseteq M$. □

LEMMA 8.33: Es seien $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ Ideale und $a \in Q(R)$ mit $\mathfrak{ab} = a\mathfrak{cd}$. Dann gilt (als R-Modul):

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{c} \oplus \mathfrak{d}$$

bzw. für $M = \mathfrak{a}\alpha + \mathfrak{b}\beta \subseteq V$ existieren γ, $\delta \in V$ mit $M = \mathfrak{c}\gamma + \mathfrak{d}\delta$.

BEWEIS. Es sei $M = \mathfrak{a}\alpha + \mathfrak{b}\beta \subseteq V$. Nach 8.27 können wir x_1, y_1 mit $\mathfrak{c}^{-1} = x_1\mathfrak{a}^{-1} + y_1\mathfrak{b}^{-1}$ finden. Definiere $\gamma := x_1\alpha + x_2\beta$. Nach 8.30 und 8.25.(6) gilt $\mathfrak{a}_\gamma = \mathfrak{a}/x_1 \cap \mathfrak{b}/x_2 = (x_1\mathfrak{a}^{-1} + x_2\mathfrak{b}^{-1})^{-1} = \mathfrak{c}$. Nun ergänzen wir γ mit δ_2 zu einer $Q(R)$ Basis von $M \otimes Q(R)$. Nach 8.31 gibt es hierzu eine adaptierte Pseudobasis $\gamma_1\mathfrak{c}_1 + \delta_1\mathfrak{d}_1$ mit $\gamma_1 = x\gamma$ und daher $\mathfrak{c}_1 = \mathfrak{c}/x$. Also erhalten wir eine Pseudobasis in der Form $\gamma\mathfrak{c} + \delta_1\mathfrak{d}_1$. Nach 8.32 existiert dann $y \in Q(R)$ mit $\mathfrak{d}_1\mathfrak{c} = y\mathfrak{dc}$. Mit $\delta := \delta_1/y$ folgt dann die Behauptung. □

KOROLLAR 8.34: Es sei $M = \sum_{i=1}^n \mathfrak{a}_i\alpha_i$ ein Modul, $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ Ideale und $\gamma \in Q(R)$ mit $\prod_{i=1}^n \mathfrak{a}_i = \gamma \prod_{i=1}^n \mathfrak{b}_i$. Dann gibt es Elemente $\beta_i \in V$ mit $M = \sum_{i=1}^n \mathfrak{b}_i\beta_i$.

BEWEIS. Übung. □

Speziell für $\mathfrak{b}_1 = \cdots = \mathfrak{b}_{n-1} = R$ und $\mathfrak{b}_n = \prod_{i=1}^n \mathfrak{a}_i$ folgt also $M \cong R^{n-1} \oplus \mathfrak{b}_n$. Einen Darstellung von dieser Form heißt auch *fast freie Darstellung* (eng. almost free representation).

KOROLLAR 8.35: Zwei torsionsfreie Moduln von gleichem Rang sind genau dann isomorph, wenn die Ideale in der gleichen Klasse $\bmod P_R$ liegen. Diese Klasse heißt *Steinitz-Klasse von M*, $\operatorname{St}(M)$.

BEWEIS. O.b.d.A. können wir $M \otimes_R Q(R) = N \otimes_R Q(R) = V$ annehmen. Es seien $M = \sum_{i=1}^n \mathfrak{a}_i\alpha_i$ und $N = \sum_{i=1}^n \mathfrak{b}_i\beta_i$ beliebige Pseudobasen. Wegen $\prod_{i=1}^n \mathfrak{a}_i = \gamma \prod_{i=1}^n \mathfrak{b}_i$ gibt es nach 8.34 Elemente $\tilde{\beta}_i$ mit $N = \sum_{i=1}^n \mathfrak{a}_i\tilde{\beta}_i$. Den Isomorphismus erhalten wir nun mittels $\alpha_i \mapsto \tilde{\beta}_i$. □

SATZ 8.36: Es sei M ein endlich erzeugter R-Modul über einem Dedekind Ring. Dann gilt $M \cong \operatorname{Tor}(M) \oplus R^k \oplus \mathfrak{a}$ mit $k \in \mathbb{N}_0$ und einem Ideal $\mathfrak{a}$.

BEWEIS. Wir haben folgende exakte Sequenz:

$$0 \to \operatorname{Tor}(M) \to M \to M/\operatorname{Tor}(M) \to 0$$

wobei $M/\operatorname{Tor}(M)$ endlich erzeugt und torsionsfrei ist (5.10). Nach 8.2.(5) gilt daher $M \cong \operatorname{Tor}(M) \oplus M/\operatorname{Tor}(M)$ und mit 8.10 folgt $M \cong \operatorname{Tor}(M) \oplus \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ für Ideale $\mathfrak{a}_i$. Mit 8.33 folgt dann die Behauptung. □

Nun wollen wir noch den Torsionsteil genauer Untersuchen und eine Verallgemeinerung der Smith-Normal-Form erhalten. Dazu werden wir uns näher mit den Pseudobasen beschäftigen.

LEMMA 8.37: Es seien $\mathfrak{a}$, $\mathfrak{b}$ Ideale, α, $\beta \in Q(R)$, α und β nicht beide 0. Setze $\mathfrak{c} := \alpha\mathfrak{a} + \beta\mathfrak{b}$. Dann gibt es $u \in \mathfrak{a}\mathfrak{c}^{-1}$ und $v \in \mathfrak{b}\mathfrak{c}^{-1}$ mit $\alpha u + \beta v = 1$.

BEWEIS. Falls $\alpha = 0$ gilt, so funktioniert $u := 0$, $v := 1/\beta$, $\beta = 0$ analog. Sei nun also $\alpha\beta \neq 0$. $\mathfrak{a}_1 := \alpha\mathfrak{a}\mathfrak{c}^{-1}$ $\mathfrak{b}_1 := \beta\mathfrak{b}\mathfrak{c}^{-1}$. Wegen $\mathfrak{d} = \mathrm{ggT}(\alpha\mathfrak{a}, \beta\mathfrak{b})$ sind $\mathfrak{a}_1$ und $\mathfrak{b}_1$ ganze Ideale mit $\mathfrak{a}_1 + \mathfrak{b}_1 = R$. Also gibt es $e \in \mathfrak{a}_1$ und $f \in \mathfrak{c}_1$ mit $e + f = 1$. $u := e/\alpha$ und $v := f/\beta$ sind dann Lösungen. □

SATZ 8.38: Es sei

$$M := \begin{pmatrix} \mathfrak{a} & \mathfrak{b} \\ a & b \\ c & d \end{pmatrix}$$

ein R-Modul vom Rang 2. Dann gibt es eine Matrix $T \in Q(R)^{2\times 2}$ mit $MT = M$ wobei TM eine Pseudobasis der Form

$$\begin{pmatrix} \mathfrak{c} & \mathfrak{d} \\ 1 & 0 \\ * & * \end{pmatrix}$$

hat, mit $\mathfrak{d} = a\mathfrak{a} + b\mathfrak{b}$ und $\mathfrak{d} = \mathfrak{a}\mathfrak{b}\mathfrak{c}^{-1}$, $\det T = 1$.

BEWEIS. Wende 8.37 an und erhalte $u \in a\mathfrak{a}\mathfrak{c}^{-1}$, $v \in b\mathfrak{b}\mathfrak{c}^{-1}$. Setze $T := \begin{pmatrix} u & -b \\ v & a \end{pmatrix}$. Dann gilt (für die Matrizen)

$$MT = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} u & -b \\ v & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ cu + dv & -cb + ad \end{pmatrix}$$

Wegen $u \in \mathfrak{a}\mathfrak{c}^{-a}$, $v \in \mathfrak{b}\mathfrak{c}^{-1}$ und $b \in \mathfrak{a}\mathfrak{d}^{-1} = \mathfrak{a}\mathfrak{c}(\mathfrak{a}\mathfrak{b})^{-1} = \mathfrak{c}\mathfrak{b}^{-1} = (a\mathfrak{a} + b\mathfrak{b})\mathfrak{b}^{-1} = a\mathfrak{a}\mathfrak{b}^{-1} + bR$ und (analog) $a \in \mathfrak{b}\mathfrak{d}^{-1}$ folgt mit 8.32 (für die Moduln) $M = MT$. □

KOROLLAR 8.39: Eine Pseudobasis $\begin{pmatrix} \mathfrak{a} & \mathfrak{b} \\ 1 & a \\ b & c \end{pmatrix}$ mit $\mathfrak{a} \mid a\mathfrak{b}$ kann unimodular in eine Pseudobasis $\begin{pmatrix} \mathfrak{a} & \mathfrak{b} \\ 1 & 0 \\ b & d \end{pmatrix}$ transformiert werden.

BEWEIS. In 8.37 kann $u = 1$, $v = 0$ gewählt werden. □

KOROLLAR 8.40: Zu Paaren $(\mathfrak{a}_i, \alpha_i) \in I_r \times Q(r)^m$ $(1 \leq i \leq n)$ von Idealen und Elementen gibt es eine Matrix $T \in Q(R)^{n\times n}$ mit $\det T = 1$ so, daß für $(\beta_1, \ldots, \beta_m) := (\alpha_1, \ldots, \alpha_m)T$ und $\mathfrak{b}_i := \mathfrak{a}_{\beta_i}$ (für $M = \sum_{i=1}^m \alpha_i\mathfrak{a}_i$) gilt:
(1) $\mathfrak{b}_1 = \mathrm{ggT}(\alpha_{1,i}\mathfrak{a}_i \mid 1 \leq i \leq m)$
(2) $M = \sum_{i=1}^m \mathfrak{b}_i\beta_i$
(3) $\beta_{1,1} = 1$, $\beta_{1,i} = 0$ $(2 \leq i \leq m)$

Dies liefert dann einen „konstruktiven“ Beweis für 8.10 und 8.31 – falls 8.37 „konstruktiv“ ist. Damit erhalten wir eine „Smith Normalform“ (Elementarteiler Normalform) für Moduln über Dedekind Ringen:

SATZ 8.41 (Elementarteiler Normalform): Es seien M und N R-Modul vom Rang n. Dann gibt es eine Basis $\omega_1, \dots, \omega_n$ von V, sowie Ideale $\mathfrak{c}_i$ und $\mathfrak{d}_i$ mit $M = \sum_{i=1}^n \mathfrak{c}_1\omega_i$, $N = \sum_{i=1} \mathfrak{c}_i\mathfrak{d}_i\omega_i$ und $\mathfrak{d}_1 \mid \mathfrak{d}_2 \mid \dots \mathfrak{d}_n$.
Falls $N \subseteq M$ gilt, so erhalten wir $\mathfrak{d}_1 \subseteq R$. $M/N \cong \oplus_{i=1}^n R/\mathfrak{d}_i$.

BEWEIS. Wir haben Pseudobasen $(\mathfrak{a}_i, \alpha_i)$ von M und $(\mathfrak{b}_i, \beta_i)$ von N. In dem wir (wenn nötig) N durch aN ersetzen, können wir $N \subseteq M$ annehmen.

Da die Moduln beide vollen Rang haben gibt es eine Matrix $T \in Q(R)^{n\times n}$ mit $(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)T$. Die Spalten von T seien $t_1, \dots, t_m$, die Zeilen $s_1, \dots, s_n$. Nach 8.32 gilt nun $t_{i,j} \in \mathfrak{a}_j^{-1}\mathfrak{b}_i$.

Per Induktion beweisen wir zunächst: Es gibt Pseudobasen $(\tilde{\mathfrak{a}}_i, \tilde{\omega}_i)$ von M und $(\tilde{\mathfrak{b}}_i, \tilde{\omega}_i)$ von N ($\Rightarrow T = \mathrm{id}$!): $n = 1$: klar.

$n \mapsto n + 1$: Für den Modul mit der Pseudobasis $\begin{pmatrix} \mathfrak{a}_1 & \dots & \mathfrak{a}_n \\ t_1 & \dots & t_n \end{pmatrix}$ gibt es nach 8.40 eine unimodulare Spaltentransformation U auf eine Pseudobasis der Form $\begin{pmatrix} \mathfrak{a}'_1 & \mathfrak{a}'_2 & \dots & \mathfrak{a}'_n \\ 1 & 0 & \dots & 0 \\ * & * & \dots & * \end{pmatrix}$ mit $\mathfrak{a}'_1 = \sum_{i=1}^n \mathfrak{a}_i t_{1,i}$. Zusätzlich gilt $MU = M$.

Für den Modul $\begin{pmatrix} \mathfrak{b}_1^{-1} & s_1 \\ \vdots & \vdots \\ \mathfrak{b}_n^{-1} & s_n \end{pmatrix}$ (s_i sind die Zeilen der neuen Matrix!) erhalten wir mit 8.40 nun eine unimodulare Zeilentransformation V auf eine Pseudobasis der Form $\begin{pmatrix} {\mathfrak{b}'_1}^{-1} & 1 & * \\ {\mathfrak{b}'_2}^{-1} & 0 & * \\ \vdots & \vdots & \vdots \\ {\mathfrak{b}'_n}^{-1} & 0 & * \end{pmatrix}$ wobei ${\mathfrak{b}'_1}^{-1} = \sum_{i=1}^n {\mathfrak{b}_i}^{-1} s_{i,1}$ ist. Hier gilt nun $NV^{-1} = N$. Da wir N und M nicht geändert haben, gilt nun $1 \in {\mathfrak{b}'_1}^{-1}\mathfrak{a}'_1$ also ${\mathfrak{b}'_1}^{-1}\mathfrak{a}'_1$ ist ein ganzes Ideal.

Das Tripel $(t_{1,1}, \mathfrak{a}_1, \mathfrak{b}_1^{-1})$ wird in ein Tripel $(1, \mathfrak{a}'_1, {\mathfrak{b}'_1}^{-1})$ überführt. Es gilt

$$\mathfrak{a}'_1 = \sum_{i=1}^n \mathfrak{a}_i t_{1,i} = \mathfrak{a}_1 t_{1,1} + \sum_{i=2}^n \mathfrak{a}_i t_{1,i}$$

und

$${\mathfrak{b}'_1}^{-1} = \sum_{i=1}^n {\mathfrak{b}_i}^{-1} t_{i,1} = {\mathfrak{b}_1}^{-1} t_{1,1} + \sum_{i=2}^n {\mathfrak{b}_i}^{-1} t_{t,1}$$

Nun iterieren wir die beiden Schritte.

Da nach dem 1. Durchlauf $t_{1,1} = s_{1,1} = 1$ gilt, werden also $\mathfrak{a}_1$, $\mathfrak{b}_1^{-1}$ und $\mathfrak{a}_1{\mathfrak{b}'_1}^{-1}$ jedesmal größer. Wegen $1 = t_{1,1} \in \mathfrak{a}_1^{-1}\mathfrak{b}_1$ gilt $\mathfrak{a}_1\mathfrak{b}_1^{-1} \subseteq R$, also kann das Produkt nur endlich oft wachsen (größer werden heißt teilen!), nach endlich vielen Schritten

bleiben also sowohl $\mathfrak{a}_1$ als auch $\mathfrak{b}_1$ invariant. Nach 8.39 erhalten wir damit T in der Form $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \dots & * \end{pmatrix}$.

Auf den verbleibenden Modul können wir nun die Induktionsvoraussetzung anwenden und erhalten $T = \mathrm{id}$.

Als nächstes werden wir $\mathfrak{a}_1\mathfrak{b}_1^{-1} \mid \mathfrak{a}_2\mathfrak{b}_2^{-1}$ erreichen, sei also ein System

$$\begin{pmatrix} & \mathfrak{a}_1 & \mathfrak{a}_2 \\ \mathfrak{b}_1^{-1} & 1 & 0 \\ \mathfrak{b}_2^{-1} & 0 & * \end{pmatrix}$$

mit $\mathfrak{a}_i\mathfrak{b}_i^{-1} \subseteq R$ gegeben. Falls $\mathfrak{a}_1 \not\supseteq \mathfrak{a}_2$, wende 8.33 an um eine Spaltentransformation auf die Form

$$\begin{pmatrix} & \mathfrak{a}_1 + \mathfrak{a}_2 & \mathfrak{a}_1 \cap \mathfrak{a}_2 \\ \mathfrak{b}_1^{-1} & * & * \\ \mathfrak{b}_2^{-1} & * & * \end{pmatrix}$$

zu erhalten. Indem wir nun das oben gezeigte auf das neue System anwenden (wobei wir mit Zeilentransformation anfangen!) erhalten wir

$$\begin{pmatrix} & \mathfrak{a}_1' & \mathfrak{a}_2' \\ \mathfrak{b}_1'^{-1} & 1 & 0 \\ \mathfrak{b}_2'^{-1} & 0 & * \end{pmatrix}$$

(durch Zeilen- und Spaltentransformationen). Ferner gilt $\mathfrak{a}_1' \supseteq \mathfrak{a}_1$ und (wegen $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1'\mathfrak{a}_2'$, $\mathfrak{a}_1' \supseteq \mathfrak{a}_1 + \mathfrak{a}_2$) $\mathfrak{a}_1' \supseteq \mathfrak{a}_2'$.

Indem wir dies nun auch für die Zeilen durchführen erhalten wir ein System

$$\begin{pmatrix} & \mathfrak{a}_1'' & \mathfrak{a}_2'' \\ \mathfrak{b}_1''^{-1} & 1 & 0 \\ \mathfrak{b}_2''^{-1} & 0 & * \end{pmatrix}$$

mit $\mathfrak{a}_1'' \supseteq \mathfrak{a}_2''$, $\mathfrak{b}_1''^{-1} \supseteq \mathfrak{b}_2''^{-1}$ und daher $\mathfrak{a}_1''\mathfrak{b}_1''^{-1} \mid \mathfrak{a}_2''\mathfrak{b}_2''^{-1}$.

Induktiv erhalten wir nun die Teilbarkeitsbedingung überall.

$M/N \cong \prod_{i=1}^n \mathfrak{c}_i/\mathfrak{c}_i\mathfrak{d}_i \cong \prod_{i=1}^n R/\mathfrak{d}_i$ ist offensichtlich korrekt (mit 8.46). □

DEFINITION 8.42: Die Ideale $\mathfrak{d}_1$ aus 8.41 heißen *Elementarteiler* von M.
$\mathrm{ord}_R(M) := \mathrm{ord}(M) := \prod_{i=1}^n \mathfrak{d}_i$ heißt *Ordnungsideal* von M.
Für nicht Torsionsmoduln definieren wir $\mathrm{ord}(M) = (0)$.
Für einen torsionsfreien Modul $M = \sum_{i=1}^n \mathfrak{a}_i\alpha_i$ definieren wir die *Moduldeterminante* $d_M := \det A \prod_{i=1}^n \mathfrak{a}_i$ wo $A = (\alpha_1, \dots, \alpha_n) \in Q(R)^{n\times n}$ ist.

8.32 zeigt, daß die Moduldeterminante wohldefiniert ist. Es gilt $\mathrm{Ann}(M) = \mathfrak{d}_n$. Für $R = \mathbb{Z}$ gilt $\mathrm{ord}(M) = (\#M)$. 8.41 zeigt

$$\mathrm{ord}(M/N) = d_N d_M^{-1}.$$

Als nächstes wollen wir (wie in 5.43) eine Eindeutigkeit zeigen. Dazu benötigen wir jedoch noch weitere Hilfsmittel.

LEMMA 8.43: Es sei $\begin{pmatrix} & \mathfrak{a}_1 & \mathfrak{a}_2 \\ \mathfrak{b}_1^{-1} & a_{1,1} & a_{1,2} \\ \mathfrak{b}_2^{-1} & a_{2,1} & a_{2,2} \end{pmatrix}$ ein System wie in 8.41. Für Transformationen U, V mit $MU = M$ und $NV^{-1} = N$ auf ein System $\begin{pmatrix} & \mathfrak{a}_1 & \mathfrak{a}_2 \\ \mathfrak{b}_1'^{-1} & a'_{1,1} & a'_{1,2} \\ \mathfrak{b}_2'^{-1} & a'_{2,1} & a'_{2,2} \end{pmatrix}$ gilt dann

$$\sum_{i,j} a_{j,i}\mathfrak{a}_i\mathfrak{b}_j^{-1} = \sum_{i,j} a'_{j,i}\mathfrak{a}'_i\mathfrak{b}'^{-1}_j$$

BEWEIS. Wir untersuchen die Auswirkungen der Elementartransformationen einzeln:

- Skalieren (mult. mit $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$). Für die Ideale heißt das: $(\mathfrak{a}_1, \mathfrak{a}_2) \mapsto (\mathfrak{a}_1/\lambda, \mathfrak{a}_2)$, die $\mathfrak{b}_i$ bleiben ungeändert. In der Summe: $a_{1,1}\lambda\mathfrak{a}_1/\lambda\mathfrak{b}_1 + a_{2,1}\lambda\mathfrak{a}_1/\lambda\mathfrak{b}_2 + a_{1,2}\lambda\mathfrak{a}_2\mathfrak{b}_1 + a_{2,2}\lambda\mathfrak{a}_2\mathfrak{b}_2$ ändert sich daher nichts.
- Multiplikation mit $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ ändert die $\mathfrak{a}_i$ $\mathfrak{b}_i$ nicht (falls λ korrekt gewählt ist!). Für die Summe gilt: $a_{1,1}\lambda\mathfrak{a}_1/\lambda\mathfrak{b}_1 + a_{2,1}\lambda\mathfrak{a}_1/\lambda\mathfrak{b}_2 + (a_{1,2} + \lambda a_{1,1})\mathfrak{a}_2\mathfrak{b}_1 + (a_{2,2} + \lambda a_{2,1})\mathfrak{a}_2\mathfrak{b}_2$. Wegen $\lambda \in \mathfrak{a}_2^{-1}\mathfrak{b}_1$ ändert sich daher nichts.

□

LEMMA 8.44: Es sei M ein $n \times n$-System wie in 8.41. Für $m \leq n$ definieren wir ein System $N := (T_{a,b}, \mathfrak{a}_a, \mathfrak{b}_b^{-1})$, $a, b \subseteq \{1, \ldots, n\}$, $\#a = \#b = m$, $T_{a,b} := \det M_{a,b}$ wo $M_{a,b}$ durch Streichen aller Zeilen $i \notin a$ und aller Spalte $j \notin b$ entsteht.
Dann gilt: Jede Spaltentransformation U die den von M erzeugten Spaltenmodul invariant läßt ändert auch den von N erzugten Spaltenmodul nicht (analoges gilt auch für den Zeilenmodul).

BEWEIS. Jede Transformation von M kann aus Elementartransformationen zusammengesetzt werden:

(1) Vertauschen zweier Spalten
(2) Skalieren einer Spalte
(3) Addition eines Vielfachen einer Spalte zu einer anderen.

Vertauschen von 2 Spalten (i, j) führt zur paarweisen Vertauschung von allen Spalten von N die genau einen Index enthalten. Spalten von N die weder i noch j enthalten ändern sich gar nicht, Spalten die beide enthalten ändern ihr Vorzeichen.

Skalieren einer Spalte i (d.h. $\mathfrak{a}_i \mapsto \lambda\mathfrak{a}_i$, $M_{j,i} \mapsto \lambda M_{j,i}$ $(1 \leq j \leq n)$) skaliert in N alle Spalten die i enthalten.

Die 3. Transformation geht analog: $T_{a,b}$ mit $i, j \notin a$ bleiben invariant, $i, j \notin a$ bleiben ebenfalls invariant. (In beiden Fallen ist die Transformationen eine Elementartransformation für $M_{a,b}$ mit den entsprechenden Idealen $\mathfrak{a}_l$, $l \in a$). Andernfalls gilt $T_{a,b} \mapsto T_{a,b} + \lambda T_{a\setminus\{i\}\cup\{j\},b}$ was eine gültige Transformation für den großen Modul darstellt. □

SATZ 8.45: Die Ideale $\mathfrak{d}_i$ aus 8.41 sind eindeutig bestimmt. Es gilt $\prod_{j=1}^{i}\mathfrak{d}_j = \sum_{a,b}\mathfrak{a}_a\mathfrak{b}_b^{-1}T_{a,b}$ mit $T_{a,b}$ wie oben.

BEWEIS. Nach 8.43 ist die Summe (= ggT) eine Modul-Invariante. Nach 8.44 lassen alle Transformationen die in 8.41 passieren den Modul N invariant, also auch die Summe. □

Alternativ können wir die Eindeutigkeit auch so zeigen: Es sei $M/N \cong \oplus_{i=1}^{n} R/\mathfrak{d}_i \cong \oplus_{i=1}^{m} R/\mathfrak{c}_i$ mit $\mathfrak{d}_1 \mid \mathfrak{d}_2 \mid \cdots \mid \mathfrak{d}_n$ und $\mathfrak{c}_1 \mid \mathfrak{c}_2 \mid \cdots \mid \mathfrak{c}_m$ wegen $\mathfrak{d}_n = \mathrm{Ann}(M/N) = \mathfrak{c}_m$ folgt $\mathfrak{d}_n = \mathfrak{c}_m$. Also gilt $(M/N)/(0,\ldots,1)\mathfrak{d}_n \cong \oplus_{i=1}^{n-1} R/\mathfrak{d}_i \cong \oplus_{i=1}^{m-1} R/\mathfrak{c}_i$. Induktiv folgt nun die Eindeutigkeit.

SATZ 8.46: $R/\mathfrak{b} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b}$ für $\mathfrak{b}$ ganz und $\mathfrak{a}$ beliebig.

BEWEIS. Zunächst sei $\mathfrak{a}$ ebenfalls ganz.

Wir zeigen: $R\mathfrak{b} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b}$ mittels $x \mapsto xr$. Nach 8.26 existiert ein $r \in K$ mit $v_\mathfrak{p}(r) = v_\mathfrak{p}(\mathfrak{a})$ für $v_\mathfrak{p}(\mathfrak{a}) \neq 0$, $= 0$ für alle Primideale die $\mathfrak{b}$ aber nicht $\mathfrak{a}$ teilen und ≥ 0 sonst. Damit folgt $Rr \subseteq \mathfrak{a}$ und die Abbildung ist wohldefiniert. $rx \in \mathfrak{a}\mathfrak{b} \iff v_\mathfrak{p}(rx) \geq v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})$ also $x \in \mathfrak{b}$.

Nun die Surjektivität: Es sei $y \in \mathfrak{a}/\mathfrak{a}\mathfrak{b}$ gegeben. Mit dem Approximationssatz finden wir ein z mit $v_\mathfrak{p}(z) = v_\mathfrak{p}(\mathfrak{a}\mathfrak{b})$ bzw. $v_\mathfrak{p}(z) = v_\mathfrak{p}(r)$ sonst. Dann gilt $y + z = y$ und $(y + z/r)$ ist ganz.

Finde $z \equiv 0 \bmod \mathfrak{a}\mathfrak{b}$ und $z \equiv y \bmod \mathfrak{c}$ wo $\mathfrak{c} := (r)\,\mathrm{ggT}((r), \mathfrak{a}\mathfrak{b})^{-1}$. Dann gilt $y - z \equiv y$ und $(y - z)/r$ ist ganz.

Es sei nun $\mathfrak{a}$ beliebig. Dann gibt es $a \in R$ mit $a\mathfrak{a} \subseteq R$. Dann gilt $R/\mathfrak{b} \cong a\mathfrak{a}/a\mathfrak{a}\mathfrak{b} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b}$ mittels $\mathfrak{a} \cong a\mathfrak{a}$. □

DEFINITION 8.47: Es sei R ein Dedekind Ring, $L/Q(R)$ eine endliche Körpererweiterung und $S := \mathrm{Cl}(R, L)$. Für ein ganzes Ideal $\mathfrak{a}$ von S definieren wir $N_{L/Q(R)}(\mathfrak{a}) = \mathrm{ord}(S/\mathfrak{a})$ als die Relativnorm von $\mathfrak{a}$.

BEMERKUNG 8.48: (1) Es gilt $N_{K/\mathbb{Q}}(\mathfrak{a}) = N(\mathfrak{a})\mathbb{Z}$ für Erweiterungen K von $\mathbb{Q}$.

(2) $N_{L/Q(R)}(\mathfrak{a}\mathfrak{b}) = N_{L/Q(R)}(\mathfrak{a})N_{L/Q(R)}(\mathfrak{b})$, denn $N_{L/Q(R)}(\mathfrak{a}) = d_\mathfrak{a}d_S^{-1}$, $N_{L/Q(R)}(\mathfrak{b}) = d_\mathfrak{b}d_S^{-1}$, und $N_{L/Q(R)}(\mathfrak{a}\mathfrak{b}) = d_{\mathfrak{a}\mathfrak{b}}d_S^{-1}$. Nach 8.46 folgt $\mathfrak{a}/\mathfrak{a}\mathfrak{b} \cong S/\mathfrak{b}$, also $d_{\mathfrak{a}\mathfrak{b}}d_\mathfrak{a}^{-1} = \mathrm{ord}(\mathfrak{a}/\mathfrak{b}\mathfrak{a}) = \mathrm{ord}(S/\mathfrak{b}) = d_\mathfrak{b}d_S^{-1}$. Nun gilt $N_{L/Q(R)}(\mathfrak{a}\mathfrak{b}) = d_{\mathfrak{a}\mathfrak{b}}d_S^{-1} = d_\mathfrak{a}d_\mathfrak{b}d_S^{-2} = N_{L/Q(R)}(\mathfrak{a})N_{L/Q(R)}(\mathfrak{b})$.

3. Klassengruppe

In diesem Kapitel sei F stets ein algebraischer Zahlkörper. Die Gruppe der gebrochenen Ideale von $\mathbb{Z}_F = \mathrm{Cl}(\mathbb{Z}, F)$ bezeichnen wir mit I_F, die der gebrochenen Hauptideale mit P_F. Die Faktorgruppe $I_F/P_F := \mathrm{Cl}_F$ heißt die Klassengruppe von F. Ihre Ordnung $\#I_F/P_F$ ist die Klassenzahl h_F von F.

Für einen Modul $\sum_{i=1}^n \omega_i \mathfrak{a}_i =: M \subseteq F/K$ ist $d(M) := \det(\mathrm{Tr}(\omega_i\omega_j))_{i,j} \prod_{i=1}^n \mathfrak{a}_i^2$ die sog. *Moduldiskriminante*. Analog zu der Bemerkung nach Definition 3.22 folgt, dass die Diskriminante modulo Quadraten (von Hauptidealen) eindeutig bestimmt ist.

Nach Blatt 8 sind $\mathbb{Z}_F$ und jedes Ideal $\mathfrak{a}$ freie $\mathbb{Z}$-Moduln vom Rang $n = [F : \mathbb{Q}]$. Mit $d(\mathbb{Z}_F)$ bzw. $d(\mathfrak{a})$ bezeichnen wir einen Erzeuger der Moduldiskriminante $d(\mathbb{Z}_F)$ bzw. $d(\mathfrak{a})$.

Wie in Blatt 11 fixieren wir das folgende: Es gelte $F = \mathbb{Q}(\alpha)$ mit $f(\alpha) = 0$ für ein normiertes irreduzibles $f \in \mathbb{Z}[x]$. In $\mathbb{C}$ gilt $f = \prod(x - \alpha^{(i)})$. Dann ist $(.)^{(i)} : k \to \mathbb{C} : \sum_{j=1}^n r_j\alpha^{j-1} \mapsto \sum_{j=1}^n r_j(\alpha^{(i)})^{j-1}$ ein Körpermonomorphismus. Wir fixieren eine Sortierung der Nullstellen. Wir nehmen an, daß $\alpha^{(1)}, \ldots, \alpha^{(r_1)} \in \mathbb{R}$ und $\alpha^{(r_1+1)} = \bar{\alpha}^{(r_1+r_2+1)}, \ldots, \alpha^{(r_1+r_2)} = \bar{\alpha}^{(r_1+2r_2)} \in \mathbb{C} \setminus \mathbb{R}$ gelte.

Es sei nun $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}_F$. Wir definieren $\Psi : \mathbb{Z}_F \to \mathbb{R}^n$ mittels

$$\omega_i \mapsto (b_{i,j})_j := (\begin{cases} \omega_i^{(j)} & 1 \le j \le r_1 \\ \Re\omega_i^{(j)} & r_1 < j \le r_1 + r_2 \\ \Im\omega_i^{(j-r_2)} & \end{cases})_j$$

Mit $\Omega := (\Psi(\omega_1), \ldots, \Psi(\omega_n))$ und $T := \mathrm{diag}(I_{r_1}, \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \ldots, \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix})$ folgt $d(\mathbb{Z}_F)^2 = (T\Omega)^t(\Omega T)$. Für das von den Spalten von Ω aufgespannte Gitter Λ folgt daher $d_\Lambda^2 = 2^{2r_2} d(\mathbb{Z}_F)$.

LEMMA 8.49: Seien $\lambda \in \mathbb{R}^{\ge 0}, n \in \mathbb{N}$ und $r, s \in \mathbb{Z}^{\ge 0}$ mit $n = r + 2s$. Dann ist die Menge

$$C_{r,s}(\lambda) := \left\{ x \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^r |x_i| + 2\sum_{i=1}^s \sqrt{x_{i+r}^2 + x_{i+r+s}^2} \le \lambda \right\}$$

konvex, kompakt und ursprungssymmetrisch. Es gilt

$$\mathrm{Vol}(C_{r,s}(\lambda)) = \lambda^n \frac{2^r}{n!} \left(\frac{\pi}{2}\right)^s.$$

BEWEIS. Zu zeigen ist nur die Aussage über das Volumen. Wegen $C_{r,s}(\lambda) = \lambda \cdot C_{r,s}(1)$ gilt

$$\mathrm{Vol}(C_{r,s}(\lambda)) = \lambda^n \,\mathrm{Vol}(C_{r,s}(1)).$$

Für $r > 0$ und $r - 1 + 2s > 0$ erhält man aus dem Prinzip von Cavalieri

$$\begin{aligned} \mathrm{Vol}(C_{r,s}(1)) &= \int_{-1}^1 \mathrm{Vol}(C_{r-1,s}(1 - |x|))\, dx = 2\int_0^1 \mathrm{Vol}(C_{r-1,s}(1 - x))\, dx \\ &= 2 \cdot \mathrm{Vol}(C_{r-1,s}(1)) \int_0^1 (1 - x)^{n-1}\, dx = \frac{2}{n} \mathrm{Vol}(C_{r-1,s}(1)). \end{aligned}$$

Trivialerweise gelten $\mathrm{Vol}(C_{1,0}(1)) = 2$ und $\mathrm{Vol}(C_{0,1}(1)) = \frac{\pi}{4}$. Ist $s > 1$, so folgt durch Übergang zu Polarkoordinaten

$$\begin{aligned}
\mathrm{Vol}(C_{0,s}(1)) &= \iint_{x^2+y^2 \le \frac{1}{4}} \mathrm{Vol}(C_{0,s-1}(1 - 2\sqrt{x^2+y^2}))\, dx\, dy \\
&= 2\pi \int_0^{\frac{1}{2}} r \cdot \mathrm{Vol}(C_{0,s-1}(1-2r))\, dr \\
&= 2\pi \cdot \mathrm{Vol}(C_{0,s-1}(1)) \int_0^{\frac{1}{2}} r(1-2r)^{2(s-1)}\, dr \\
&= \frac{\pi}{2} \frac{\mathrm{Vol}(C_{0,s-1}(1))}{(2s)(2s-1)}.
\end{aligned}$$

Damit ergibt sich

$$\begin{aligned}
\mathrm{Vol}(C_{r,s}(\lambda)) &= \lambda^n \mathrm{Vol}(C_{r,s}(1)) \\
&= \lambda^n \frac{2}{n} \cdot \ldots \cdot \frac{2}{n-r+1} \mathrm{Vol}(C_{0,s}(1)) \\
&= \lambda^n \frac{2^r (n-r)!}{n!} \left(\frac{\pi}{2}\right)^{s-1} \frac{2}{(2s)!} \frac{\pi}{4} \\
&= \lambda^n \frac{2^r}{n!} \left(\frac{\pi}{2}\right)^s.
\end{aligned}$$

□

Satz 8.50: Sei $\mathfrak{a}$ ein Ideal $\neq \{0\}$ in $\mathbb{Z}_F$. Dann enthält $\mathfrak{a}$ ein Element $\alpha \neq 0$ mit

$$|N(\alpha)| \le \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} N(\mathfrak{a}) \sqrt{|d(\mathbb{Z}_F)|}.$$

Beweis. $\Psi(\mathfrak{a})$ (Ψ wie oben (Blatt 11)) ist ein n–dimensionales Gitter im $\mathbb{R}^n$, und es gilt

$$d(\Psi(\mathfrak{a})) = \frac{1}{2^{r_2}} N(\mathfrak{a}) \sqrt{|d(\mathbb{Z}_F)|}.$$

Bestimme nun $\lambda \in \mathbb{R}^{>0}$ mit

$$\lambda^n = n! \left(\frac{4}{\pi}\right)^{r_2} N(\mathfrak{a}) \sqrt{|d(\mathbb{Z}_F)|}$$

$\Rightarrow \mathrm{Vol}(C_{r_1,r_2}(\lambda)) = 2^n d(\Psi(\mathfrak{a}))$ nach Lemma 8.49. Gemäß dem Minkowskischen Gitterpunktsatz enthält $C_{r_1,r_2}(\lambda)$ einen nicht–trivialen Gitterpunkt $\underline{x} \in \Psi(\mathfrak{a})$. Setze $x := \Psi^{-1}(\underline{x})$. Aus der Ungleichung zwischen arithmetischem und geometrischem Mittel folgt dann

$$\begin{aligned}
|N(x)|^{\frac{1}{n}} = \left(\prod_{i=1}^n |x^{(i)}|\right)^{\frac{1}{n}} &\le \frac{1}{n} \left(\sum_{i=1}^{r_1} |x^{(i)}| + 2 \sum_{\substack{i=r_1+1 \\ i-r_1 \equiv 1 \bmod 2}}^{n} |x^{(i)}| \right) \\
&= \frac{1}{n} \left(\sum_{i=1}^{r_1} |x_i| + 2 \sum_{\substack{i=r_1+1 \\ i-r_1 \equiv 1 \bmod 2}}^{n} \sqrt{x_i^2 + x_{i+1}^2} \right) \le \frac{\lambda}{n}
\end{aligned}$$

$\Rightarrow$ Behauptung. □

Satz 8.51: Jede Idealklasse von I_F/P_F enthält ein Ideal $\mathfrak{a}$ in $\mathbb{Z}_F$ mit

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d(\mathbb{Z}_F)|} =: M_F.$$

M_F heißt die Minkowski-Konstante von F.

Beweis. Sei C eine beliebige Idealklasse von I_F/P_F. Wähle ein ganzes Ideal $\mathfrak{c}$ aus der inversen Klasse C^{-1} sowie $x \in \mathfrak{c}$ mit

$$|N(x)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} N(\mathfrak{c})\sqrt{|d(\mathbb{Z}_F)|}$$

$\Rightarrow x \cdot \mathbb{Z}_F \subseteq \mathfrak{c} \Rightarrow$ es existiert ein ganzes Ideal $\mathfrak{a} \in I_F$ mit $x \cdot \mathbb{Z}_F = \mathfrak{a} \cdot \mathfrak{c} \Rightarrow \mathfrak{a} \in C \Rightarrow$ Behauptung wegen $|N(x)| = N(\mathfrak{a}) \cdot N(\mathfrak{c})$. □

Korollar 8.52: $h_F < \infty$.

Beweis. In $\mathbb{Z}_F$ existieren nur endlich viele Ideale $\mathfrak{a}$ mit $N(\mathfrak{a}) < M_F$. □

Korollar 8.53:

$$\sqrt{|d(\mathbb{Z}_F)|} \geq \frac{n^n}{n!}(\frac{\pi}{4})^{r_2} > 1$$

Wir betrachten nun $F := \mathbb{Q}(\sqrt{5})$. Wie wir auf Blatt 8 gesehen haben gilt $\mathbb{Z}_F = \mathbb{Z} + \mathbb{Z}(1+\sqrt{5})/2$, daher folgt $d(\mathbb{Z}_F) = 5$. Wegen $M_F = 2/4\sqrt{5} < 2$ folgt $h_F = 1$.

Für $F := \mathbb{Q}(\sqrt{-5})$ erhalten wir $\mathbb{Z}_F = \mathbb{Z}[\sqrt{-5}]$ und daher $d(\mathbb{Z}_F) = 20$ (eigentlich -20). Also erhalten wir $M_F = \frac{2}{4}\frac{4}{\pi}2\sqrt{5} = 2.847\ldots < 3$. Die Klassengruppe wird also von Idealen $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq 2$ erzeugt, speziell reicht es also Primideal mit $N(\mathfrak{p}) < 3$ zu betrachten. Nach Blatt 14 reicht es die Primideale über der 2 zu betrachten. Nach Blatt 13 ist $\mathfrak{p} := 2\mathbb{Z}_F + (1+\sqrt{-5})\mathbb{F}_F$ ein Primideal der Norm 2 welches kein Hauptideal ist. Es gilt $\mathfrak{p}^2 = 4\mathbb{Z}_F + (-4+2\sqrt{-5})\mathbb{Z}_F = 2\mathbb{Z}_F$, also ist $\mathfrak{p}$ das einzige Ideal mit Norm < 3 und $\mathfrak{p}$ hat Ordnung 2, $\mathrm{Cl}_F = \langle \mathfrak{p}P_F \rangle \cong C_2$.

ANHANG A

Übungszettel

1. Übung zur Algebra II

(1) (4 Punkte) Sortieren. Eine riesige Datei (konstanter Satzlänge) soll sortiert werden. In einem ersten Durchlauf wurden die Schlüssel sortiert. Ergebnis: Eine Funktion $F : \mathbb{N}_n \to \mathbb{N}_n$ so, daß $F(1)$ die Position des 1. Datensatzes angibt, $F(2)$ die des 2. u.s.w. Im zweiten Durchlauf soll nun die Datei selber sortiert werden, dazu wird folgendes Programm benutzt:

```
for i:=1 to n do
  if not F(i)=i then
    j := i;
    T := Data(j);
    repeat
      k := F(j);
      Data(j) := Data(k);
      F(j) := j;
      j := k;
    until F(j)=i;
    Data(j) := T;
    F(j) := j;
  end if;
end do;
```

   (a) Was hat das mit Gruppentheorie zu tun?
   (b) Warum funktioniert der Algorithmus?

(2) (4 Punkte) Berechne:
   (a)

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 8 & 9 & 11 & 5 & 6 & 4 & 12 & 3 & 10 & 7 & 1 \end{pmatrix}$$

   als Produkt von Transpositionen und als Produkt disjunkter Zykeln;
   (b) die Produkte (1,3,2)(2,4,6,8), (1,2)(4,5,6,3)(3,4)(5,6,3);
   (c) die Inversen von (3,1,2)(4,6,5), (1,6,5)(4,3,2,6,1);
   (d) die Konjugierten $\pi\sigma\pi^{-1}$ für $\pi = (2,3)(3,4)$, $\sigma = (1,2,3)$ sowie $\pi = (1,3)(2,4,1)$ und $\sigma = (1,2,3,4,5)$.

(3) (6 Punkte)
   (a) Bestimme alle Untergruppen von A_4. Welche sind Normalteiler?
   (b) Bestimme alle Normalreihen von S_3.
   (c) Bestimme eine Normalreihe von A_4.

(4) (6 Punkte) Zeige: Jede endliche Gruppe ist isomorph zu einer Untergruppe einer einfachen Gruppe.

2. Übung zur Algebra II

(1) (6 Punkte) Es sei K/k eine Körpererweiterung, Γ/k eine normale Hülle und $\mathrm{Aut}(\Gamma/k) \supseteq G(K/k) = \{\sigma_i \mid 1 \leq i \leq [K:k]\}$. Auf $K[t]$ definieren wir $N(f) := \prod_{i=1}^{n} \sigma_i(f)$ mit $n := [K:k]$ und $\sigma_i(f) = \sigma_i(\sum a_j t^j) := \sum \sigma_i(a_j) t^j$. Dann gilt:
   (a) $N : K[t] \to k[t]$
   (b) Für $g \in k[t]$ gilt $N(g) = g^n$
   (c) Ist $f \in K[t]$ irreduzibel, so gilt $N(f) = g^l$ mit $g \in k[t]$ irreduzibel.
   (d) Es sei $f \in K[t]$ mit $N(f) =: g$ quadratfrei. In $k[t]$ gelte $g = \prod g_i$ mit $g_i \in k[t]$ irreduzibel. Dann folgt $f = \prod \mathrm{ggT}(f, g_i)$, wobei der ggT in $K[t]$ gebildet wird und $\mathrm{ggT}(f, g_i)$ in $K[t]$ irreduzibel ist.
   (e) Es sei $K = k[\alpha]$ und $f \in K[t]$. Dann gibt es nur endlich viele $s \in k$ so, daß $N(f(t + s\alpha))$ nicht quadratfrei ist.

(2) (6 Punkte) Es sei $L/K/k$ ein Körperturm, Γ/k normal mit $L \subseteq \Gamma$. $N : K[t] \to k[t]$ sei wie in der letzten Aufgabe definiert. Ferner sei $L = K[\beta]$, $K = k[\alpha]$. Elemente aus K werden wir als Polynome in $k[t]$ schreiben: $K \ni x = f(\alpha)$ mit $\alpha \in k[t]$. Ferner sei $F \in K[t]$ das Minimalpolynom von β. Wir nehmen an, daß $N(F)$ quadratfrei ist. Dann gelten:
   (a) Im Folgenden nehmen wir $N(F)$ quadratfrei an. Wenn wir $F \in k[\alpha, t]$ schreiben so gilt $\mathrm{ggT}(F(t, \beta), m_\alpha(t)) = at + b$ mit $0 \neq a,\ b \in k$.
   (b) Falls $N(F)$ quadratfrei ist, so folgt $L = k[\beta]$. Wie sieht die Darstellung von α in $k[\beta]$ aus?
   (c) Warum ist dies eine konstruktive Variante des Satzes vom primitiven Element? (In Charakteristik 0)

(3) (4 Punkte) $D(t) = \det((S_{i+j-2}(t))_{1 \leq i,j \leq n})$ für $t = (t_1, \ldots, t_n)$

(4) (4 Punkte) Es sei $t := (t_1, \ldots, t_n)$. Wir definieren $\pi : K(t) \to K(t) : f(t) \mapsto f(t_{\pi[1]}, \ldots, t_{\pi[n]})$ für $\pi \in S_n$. Dann gilt:
   (a) $\pi \in \mathrm{Aut}(K(t))$
   (b) Für $M := \mathrm{Fix}(S_n, K(t))$ gilt $M = K(\underline{\sigma})$ mit $\underline{\sigma} := (\sigma_1, \ldots, \sigma_n)$
   (c) $K(t)/M$ ist Zerfällungskörper von $f := \sum_{i=0}^{n} (-1)^i \sigma_i x^i$
   (d) $G(K(t)/M) \cong S_n$

3. Übung zur Algebra II

(1) (4 Punkte)
   (a) Finde einen vollkommenen Körper der echt größer als $\mathbb{C}$ ist.
   (b) Finde einen vollkommenen Körper der echt größer als $\mathbb{R}$ ist und $\mathbb{C}$ nicht enthält.
   (c) Finde einen Körper K und eine inseparable Erweiterung von Grad 12 über K.
   (d) Finde je einen Körper K der unendlich viele verschiedene Teilkörper besitzt mit $\chi(K) = 0$ und mit $\chi(K) = p$.

(2) (4 Punkte) Es sei L/K endlich algebraisch. Dann gilt:
   (a) L vollkommen $\Rightarrow$ K vollkommen.
   (b) K vollkommen $\Rightarrow$ L vollkommen.

(3) (4 Punkte) Es sei $M/\mathbb{Q}$ mit $[M:\mathbb{Q}] = 2$ gegeben.
   (a) Es gibt ein $a \in M$ mit $a^2 \in \mathbb{Q}$ und $M = \mathbb{Q}(a)$.
   (b) Gilt $M = \mathbb{Q}(a) = \mathbb{Q}(b)$ mit $a^2,\ b^2 \in \mathbb{Q}$, so folgt $(a/b)^2 \in \mathbb{Q}^2$.

(4) (4 Punkte) Es sei $K := \mathbb{Q}(\sqrt{2})$ und $L := K(\sqrt{5})$. Berechne

(a) $\mathrm{Aut}(L/K)$
(b) $G := \mathrm{Aut}(L/\mathbb{Q})$
(c) alle Untergruppen von G
(d) alle Teilkörper von L

(5) (4 Punkte) Es sei $K := \mathbb{F}_p$ ein Körper mit p Elementen. s und t seien unabhängige transzendente Elemente, $L := \mathbb{F}_p(s^p, t^p)$.
(a) $M := \mathbb{F}_p(s,t)$ ist rein inseparabel über L mit $[M : L] = p^2$.
(b) Für jedes $x \in M \setminus L$ gilt: $[L(x) : L] = p$
(c) Es gibt unendlich viele Teilkörper zwischen L und M
(d) Warum klappt das für $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ nicht?

4. Übung zur Algebra II

(1) (4 Punkte) Es sei $M/L/K$ ein endlicher Körperturm.
(a) Falls M/K normal ist, so auch M/L.
(b) Finde M, L und K mit M/L normal, L/K normal und M/K nicht normal.
(c) Finde M, L und K mit M/K normal und L/K nicht normal.

(2) (6 Punkte) Es sei L/K eine endliche Körpererweiterung. Dann ist L ein K-Vekorraum der Dimension $n := [L : K]$. Für $\alpha \in L$ definieren wir $\phi_\alpha : L \to L : x \mapsto \alpha x$ die „Multiplikation mit α“-Abbildung. Zeige:
(a) ϕ_α ist ein Vektorraumendomorphismus. Für $\alpha \neq 0$ sogar ein Automorphismus.
(b) $L \to \mathrm{End}(L) : \alpha \mapsto \phi_\alpha$ ist K-linear, ferner gilt $\phi_\alpha \phi_\beta = \phi_{\alpha\beta}$.
(c) Es sei m_α das Minimalpolynom von α über K, f das charakteristische Polynom von ϕ_α und M das Minimalpolynom von ϕ_α. Dann gilt $m_\alpha = M$, $f = M^l$ mit $l \in \mathbb{N}$ geeignet.
(d) Für eine beliebige Basis $b_1, \ldots, b_n$ von L entspreche ϕ_α der Matrix M_α. Dann gilt: $\det(M_\alpha) = \pm N_{L/K}(\alpha)$, $\mathrm{Tr}(M_\alpha) = \pm \mathrm{Tr}_{L/K}(\alpha)$
M_α heißt eine Darstellungsmatrix für α.

(3) (4 Punkte) Es sei $M/L/K$ ein endlicher Körperturm sowie $x \in M$. Zeige:
(a) $N_{M/K}(x) = N_{L/K} N_{M/L}(x)$
(b) $\mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K} \mathrm{Tr}_{M/L}(x)$
(c) Wie kann dieses an den Darstellungsmatrizen abgelesen werden?

(4) (6 Punkte) Es sei $K := \mathbb{Q}(\sqrt{3}, \sqrt{5})$ und $L := \mathbb{Q}(\sqrt{3})$. Für $\alpha := 1 + \sqrt{15}$ und $\beta := \sqrt{3} + \sqrt{5}$ berechne:
(a) $N_{K/Q}(\alpha)$, $N_{K/L}(\alpha)$, $N_{K/Q}(\beta)$, $N_{K/L}(\beta)$
(b) $m_{\alpha/\mathbb{Q}}$, $m_{\beta/\mathbb{Q}}$
(c) Finde jeweils ein Element mit $N_{K/Q}(x) = 1$ und $\mathrm{Tr}_{K/Q}(y) = 0$.

5. Übung zur Algebra II

(1) (4 Punkte) (Galoisgruppen operieren transitiv auf den Nullstellen) Es sei $f \in K[t]$ irreduzibel, separabel und Γ/K ein Zerfällungskörper. Über Γ gelte: $f = \ell(f) \prod_{i=1}^{n} (t - \alpha_i)$. Für $1 \leq i, j \leq n$ gibt es dann $\sigma \in G(\Gamma/K)$ mit $\sigma(\alpha_i) = \alpha_j$

(2) (4 Punkte) Es sei $f \in K[t]$ separabel, irreduzibel vom Grad 4. Die Nullstellen $\alpha_1, \ldots, \alpha_4 \in \Gamma$ seien fixiert. Gibt es ein f so, daß $\langle (\alpha_1, \alpha_2), (\alpha_3, \alpha_4) \rangle < S_4$ eine Darstellung für $G(f)$ ist?

(3) (4 Punkte) Es sei M/K eine einfache Körpererweiterung, Γ/K eine (minimale) normale Hülle, $G := G(\Gamma/K)$ und $G_M := \{\sigma \in G \mid \sigma(x) = x \; \forall x \in M\}$. Gegeben sei die Operation von G auf den Konjugierten eines primitiven Elementes und eine Darstellung von G (und G_M) als Permutationsgruppe. Lassen sich mit diesen Angaben alle Zwischenkörper $M/L/K$ berechnen? (Wenn über die Gruppe „alles“ bekannt ist). Wenn ja, wie?
(4) (4 Punkte) Berechne $G(x^4 + 1/\mathbb{Q})$.
(5) Es sei $K/\mathbb{Q}$ endlich, algebraisch mit $K = \mathbb{Q}(\alpha)$, $f(\alpha) = 0$, $f \in \mathbb{Z}[t]$ normiert und irreduzibel.
   (a) $R := \mathbb{Z}[\alpha]$ ist dann eine unitäre Ring-Erweiterung von $\mathbb{Z}$.
   (b) Es sei (p) ein Primideal in $\mathbb{Z}$ und $\mathbb{F}_p = \mathbb{Z}/(p)$ der Zugehörige Restklassenkörper. R/pR ist dann ein $\mathbb{F}_p$ Vektorraum. Es gilt $R/pR \cong \prod_{i=1}^{n} R_i$ wobei $R_i \cong \mathbb{F}_p[t]/f_i^{l_i}\mathbb{F}_p[t]$ gilt und die $f_i \in \mathbb{F}_p[t]$ irreduzibel sind. (Chinesischer Restsatz)
   (c) Für Ideale $P_i := (p, f_i(\alpha))$ von R gilt $R/P_i \cong R_i$. Für $l_i = 1$ ist P_i maximal.
   (d) Falls $K/\mathbb{Q}$ Galoissch ist, operiert $G(K/\mathbb{Q})$ transitiv auf den P_i.

6. Übung zur Algebra II

(1) (4 Punkte) Es sei M ein R-Modul.
   (a) $R[1]$ ist ein unitärer Ring. Die kanonische Einbettung $R \to R[1]$ ist injektiv.
   (b) M ist (kanonisch) ein $R[1]$ Modul.
(2) (4 Punkte) Es sei R unitär und M ein R-Modul (nicht notwendig unitär). Dann gilt $M = M_1 + M_0$ mit Teilmoduln $M_1 := \{m \in M \mid 1m = m\}$ und $M_0 := \{m \mid Rm = 0\}$. Ferner ist die Summe direkt.
(3) (4 Punkte) Es sei M ein R-Modul und R Integritätsring. Dann ist M als Quotient eines freien Moduls darstellbar.
(4) (4 Punkte) Es sei K ein Körper, $V := K^n$ und $\phi \in \mathrm{End}_K(V)$. Dann ist V ein $K[x]$-Torsionsmodul mittels $f(x)m := f(\phi)[m]$. Ist V ein Quotient von $K[x]^n$?
(5) (4 Punkte) Beweise je eine Aussage von 5.3 und 5.6 der Vorlesung.

7. Übung zur Algebra II

Für alle Aufgaben sei R ein unitärer kommutativer Ring, M und N seien R-Moduln. Weitere Einschränkungen je nach Aufgabe.

(1) (2 Punkte) M und N seien endlich erzeugte freie R-Moduln, dann gilt: $\mathrm{Hom}_R(M, N) \cong M \otimes N$
(2) (4 Punkte) Es seien G und G' endlich erzeugte abelsche Gruppen (also $\mathbb{Z}$-Moduln).
   (a) Für $G = \langle a \rangle$, $G' = \langle b \rangle$ gilt $G \otimes G' \cong \langle c \rangle$ mit $\mathrm{ord}(c) = \mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b))$. Wobei wir $\mathrm{ggT}(\infty, a) = a$ annehmen.
   (b) Berechne $G \otimes G'$ (mit Hilfe des Hauptsatzes über endlich erzeugte Abelsche Gruppen und Teil a).
(3) (4 Punkte) Zeige die Eindeutigkeit (bis auf Isomorphie) in Satz 5.18.
(4) (4 Punkte)
   (a) Es sei $0 \to M \xrightarrow{f} N$ eine exakte Sequenz. Dies ist äquivalent dazu, daß f injektiv ist. Ferner ist M isomorph zu einem Teilmodul von N.

(b) Es sei $M \xrightarrow{g} N \to 0$ exakt. Dies ist äquivalent dazu, daß g surjektiv ist. Ferner ist N isomorph zu einem Faktormodul von M.

(5) (4 Punkte) Es gelte $2 \in R^\times$, M sei frei mit endlicher Basis und $\psi : M \otimes M \to M \otimes M : m \otimes n \mapsto n \otimes m$. Ferner sei $S := \ker(\psi - \mathrm{Id})$ und $A := \ker(\psi + \mathrm{Id})$.
   (a) Zeige $M \otimes M \cong S \dot{+} A$
   (b) Sind A und S frei? Wenn ja, gib jeweils Basen an.
   (c) Für jede symmetrische bilineare Abbildung $\phi : M \times M \to N$ (d.h. $\phi(x, y) = \phi(y, x)$) gibt es genau ein $\hat{\phi} \in \mathrm{Hom}_R(M \otimes M, N)$ mit $\hat{\phi}(a \otimes b + b \otimes a) = 2\phi(a, b)$ $\forall a, b \in M$.

(6) (2 Punkte) Beweise Satz 5.26 mit Hilfe von 5.19.

8. Übung zur Algebra II

(1) (16 Punkte) Es sei $K = \mathbb{Q}(\alpha)$ ein Zahlkörper, α ist Nullstelle eines normierten irreduziblen Polynoms $f \in \mathbb{Z}[t]$. $\mathbb{Z}_K := \{\beta \in K \mid \exists g \in \mathbb{Z}[t] : g(\beta) = 0 \ g \text{ normiert}\}$. Ziel: $\mathbb{Z}_K$ ist ein freier $\mathbb{Z}$-Modul vom Rang n.
   (a) Für jedes $\beta \in \mathbb{Z}_K$ ist $\mathbb{Z}[\beta]$ ein endlich erzeugter $\mathbb{Z}$-Modul.
   (b) Für β, $\gamma \in \mathbb{Z}_K$ ist $\mathbb{Z}[\beta, \gamma]$ ebenfalls endlich erzeugter $\mathbb{Z}$-Modul.
   (c) $\mathbb{Z}_K$ ist ein Ring.
   (d) Es sei $M \subseteq K$ ein freier $\mathbb{Z}$-Modul vom Rang n mit Basis $b_1, \ldots, b_n$. Dann ist $(b_i)_i$ eine $\mathbb{Q}$-Basis für K.
   (e) Für einen freien $\mathbb{Z}$-Modul $M \subseteq \mathbb{Z}_K$ vom Rang n mit Basis $(b_i)_i$ gilt $d(b_1, \ldots, b_n) \in \mathbb{Z}$. (Wobei $d(b_1, \ldots, b_n) = \det((\mathrm{Tr}(b_i b_j))_{i,j})$ die Diskriminante der Basis ist.)
   (f) Es seien $M \subseteq N \subseteq K$ freie $\mathbb{Z}$-Moduln vom Rang n mit Basis $(b_i)_i$ bzw. $(c_i)_i$. Dann gilt $d(c_1, \ldots, c_n) | d(b_1, \ldots, b_n)$. Ferner gilt: $d(b_1, \ldots, b_n)/d(b_1, \ldots, b_n) = (N : M)^2$.
   (g) $\mathbb{Z}_K$ ist über $\mathbb{Z}$ frei vom Rang n.
   (h) Jedes Ideal $\mathbf{a} \neq 0$ von $\mathbb{Z}_K$ ist ein $\mathbb{Z}$-Modul vom Rang n

(2) (4 Punkte) Berechne $\mathbb{Z}_{\mathbb{Q}(\sqrt{2})}$ und $\mathbb{Z}_{\mathbb{Q}(\sqrt{5})}$.

9. Übung zur Algebra II

(1) (5 Punkte)
   (a) Es seien M, M', N R-Moduln, und α, $\beta \in \mathrm{Hom}_R(M, M')$. α^*, $\beta^* : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N)$ seien wie in der Vorlesung definiert. Dann gilt $\alpha^* + \beta^* = (\alpha + \beta)^*$.
   (b) Es seien M, M', M'', N R-Moduln, und $\alpha \in \mathrm{Hom}_R(M', M'')$ und $\beta \in \mathrm{Hom}_R(M, M')$. α^*, β^* seien wie in der Vorlesung definiert. Dann gilt $(\alpha\beta)^* = \beta^*\alpha^*$.

(2) (5 Punkte) Zeige die Aussage über die Surjektivität in Lemma 6.4.

(3) (5 Punkte) Finde 3 verschiedene C_4-Erweiterungen von $\mathbb{Q}$.

(4) (5 Punkte) Finde 3 verschiedene C_5-Erweiterungen von $\mathbb{Q}$. Hier ist es nicht nötig ein Polynom anzugeben, es reicht die Körper eindeutig zu charakterisieren.

10. Übung zur Algebra II

(1) (5 Punkte) Es seien N, E Gruppen und $\alpha : E \to \mathrm{Aut}N$ ein Antihomomorphismus. Auf $E \times N$ definieren wir die Operation $(a, x) * (b, y) := (ab, \alpha(b)[x]y)$
   (a) $(a, x) * (1, 1) = (1, 1) * (a, x)$
   (b) $*$ ist assoziativ
   (c) $(E \times N, *) =: E \rtimes_\alpha N =: G$ ist eine Gruppe
   (d) $E \cong (E, 1)$ und $N \cong (1, N)$
   (e) $1 \to N \to G \to E \to 1$ ist exakt
   (f) Bestimme (ein) τ sowie das zugehörige λ für diese Gruppenerweiterung.

(2) (5 Punkte) Es sei $1 \to N \to G \to E \to 1$ eine zerfallende Erweiterung. Zeige: $G = N \ltimes_\alpha E$ für ein passendes $\alpha : E \to \mathrm{Aut}N$.

(3) (5 Punkte) Es sei G eine Gruppe und $N \lhd G$ sowie $E \lhd G$ Normalteiler mit $N \cap E = \{1\}$ und $G = NE$. Bestimme $\alpha : E \to \mathrm{Aut}N$ mit $G \cong N \ltimes_\alpha E$.

(4) (5 Punkte) Für $E = N = C_2$ gilt $H^2(E, N) = C_2$. Andererseits ist $1 \to C_2 \to G \to C_2 \to 1$ exakt für $G = C_4$ und $G = V_4$. Gilt $1_{H^2} = C_4$?

11. Übung zur Algebra II

(1) (4 Punkte) Hilbert 90, Teil2: Es sei K/k eine normale Körpererweiterung und $G := G(K/k)$ die Galoisgruppe.
   (a) Zeige: K^+ ist ein G-Modul.
   (b) Zeige: $H^1(G, K^+) = 0$
   (c) Angenommen, $G = \langle g \rangle$ und $\mathrm{Tr}_{K/k}(x) = 0$. Dann gibt es ein $y \in K$ mit $k = y - g(y)$.

(2) (4 Punkte) Es sei $Q(x, y, z) := 2x^2 + 2xy + 2xz + 2y^2 + 2yz + 2z^2$ (das Beispiel aus der Vorlesung). Berechne alle $x \in \mathbb{Z}^3$ mit $Q(x) \leq 2$.

(3) (4 Punkte) Es sei $\Lambda \subseteq \mathbb{R}^n$ ein Gitter vom Rang n mit Basis $b_1, \ldots, b_n$. Die Matrix $G := (b_i^t b_j)_{i,j}$ heißt Gram-Matrix zu Λ.
   (a) Ein Gitter heißt ganz (engl. integral lattice), falls $G \in \mathbb{Z}^{n \times n}$ gilt. Finde ein ganzes Gitter $\Lambda \subseteq \mathbb{Q}^4$ der Dimension 4 mit $\Lambda \not\subset \mathbb{Z}^4$
   (b) Kann es ein ganzes Gitter $\Lambda \subseteq \mathbb{Z}^l$, $\Lambda \subseteq \mathbb{Q}^l$ geben mit $l < 4$?

(4) (4 Punkte) Es sei $k/\mathbb{Q}$ ein Zahlkörper vom Grad n und $\mathbb{Z}_k$ der Ring der algebraisch ganzen Zahlen von k. Es gelte $k = \mathbb{Q}(\alpha)$ mit $f(\alpha) = 0$ für ein normiertes irreduzibles $f \in \mathbb{Z}[x]$.
   (a) In $\mathbb{C}$ gilt $f = \prod(x - \alpha^{(i)})$. Zeige: $(.)^{(i)} : k \to \mathbb{C} : \sum_{j=1}^n r_j \alpha^{j-1} \mapsto \sum_{j=1}^n r_j (\alpha^{(i)})^{j-1}$ ist ein Körpermonomorphismus.
   (b) Wir fixieren eine Sortierung der Nullstellen. Wir nehmen an, dass $\alpha^{(1)}, \ldots, \alpha^{(r_1)} \in \mathbb{R}$ und $\alpha^{(r_1+1)} = \bar{\alpha}^{(r_1+r_2+1)}, \ldots, \alpha^{(r_1+r_2)} = \bar{\alpha}^{(r_1+2r_2)} \in \mathbb{C} \setminus \mathbb{R}$ gelte. Es sei nun $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}_k$. Wir definieren $b_i \in \mathbb{R}^n$ mittels
   $$b_{i,j} := \begin{cases} \omega_i^{(j)} & 1 \leq j \leq r_1 \\ \sqrt{2}\Re\omega_i^{(j)} & r_1 < j \leq r_1 + r_2 \\ \sqrt{2}\Im\omega_i^{(j-r_2)} & \end{cases}$$
   Zeige: Das Gitter Λ_k welches von $b_1, \ldots, b_n$ erzeugt wird ist als $\mathbb{Z}$-Modul isomorph zu $\mathbb{Z}_k$.
   (c) $T_2 : k \to \mathbb{R} : \mu \mapsto \sum_{i=1}^n |\mu^{(i)}|^2$ entspricht der Längenfunktion von Λ_k
   (d) Aus der Analysis wird die Ungleichung zwischen geometrischem und arithmetischem Mittel als bekannt vorausgesetzt: $\sqrt[n]{\prod_{i=1}^n x_i} \leq \frac{1}{n} \sum_{i=1}^n x_i$ für $x_i \geq 0$. Zeige: der kürzeste Vektor in $\Lambda_k \setminus \{0\}$ hat Länge n.

(5) (4 Punkte)
   (a) Zeige Hilfssatz 5.47
   (b) Finde Gitter $\Lambda_n \subseteq \mathbb{R}^2$ so, daß sie von Elementen der Länge ≥ 1 erzeugt werden und (nicht triviale) Elemente der Länge $\leq 1/n$ enthalten.

12. Übung zur Algebra II

(1) Sei $\beta_{i,j} := \begin{cases} (\sqrt{3}/2)^{i-1} & j = i \\ 0 & j < i\,,\ (1 \leq i \leq n) \\ 1/2(\sqrt{3}/2)^{i-1} & \text{sonst} \end{cases}$ und Λ_k das Gitter, welches von den ersten k Spalten $b_1, \ldots, b_k$ von $(\beta_{i,j})_{i,j} \in \mathbb{R}^{n\times n}$ aufgespannt wird. Zeige:
   (a) $b_1, \ldots, b_k$ ist eine LLL-Basis von Λ_k.
   (b) Für $k \geq 2$ gilt $\min \Lambda_k = (\sqrt{3}/2)^{k-2}$. (Hinweis: betrachte $b_k - b_{k-1}$.)
(2) Sei $\Lambda \subset \mathbb{R}^2$ ein 2-dimensionales Gitter. Wieviele Vektoren minimaler Länge kann es geben?
(3) Paarreduktion Zwei Vektoren $a, b \in \mathbb{R}^n$ heissen Paarreduziert, falls $\|a\| \leq \|b\|$ und $|a^t b| \leq 1/2\|a\|^2$ gilt.
   (a) Seien $a, b \in \mathbb{R}^n$ unabhängig. Betrachte folgendes Verfahren:
      - Falls $\|a\| > \|b\|$, so vertausche a und b.
      - Ersetze b durch $b - \lfloor a^t b/\|a\|^2 \rceil a$. ($\lfloor r \rceil \in \mathbb{Z} \cap]r - 1/2, r + 1/2]$)
      - Wiederhole die beiden Schritte, bis sich nichts mehr ändert.

      Dann sind a, b paarreduziert (und erzeugen das selbe Gitter wie die Startvektoren).
   (b) Paarreduzierte Vektoren sind LLL reduziert.
(4) Sei $\Lambda \subseteq \mathbb{R}^n$ ein n-dimensionales Gitter.
   (a) Es gibt eine Grammatrix $(g_{i,j})_{i,j}$ für Λ mit $g_{1,1} \leq g_{2,2} \leq \cdots \leq g_{n,n}$ und $|g_{i,j}| \leq 1/2 g_{i,i}$ für $i < j$.
   (b) Sei $n = 3$. Wieviele Vektoren minimaler Länge kann es maximal geben?
(5) Sei $\Lambda \subseteq \mathbb{R}^n$ ein n-dimensionales Gitter mit ganzzahliger Grammatrix. Wir definieren ein duales Gitter $\Lambda^\#$ als $\Lambda^\# := \{x \in \mathbb{R}^n \mid x^t \Lambda \subseteq \mathbb{Z}\}$
   (a) $\Lambda \subseteq \Lambda^\#$
   (b) $(\Lambda^\# : \Lambda) = d(\Lambda)$
   (c) Finde eine Abschätzung für das 1. Minimum von $\Lambda^\#$ in Abhängigkeit von Λ.

13. Übung zur Algebra II

(1) Beweise 8.1.(2) und 8.1.(3). Überlege genau, für welche Indexmengen die Aussagen stimmen. (endlich, abzählbar, groß)
(2) Es sei $\mathbb{F}_q$ ein endlicher Körper. Zeige: $\mathbb{F}_q[x]$ ist ein Dedekind Ring.
(3) Es seien $\mathfrak{a}$, $\mathfrak{b}$ ganze Ideale von einem Dedekindring R. $N(\mathfrak{a}) := \#R/\mathfrak{a}$ ist die Norm von $\mathfrak{a}$.
   (a) $\mathfrak{a}/\mathfrak{ab} \cong R/\mathfrak{b}$.
   (b) $1 \to R/\mathfrak{b} \to R/\mathfrak{ab} \to R/\mathfrak{a} \to 1$ ist exakt.
   (c) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$
   (d) Für $a \in R$ gilt $|N(a)| = N(aR)$, falls $R \subseteq K$, K ein Zahlkörper und $N(a)$ die gewöhnliche Norm bedeutet.

   (e) $N(\mathfrak{a}) \in \mathfrak{a}$
(4) Es sei R ein Dedekindring in einem Zahlkörper und $\mathfrak{a}$ ein Ideal. Zeige: $\mathfrak{a}$ ist genau dann ein Hauptideal, wenn es ein $a \in \mathfrak{a}$ mit $|N(a)| = N(\mathfrak{a})$ gibt.
(5) Es sei $R := \mathbb{Z}[\sqrt{-5}]$, $\mathfrak{a} := 2R + (1 + \sqrt{-5})R$. Zeige:
   (a) $N(\mathfrak{a}) = 2$
   (b) $\mathfrak{a}$ ist kein Hauptideal.
   (c) $\mathfrak{a}$ ist Primideal.

14. Übung zur Algebra II

(1) (5 Punkte) Beweise Korollar 8.34
(2) (4 Punkte) Finde einen endlich erzeugten, nicht freien, torsionsfreien Modul vom Rang > 1 über einem Dedekind Ring R.
(3) (5 Punkte) Es sei $\mathfrak{a} = \alpha R + \beta R$ ein Ideal in einem Dedekind Ring R (α, $\beta \in Q(R)$). Dann gilt $\mathfrak{a}^n = \alpha^n R + \beta^n R$ für $n \in \mathbb{N}$.
(4) (6 Punkte) Es sei K/k eine Zahlkörpererweiterung und $R := \mathbb{Z}_k$, $S := \mathbb{Z}_K$ der ganze Abschluss von $\mathbb{Z}$ in k bzw. K.
   (a) Es sei $\mathfrak{p}$ ein Primideal in S. Dann ist $\mathfrak{p} \cap k$ ein Primideal in R
   (b) Es sei $k = \mathbb{Q}$ und $\mathfrak{p}$ ein Primideal in S. Dann gilt $\min \mathfrak{p} \setminus \{0\} \cap \mathbb{N} = p$, ($p$ Primzahl in $\mathbb{Z}$)
   (c) $pS = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$.
   (d) Voraussetzung wie oben. Dann ist $N(\mathfrak{p}_i) = p^{f_i}$ wo $f_i \in \mathbb{N}$ und p eine Primzahl in $\mathbb{Z}$ bedeutet.
   (e) $n = (K : k) = \sum_{i=1}^{r} e_i f_i$
   (f) Es gibt nur endlich viele ganze Ideale beschränkter Norm.

Literaturverzeichnis

[1] Birkhoff, Bartee, *Modern Applied Algebra*
[2] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[3] Th. W. Hungerford, *Algebra*, 1974.
[4] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[5] R. Kochendörffer, *Einführung in die Algebra*, VEB, 1963.
[6] S. Lang, *Algebra*, Addison-Wesley, 1971.
[7] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag.
[8] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[9] M. Pohst, *Lineare Algebra I, II*, Skript
[10] M. Pohst, *Algebra I*, Skript
[11] Derek J. S. Robinsion *A Course in the theory of Groups*, Springer, Graduate Texts in Mathematics, 1996
[12] W. M. Ruppert *Kommutative Algebra I, II*, Skript, Uni Erlangen
[13] Michio Suzuki, *Group Theory I*, Springer, Grundlehren, 1982
[14] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.

Index