Algebraische Zahlentheorie

Rainer Vogt

Sommersemester 2010

Inhaltsverzeichnis

Teil I
Algebraische Grundlagen

In diesem Kapitel wiederholen und ergänzen wir Teile aus der Einführung in die Algebra, die für uns wichtig sind. Wir bezeichnen diese Veranstaltung kurz mit "Einführung" und beziehen uns bei Zitaten auf das Skript von Herrn Römer aus dem Jahr 2007.

1 Ringe und Körper

Ringe

Unter einem Ring verstehen wir in dieser Vorlesung stets einen kommutativen Ring mit Einselement. Ein Element $a \in R$ heißt *Nullteiler*, wenn es ein $b \neq 0$ in R gibt, so dass $a \cdot b = 0$. Ist $0 \in R$ der einzige Nullteiler, dann heißt R *nullteilerfrei*. Einen nullteilerfreien Ring $R \neq 0$ nennen wir *Integritätsring*. Die Gruppe alle Einheiten von R bezeichnen wir mit R^*. Ist $R \neq 0$ und $R^* = R \backslash \{0\}$, dann nennen wir R einen *Körper*.

1.1 Satz: (Einführung 2.14) Jeder endliche Integritätsring ist ein Körper.

Ein *Unterring* S eines Ringes R ist eine Teilmenge mit $1 \in S$, so dass die Addition und Multiplikation von R auf S eine Ringstruktur definieren. Wir nennen das Paar $S \subset R$ eine *Ringerweiterung*.

Ringhomomorphismen

Ein *Homomorphismus* von Ringen ist eine strukturerhaltende Abbildung

$$f : R_1 \to R_2$$

von Ringen. Explizit bedeutet das:

$$\begin{array}{rcll} f(1_{R_1}) & = & 1_{R_2} & \\ f(x+y) & = & f(x) + f(y) & \forall x, y \in R_1 \\ f(x \cdot y) & = & f(x) \cdot f(y) & \forall x, y \in R_1 \end{array}$$

Wir erinnern an

$$\begin{array}{rcl} \operatorname{Kern} f & = & \{x \in R_1;\ f(x) = 0\} \\ \operatorname{Bild} f & = & \{f(x) \in R_2;\ x \in R_1\} \end{array}$$

Bild f ist ein Unterring von R_2 und Kern f ist ein *Ideal* in R_1.

Ideale

Ideale werden in dieser Vorlesung eine große Rolle spielen. Ein Ideal J in einem Ring R ist eine nicht-leere Teilmenge, so dass gilt

$$x, y \in J \Rightarrow x + y \in J \quad \text{und} \quad r \cdot x \in J \qquad \forall x, y \in J, \forall r \in R.$$

Insbesondere ist $(J, +)$ eine Untergruppe von $(R, +)$.
Ist $J \subset R$ ein Ideal, dann wird durch

$$x \sim y \iff x - y \in J$$

eine Äquivalenzrelation auf R definiert. Die Äquivalenzklasse $\overline{x}$ von x ist gegeben durch

$$\overline{x} = x + J \subset R.$$

Die Menge R/J aller Äquivalenzklassen besitzt eine Ringstruktur, definiert durch

$$\overline{x} + \overline{y} = \overline{x + y} \quad \text{und} \quad \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

Die *Projektion* $p : R \to R/J$, $x \mapsto \overline{x}$ ist ein Epimorphismus von Ringen mit Kern J. Wir nennen R/J *Restklassenring modulo* J. Er besitzt folgende universelle Eigenschaft.

1.2 Satz: (Einführung 3.5) Sei $f : R \to S$ ein Homomorphismus von Ringen, $J \subset \operatorname{Kern} f$ ein Ideal. Dann gibt es genau einen Homomorphismus von Ringen $\overline{f} : R/J \to S$, so dass $f = \overline{f} \circ p$. Weiter gilt

$$\operatorname{Bild} \overline{f} = \operatorname{Bild} f, \qquad \operatorname{Kern} \overline{f} = p(\operatorname{Kern} f) = (\operatorname{Kern} f)/J.$$

Sei R ein Ring und $A \subset R$ eine beliebige Teilmenge. Das kleinste Ideal von R, das A enthält, wird mit (A) bezeichnet und heißt das *von A erzeugte Ideal*. "Kleinst" bedeutet dabei, dass $(A) \subset J$ gilt, falls J ein Ideal ist, das A enthält. Man prüft leicht nach, dass (A) existiert:

$$(A) = \bigcap \{J; J \subset R \text{ Ideal}, A \subset J\}$$

Ein Ideal, das von einem einzigen Element erzeugt wird, heißt *Hauptideal*. Ein Integritätsring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*. Ein Beispiel ist $\mathbb{Z}$.

Sind I, J Ideale von R, dann sind auch $I + J$ und $I \cap J$ Ideale. Wir definieren das *Produktideal* $I \cdot J$ als das von der Menge $\{x \cdot y \in R; x \in I, y \in J\}$ erzeugte Ideal.

1.3 Aufgabe: (1) Zwei Ideale I, J von R heißen *coprim*, falls $I + J = R$. Zeigen Sie: Sind I und J coprim, dann gilt $I \cdot J = I \cap J$.

(2) Sei $R \neq 0$ ein Ring. Zeigen Sie: R ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale von R sind.

Ein Ideal $P \subset R$ heißt *Primideal*, wenn $P \neq R$ und für alle $a, b \in R$ mit $a \cdot b \in P$ folgt, dass $a \in P$ oder $b \in P$. Ein Ideal $M \subset R$ heißt *maximales Ideal*, wenn $M \neq R$ und für alle Ideale $J \subset R$ mit $M \subset J \subset R$ folgt, dass $J = M$ oder $J = R$. Es gilt

1.4 Satz: (Einführung 4.10 und 4.12) Sei J ein Ideal im Ring R. Dann gilt

(1) J ist ein Primideal $\iff$ R/J ist ein Integritätsring.

(2) J ist maximal $\iff$ R/J ist ein Körper.

Quotientenringe

Jeder Unterring R eines Körpers K ist ein Integritästring. Umgekehrt kann jeder Integritätsring R in einem Körper K eingebettet werden, z.B. in seinem *Quotientenkörper* $Q(R)$ (s. Einführung 4.6 und 4.7). Sei $T = R\backslash\{0\}$. Dann besteht $Q(R)$ aus den Äquivalenzklassen von Paaren $(a, b) \in R \times T$ unter der Äquivalenzrelation

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \cdot b_2 = b_1 \cdot a_2.$$

Die Äquivalenzklasse von (a, b) wird üblicherweise mit $\frac{a}{b}$ bezeichnet. Die Rechenregeln sind die der Bruchrechnung. Wir erinnern an die universelle Eigenschaft des Quotientenkörpers.

1.5 Satz: Sei R ein Integritätsring und $Q(R)$ sein Quotientenkörper. Die *kanonische Einbettung* $\iota : R \to Q(R)$, $a \mapsto \frac{a}{1}$ ist ein Monomorphismus von Ringen. Ist $f : R \to S$ ein Ringhomomorphismus, so dass $f(R\backslash\{0\}) \subset S^*$, dann gibt es genau einen Ringhomomorphismus. $\overline{f} : Q(R) \to S$, so dass $f = \overline{f} \circ \iota$.

1.6 Bemerkung: Sei $R \neq 0$ ein Ring. K ein Körper und $f : K \to R$ ein Homomorphismus von Ringen, dann ist f injektiv. Insbesondere ist $\overline{f}$ in 1.5 injektiv.

Charakteristik

Es gibt genau einen Ringhomomorphismus

$$\varphi : \mathbb{Z} \to R$$

für jeden Ring R. Sein Kern ist ein Ideal in $\mathbb{Z}$, insbesondere also eine Untergruppe von $(\mathbb{Z}, +)$. Dann gibt es genau ein $n \in \mathbb{N}$, so dass $n \cdot \mathbb{Z} = \operatorname{Ker} \varphi$. Dieses n ist die *Charakteristik* von R, bezeichnet mit $\operatorname{char}(R)$.

1.7 Satz: (Einführung 2.19) Die Charakteristik eines Integritätsrings ist entweder 0 oder eine Primzahl.

Primkörper

Ist R ein Integritätsring der mindestens einen Teilkörper enthält. Dann ist der Durchschnitt aller Teilkörper von R der kleinste Teilkörper, genannt *Primkörper* von R.

Ist $\operatorname{char}(R) = 0$, ist $\varphi : \mathbb{Z} \to R$ injektiv. Falls R einen Primkörper hat, ist dieser $\mathbb{Q}$. Das Beispiel $\mathbb{Z}$ zeigt, dass R keinen Körper zu enthalten braucht.

Ist $\operatorname{char}(R) = p$ und p prim, dann ist die induzierte Abbildung $\overline{\varphi} : \mathbb{Z}/p \to R$ nach 1.2 injektiv. Also enthält R den Primkörper $\mathbb{F}_p = \mathbb{Z}/p$.

1.8 Aufgabe: Sei K Teilkörper eines Integritätsringes R. Dann definieren die Addition und Multiplikation in R eine K-Vektorraumstruktur auf R.
Zeigen Sie: Ist $\dim_K R$ endlich, dann ist R selbst ein Körper.

2 Teilbarkeitslehre

2.1 Konvention: Wenn wir es nicht ausdrücklich anders formulieren, sind alle betrachteten Ringe Integritätsringe.

Gilt $a \cdot x = b$ in R, nennen wir a einen *Teiler* von b und schreiben $a|b$. Da jedes $a \in R^*$ und b selbst stets Teilern von b sind, nennen wir sie die *trivialen Teiler* von b.

a und b aus R heißen *assoziiert*, wenn $(a) = (b)$. Wir schreiben $a \sim b$. Offensichtlich ist $a \sim b$ genau dann, wenn $a|b$ **und** $b|a$.

2.2 Definition: Sei R ein Integritätsring und $0 \neq a \in R \backslash R^*$.

(1) a heißt *irreduzibel*, wenn aus $a = b \cdot c$ folgt, dass $b \in R^*$ oder $c \in R^*$ (d.h. a lässt sich nur trivial faktorisieren).

(2) a heißt *prim*, wenn aus $a|b \cdot c$ folgt, dass $a|b$ oder $a|c$. Ist $a \neq 0$, dann ist a genau dann prim, wenn (a) ein Primideal ist.

2.3 Satz: (Einführung Abschnitt 5) In einem Integritätsring R gilt

(1) $a \sim b \iff \exists x \in R^*$ mit $a \cdot x = b$

(2) jedes Primelement ist irreduzibel.

(3) Sind $a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ zwei Faktorisierungen von a in Primelemente, dann ist $m = n$ und nach einer geeigneten Umnummerierung gilt $p_i \sim q_i$.

Ein zentrales Thema dieser Vorlesung wird die Zerlegbarkeit in Primelemente sein.

2.4 Definition: Ein Integritätsring R heißt *faktoriell*, wenn sich jedes Element $0 \neq a \in R \backslash R^*$ als Produkt von Primelementen schreiben lässt.

2.5 Satz: (Einführung 5.6 und 5.7)

(1) In einem Hauptidealring R sind für $0 \neq a \in R \backslash R^*$ äquivalent:

(i) a ist prim.

(ii) a ist irreduzibel.

(iii) (a) ist maximales Ideal.

(2) Ein Hauptidealring ist faktoriell.

In einem Hauptidealring kann man Teilertheorie idealtheoretisch betreiben.

2.6 Definition: Sei R Integritätsring. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$ aus R, wir schreiben $d = \mathrm{ggT}(a_1, \ldots, a_n)$, wenn gilt:

(1) $d|a_i$ für $i = 1, \ldots, n$

(2) Aus $x|a_i$ für $i = 1, \ldots, n$ folgt $x|d$.

Ein Element $v \in R$ heißt *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$, wir schreiben $v = \mathrm{kgV}(a_1, \ldots, a_n)$, wenn gilt

(1) $a_i|v$ für $i = 1, \ldots, n$.

(2) Aus $a_i|w$ für $i = 1, \ldots, n$ folgt $v|w$.

d und v brauchen nicht zu existieren und, wenn sie existieren, sind sie höchstens bis auf Assoziiertheit eindeutig. In faktoriellen Ringen kann man d und v über die Primfaktorzerlegungen bestimmen, in Hauptidealringen gilt

2.7 Satz: (Einführung Abschnitt 5.14. Übung) Sei R ein Hauptidealring und seien $a_1, \ldots, a_n \in R$. Dann gilt

(1) $d = \mathrm{ggT}(a_1, \ldots, a_n) \iff (d) = (a_1) + \ldots + (a_n) = (a_1, \ldots, a_n)$,

(2) $a, b \in R$ sind teilerfremd $\iff \exists x, y \in R$ mit $1 = x \cdot a + y \cdot b$,

(3) $v = \mathrm{kgV}(a_1, \ldots, a_n) \iff (v) = (a_1) \cap \ldots \cap (a_n)$.

Aus (1) ergibt sich, dass der $\mathrm{ggT}(a_1, \ldots, a_n) = d$ eine Darstellung

$$d = x_1 a_1 + \ldots + x_n a_n$$

mit $x_i \in R$ besitzt. Oft ist man an solchen Darstellungen interessiert. Ist R ein euklidischer Ring, dann erlaubt der euklidische Algorithmus die Berechnung einer solchen Darstellung (s. Einführung 5.15). Wir erinnern:

2.8 Definition: Ein *euklidischer Ring* ist ein Integritätsring R zusammen mit einer Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}$, genannt *Grad-* oder *Normabbildung*, so dass gilt

(1) $\delta(x) \leq \delta(x \cdot y) \quad \forall x, y \in R\backslash\{0\}$.

(2) Ist $a \in R$ und $b \in R\backslash\{0\}$, dann gibt es $q, r \in R$, so dass

$$a = qb + r \qquad \text{mit } r = 0 \text{ oder } \delta(r) < \delta(b).$$

2.9 Aufgabe: Zeigen Sie: Sei R euklidischer Ring und $x \in R\backslash\{0\}$. Dann gilt $\delta(1) \leq \delta(x)$. Gleichheit gilt genau dann, wenn $x \in R^*$.

2.10 Satz: (Einführung Abschnitt 5.11) Ein euklidischer Ring ist Hauptidealring.

3 Polynomringe

Sei R ein Ring und $R[X]$ der Polynomring über R. Wir erinnern an den Divisionsalgorithmus.

3.1 Satz: (Einführung 6.7) Seien $f, g \in R[X]$, $g \neq 0$ und der Leitkoeffizient von g aus R^*. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[X]$, so dass

$$f = q \cdot g + r \qquad \text{mit } r = 0 \text{ oder } \operatorname{grad} r < \operatorname{grad} g.$$

Als Folgerung erhält man

3.2 Satz: (Einführung 6.8) Ist K ein Körper, dann ist $K[X]$ ein euklidischer Ring und damit auch Hauptidealring.

Sei $r \in R$. Dann definiert die *Einsetzabbildung*

$$E_r : R[X] \to R, \qquad \left(f = \sum_{i=0}^{n} a_i \cdot X^i \right) \mapsto \left(\sum_{i=0}^{n} a_i r^i =: f(r) \right)$$

einen Ringhomomorphismus. Gilt $f(r) = 0$, heißt r *Nullstelle* von f. Ist $r \in R$ Nullstelle von $f \in R[X]$, dann ist $(X - r)$ ein Teiler von f.
Wir interessieren und für Primelemente in $R[X]$.

3.3 Satz: (Einführung 6.12) Sei R ein Ring $J \cap R$ ein Ideal und $\overline{J} \subset R[X]$ das von J in $R[X]$ erzeugte Ideal. Dann gilt

(1) $\overline{J} \subset R = J$

(2) $R[X]/\overline{J} \cong (R/J)[X]$

(3) $J \subset R$ ist Primideal $\iff$ $\overline{J} \subset R[X]$ ist Primideal.

3.4 Satz: (Einführung 6.5) $R[X]$ ist genau dann ein Integritätsring, wenn R ein Integritätsring ist. In diesem Fall gilt $(R[X])^* = R^*$.

3.5 Satz: (Einführung Abschnitt 7) Sei R Integritätsring und $a \in R$

(1) a ist prim in R $\iff$ a ist prim in $R[X]$.

(2) a ist irreduzibel in R $\iff$ a ist irreduzibel in $R[X]$.

(3) R ist faktoriell $\iff$ $R[X]$ ist faktoriell.

(4) Ist $\varepsilon \in R^*$, dann gilt: $f(X) \in R[X]$ ist genau dann irreduzibel, wenn $f(\varepsilon X + a)$ irreduzibel ist.

Ist K ein Körper, dann ist $K[X]$ ein Hauptidealring. Also sind irreduzible Elemente auch prim. Deshalb sind die folgenden Resultate für uns wichtig. Wir erinnern daran, dass ein Polynom *primitiv* ist, falls der ggT seiner Koeffizienten 1 ist.

3.6 Satz: (Einführung 7.8 und 7.9) Sei R ein faktorieller Ring $0 \neq f, g \in R[X]$ und $Q(R)$ der Quotientenkörper.

(1) Ist $\text{grad}(f) > 0$, dann sind äquivalent

   (i) f ist irreduzibel in $R[X]$

   (ii) f ist irreduzibel in $Q(R)[X]$ und f ist primitiv.

(2) Ist f primitiv und ist f Teiler von g in $Q(R)[X]$, dann ist f Teiler von g in $R[X]$.

Wir listen zwei nützliche Irreduzibilitätskriterien.

3.7 Satz: (Einführung 7.12 und 7.16) Sei R ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv vom Grad $n > 0$.

(1) (Eisensteinsches Kriterium) Ist $p \in R$ prim mit $p \nmid a_n$, $p | a_i$ für $i = 0, 1, \ldots, n-1$, aber $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$, also auch in $Q(R)[X]$.

(2) (Reduktionskriterium) Sei $P \subset R$ ein Primideal, $a_n \notin P$ und $\overline{R} = R/P$. Sei $\overline{a}_i$ die Restklasse von a_i in $\overline{R}$ und $\overline{f} = \sum_{i=0}^{n} \overline{a}_i X^i \in \overline{R}[X]$. Ist $\overline{f}$ irreduzibel in $\overline{R}[X]$, dann ist f irreduzibel in $Q(R)[X]$ und $R[X]$.

3.8 Definition: Sei $f \in R[X]$. Wir nennen $a \in R$ eine *n-fache Nullstelle* von f, wenn $(X-a)^n$ Teiler von f ist, aber $(X-a)^{n+1} \nmid f$. Besitzt f n-fache Nullstellen mit $n \geq 2$, sagen wir, f hat *mehrfache Nullstellen.*

Wir nutzen die *formale Ableitung* Df eines Polynoms f, um Mehrfachnullstellen zu entdecken. Ist $f = \sum_{i=0}^{n} a_i X^i \in R[X]$, definieren wir

$$Df = \sum_{i=1}^{n} i a_i X^{i-1}.$$

Man prüft leicht nach, dass

$$\begin{aligned} D(f+g) &= D(f)+D(g) \\ D(fg) &= (Df)\cdot g + f\cdot D(g). \end{aligned}$$

3.9 Satz: Sei K ein Körper, $\mathrm{char}(K)=0$ und $0\neq f\in K[X]$. Dann besitzt f genau dann einen Teiler g^2 mit $\mathrm{grad}(g)>0$, wenn g Teiler von f und $D(f)$ ist.

Beweis: Angenommen $f=g^2\cdot h$ mit $\mathrm{grad}(g)>0$. Dann folgt

$$D(f)=2g\cdot D(g)\cdot h+g^2\cdot h,$$

so dass g auch $D(f)$ teilt.
Angenommen, für jeden irreduziblen Faktor g von f gilt $g^2\nmid f$. Dann haben wir $f=g\cdot h$, wobei g und h coprim sind. Angenommen g teilt auch

$$D(f)=D(g)\cdot h+g\cdot D(h)$$

dann teilt g auch $D(g)\cdot h$ und damit $D(g)$. Da $\mathrm{char}(K)=0$, gilt aber $\mathrm{grad}\,D(g)=\mathrm{grad}(g)-1$. Also kann g kein Teiler von $D(g)$ sein. □

3.10 Folgerung: Sei $K\subset F$ eine Körpererweiterung, $\mathrm{char}(K)=0$. Dann hat ein über K irreduzibles Polynom f keine Mehrfachnullstellen in F.

Beweis: Da f irreduzibel ist, sind $D(f)$ und f coprim. Also gibt es nach 2.7 Polynome $p,q\in K[X]$, so dass $p\cdot f+q\cdot D(f)=1$.
Da diese Gleichung auch in $F[X]$ gilt, sind f und $D(f)$ coprim in $F[X]$. Nach 3.9 hat f keine Mehrfachnullstelle in F. □

4 Körpererweiterungen

Sei $K\subset F$ eine Körpererweiterung und $A\subset F$ beliebig. Mit $K[A]$ bezeichnen wir den kleinsten Teilring und mit $K(A)$ den kleinsten Teilkörper von F, der K und A enthält. Ist A endlich und $F=K(A)$, heißt die Erweiterung F/K *endlich erzeugt*. Gilt $F=K(a)$ heißt F/K *einfache Erweiterung*.

4.1 Definition: $a\in F$ heißt *algebraisch* über K, wenn a Nullstelle eine Polynoms $0\neq f\in K[X]$ ist. Ansonsten heißt a *transzendent* über K. Die Körpererweiterung F/K heißt *algebraisch*, wenn jedes $a\in F$ über K algebraisch ist.

4.2 Satz: (Einführung 8.6) Sei F/K Körpererweiterung, $a \in F$ und $E_a : K[X] \to F$, $f \mapsto f(a)$ der Einsetzhomomorphismus. Dann sind äquivalent

(1) a ist algebraisch,

(2) E_a ist nicht injektiv,

(3) $K[a] = K(a)$,

(4) Kern E_a wird von einem irreduziblen normierten Polynom $f_a \in K[X]$ erzeugt.

f_a ist das eindeutig bestimmte normierte Polynom kleinsten Grades, das a als Nullstelle hat. Es wird das *Minimalpolynom* von a genannt.

Ist $K \subset F$ eine Körpererweiterung, dann definieren Addition und Multiplikation eine K-Vektorraumstruktur auf F. Die Dimension $\dim_K F$ dieses K-Vektorraums heißt *Grad der Körpererweiterung* F/K und wird mit $[F : K]$ bezeichnet. F/K heißt *endlich* oder *unendlich*, je nachdem ob $[F : K]$ endlich oder unendlich ist.

4.3 Satz: (Einführung 8.9) Sei F/K Körpererweiterung und $a \in F$ algebraisch über K mit Minimalpolynom f_a vom Grad n. Der Einsetzhomomorphismus $E_a : K[X] \to F$ induziert nach 1.2 einen Isomorphismus

$$\overline{E}_a : K[X]/(f_a) \cong K[a] = K(a).$$

Weiter ist $\{1, a, a^2, \ldots, a^{n-1}\}$ eine K-Basis von $K(a)$, so dass

$$\dim_K K(a) = [K(a) : K] = n = \operatorname{grad} f_a.$$

Wir erinnern an die

4.4 Gradformel: (Einführung 8.11) Sind $K \subset L \subset F$ Körpererweiterungen, dann gilt

$$[F : K] = [F : L] \cdot [L : K].$$

Genauer: Sind F/L und L/K endlich und ist $\{a_1, \ldots, a_k\}$ eine K-Basis von L und $\{b_1, \ldots, b_l\}$ eine L-Basis von F, dann ist $\{a_i \cdot b_j;\ i = 1, \ldots, k,\ j = 1, \ldots, l\}$ eine K-Basis von F.

Es folgt jetzt leicht

4.5 Satz: (Einführung 8.13 und 8.16) Seien $K \subset L \subset F$ Körpererweiterungen.

(1) F/K ist endlich $\iff$ F/K ist algebraisch und endlich erzeugt.

(2) F/K ist algebraisch $\iff$ L/K und F/L sind algebraisch.

Sei nun $f \in K[X]$ irreduzibel. Dann ist $(f) \subset K[X]$ maximal und damit $K[X]/(f)$ nach 1.4 ein Körper. Da

$$K \subset K[X] \xrightarrow{\text{proj.}} K[X]/(f)$$

als Körperhomomorphismus nach 1.6 injektiv ist, ist $K \subset K[X]/(f) =: F$ eine Körpererweiterung. Damit können wir f auch als Polynom über F auffassen. Sei $a = \text{proj}(X) \in F$. Da proj ein Ringhomomorphismus ist, gilt $E_a(f) = f(a) = f(\text{proj}(X)) = \text{proj}(f(X)) = 0$. Also ist a Nullstelle von f in F. Iterieren ist das Verfahren, erhalten wir einen Körper, über dem f *zerfällt*, d.h. ein Produkt linearer Polynome ist.

4.6 Definition: Sei $\mathcal{F} \subset K[X]$ eine Menge von nicht konstanten Polynomen und F/K eine Körpererweiterung. Wir sagen $\mathcal{F}$ *zerfällt über* F, wenn jedes $f \in \mathcal{F}$ über F zerfällt. Wird außerdem F über K von den Nullstellen der Polynome aus $\mathcal{F}$ erzeugt, heißt F *Zerfällungskörper* von $\mathcal{F}$.

Wir haben gesehen, dass Zerfällungskörper für endliche Mengen $\mathcal{F}$ immer existieren. Im Abschnitt 9 der Einführung wurde gezeigt, dass sie bis auf Isomorphie von Körpern eindeutig bestimmt sind. Man kann die Resultate mit Hilfe von Zorn's Lemma auf beliebige Mengen $\mathcal{F} \subset K[X]$ erweitern. Wir nehmen das ohne Beweis zur Kenntnis. Nimmt man $\mathcal{F} = K[X]$, erhält man den algebraischen Abschluss von K.

4.7 Definition: Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom aus $K[X]$ über K zerfällt. Ein *algebraischer Abschluss* von K ist ein Erweiterungskörper $K \subset F$, so dass F/K algebraisch und F algebraisch abgeschlossen ist.

4.8 Satz: (ohne Beweis) Jeder Körper K hat einen algebraischen Abschluss, bezeichnet mit $\overline{K}$, der bis auf K-Isomorphie (s. Definition 4.10) eindeutig gegeben ist.

Der Beweis der Eindeutigkeit macht sich folgendes Ergebnis zu Nutze, das aus einer einfachen Anpassung der Beweise der Sätze 9.4 und 9.4 der Einführung folgt.

4.9 Aufgabe: (1) Sei $K(a)/K$ einfache Körpererweiterung, a algebraisch über K mit Minimalpolynom $f = \sum_{i=0}^{n} c_i X^i$. Sei $\varphi_0 : K \to F$ ein Körperhomomorphismus und $\varphi_0(f) = \sum_{i=0}^{n} \varphi_0(c_i) X^i \in F[X]$. Dann definiert $\varphi \mapsto \varphi(a)$ eine Bijektion

$$\left\{ \begin{array}{c} \text{Körperhomomorphismen} \\ \varphi : K(a) \to F \text{ mit } \varphi|K = \varphi_0 \end{array} \right\} \cong \left\{ \begin{array}{c} \text{Nullstellen von} \\ \varphi_0(f) \text{ in } F \end{array} \right\}$$

(2) Sei F/K eine endliche Erweiterung und $\varphi_0 : K \to L$ ein Körperhomomorphismus in einen algebraisch abgeschlossenen Körper L. Dann besitzt φ_0 eine Erweiterung $\varphi : F \to L$, d.h. es gibt einen Körperhomomorphismus $\varphi : F \to L$, so dass $\varphi|K = \varphi_0$ ist. Ist $a \in F$, $f \in K[X]$ sein Minimalpolynom, und ist $b \in L$ eine Nullstelle von $\varphi_0(f)$, kann φ so gewählt werden, dass $\varphi(a) = b$ ist.

4.10 Definition: Seien F/K und L/K Körpererweiterungen. Ein Körperhomomorphismus $\varphi : F \to L$ heißt *K-Morphismus*, wenn $\varphi|K = \mathrm{id}_K$ ist. Die Gruppe $\mathrm{Gal}(F/K)$ der K-Automorphismen von F heißt *Galois-Gruppe* der Körpererweiterung F/K.

4.11 Aufgabe: Sei $f \in K[X]$, $\mathrm{Null}(f)$ die Menge der Nullstellen von f in F und $\sigma \in \mathrm{Gal}(F/K)$. Dann definiert σ eine Permutation von $\mathrm{Null}(f)$.

Im Kapitel II werden separable Erweiterungen wichtig sein.

4.12 Definition: Sei K ein Körper. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn seine irreduziblen Faktoren im algebraischen Abschluss $\overline{K}$ von K nur einfache Nullstellen haben. Ist F/K eine Körpererweiterung, dann heißt $a \in F$ *separabel*, wenn sein Minimalpolynom aus $K[X]$ separabel ist. Sind alle $a \in F$ separabel, nennt man die Körpererweiterung F/K *separabel*.

Aus 3.10 folgt

4.13 Satz: Ist $\mathrm{char}(K) = 0$, ist jedes $f \in K[X]$ separabel und damit auch jede Körpererweiterung $K \subset F$.

Weiter gilt

4.14 Satz: Ist $K \subset F$ eine Erweiterung endlicher Körper, dann ist F/K separabel.

Das folgt sofort aus folgenden zwei Ergebnissen der Einführung in die Algebra.

4.15 (Einführung 4.3) Ist K ein endlicher Körper, dann ist $\mathrm{char}(K) = p$ mit p prim und $|K|$ ist eine Potenz von p.

4.16 Satz: (Einführung 8.9 und dessen Beweis) Ist p prim und $k \geq 1$ aus $\mathbb{N}$, dann gibt es auf Isomorphie genau einen Körper K mit p^k Elementen. Er besteht aus den Nullstellen des Polynoms $f = X^{p^k} - X$. Insbesondere ist f separabel und K der Zerfällungskörper von f.

Wir benötigen später den Satz über primitive Elemente.

4.17 Definition: Ist $K \subset F$ einfache Körpererweiterung, dann heißt *a primitives Element* von F/K, falls $F = K(a)$ ist.

4.18 Satz: Sei $F = K[\alpha_1, \ldots, \alpha_r]$ endliche Erweiterung von K, und seien $\alpha_2, \ldots, \alpha_r$ separabel über K. Dann gibt es ein primitives Element $\gamma \in F$, so dass $F = K(\gamma)$.

Beweis: Ist K endlich, dann ist auch F endlich. Da endliche Untergruppen der multiplikativen Gruppe eines Körpers zyklisch sind (s. Aufgabe 4.21), ist $(F^*, \cdot)$ zyklisch. Für einen Erzeuger γ von $(F^*, \cdot)$ gilt dann $F = K(\gamma)$.
Sei jetzt K unendlich. Es genügt, den Satz für $r = 2$ zu zeigen, der Rest folgt durch Induktion, da $K[\alpha_1, \ldots, \alpha_r] = K[\alpha_1, \ldots, \alpha_{r-1}][\alpha_r]$ ist. Sei also $F = K(\alpha, \beta)$ und β separabel über K. Seien f und g aus $K[X]$ die Minimalpolynome von α und β. Seien weiterhin

$$\begin{array}{ll} \alpha_1 = \alpha, \quad \alpha_2, \ldots, \ \alpha_s & \text{die Nullstellen von } f \\ \beta_1 = \beta, \quad \beta_2, \ldots, \ \beta_t & \text{die Nullstellen von } g \end{array}$$

in einem algebraischen Abschluss $\overline{F}$ von F. Da g separabel ist, sind die β_i alle verschieden. Damit hat die Gleichung

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1 \quad j > 1$$

genau eine Lösung, nämlich $X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$. Da K unendlich ist, gibt es ein $c \in K$, das von allen diesen Lösungen verschieden ist, d.h.

$$\alpha_i + c\beta_j \neq \alpha + c\beta \quad \text{für } j \neq 1.$$

Behauptung: $F = K(\gamma)$ mit $\gamma = \alpha + c\beta$.
Beweis: $K(\gamma) \subset F = K(\alpha, \beta)$.

Die Polynome g und $f(\gamma - cX)$ aus $(K(\gamma))[X]$ haben β als Nullstelle. β ist ihre einzige gemeinsame Nullstelle in $\overline{F}$, denn für $j > 1$ gilt $\gamma - c\beta_j \neq \alpha_i$ für alle i, d.h. β_j ist nicht Nullstelle von $f(\gamma - cX)$. Also gilt

$$X - \beta = \mathrm{ggT}(g, f(\gamma - cX)) \quad \text{in } \overline{F}[X]$$

Das folgende Lemma zeigt, dass $X - \beta$ auch der ggT in $K(\gamma)[X]$ ist. Also ist $\beta \in K(\gamma)$ und damit auch $\alpha = \gamma - c\beta$. Es folgt $K(\alpha, \beta) \subset K(\gamma)$. □

4.19 Lemma: Seien $f, g \in K[X]$ und $d_K \in K[X]$, $d_F \in F[X]$ normierte Polynome, so dass $d_K = \mathrm{ggT}(f, g)$ in $K[X]$ und $d_F = \mathrm{ggT}(f, g)$ in $F[X]$. Dann gilt $d_K = d_F$.

Beweis: In $K[X]$ gilt $(d_K) = (f) + (g)$, also

$$K[X] \cdot d_K = K[X] \cdot f + K[X] \cdot g.$$

Es folgt

$$\begin{aligned} F[X] \cdot d_K &= F[X] \cdot K[X] \cdot d_K \\ &= F[X] \cdot K[X] \cdot f + F[X] \cdot K[X] \cdot g \\ &= F[X] \cdot f + F[K] \cdot g \end{aligned}$$

also $d_K = \mathrm{ggT}(f, g)$ in $F[X]$. □

Mit 4.13 und 4.14 erhalten wir

4.20 Folgerung: Ist $\mathrm{char}(K) = 0$ oder ist K endlich, dann ist jede endliche Erweiterung $K \subset F$ einfach.

Wir schließen mit ein paar Aufgaben.

4.21 Aufgabe: (1) Sei $(G, \cdot)$ eine abelsche Gruppe und seien $a_1, \ldots, a_n$ aus G Elemente mit $\mathrm{ord}(a_i) = k_i$. Sei $v = \mathrm{kgV}(k_1, \ldots, k_k)$. Dann gibt es ein $a \in G$ mit $\mathrm{ord}(a) = k$.

(Hinweis: Induktion nach n. Für $n = 2$ empfiehlt es sich, zunächst den Fall $\mathrm{ggT}(k_1, k_2) = 1$ zu behandeln.)

(2) Zeigen Sie: Sei K ein Körper. Dann ist jede endliche Untergruppe G von $(K^*, \cdot)$ zyklisch.

(Hinweis: Sei $G = \{a_1, \ldots, a_n\}$, $\mathrm{ord}(a_i) = k_i$ und $v = \mathrm{kgV}(k_1, \ldots, k_n)$. Betrachten Sie das Polynom $X^v - 1$ und wenden Sie Teil (1) an.)

4.22 Aufgabe: Sei K ein Körper und $\overline{K}$ sein algebraischer Abschluss. Sei $f \in K[X]$ und $Z \subset \overline{K}$ sein Zerfällungskörper. Zeigen Sie: Ist $\sigma : Z \to \overline{K}$ ein K-Morphismus, dann ist $\sigma(Z) \subset Z$ und die Zuordnung $x \mapsto \sigma(x)$ definiert einen K-Automorphismus von Z.

4.23 Aufgabe: (1) Sei F/K eine Körpererweiterung mit Galois-Gruppe G. Sei $U \subset G$ eine Untergruppe von G und

$$F^U = \{x \in F : \ \sigma(x) = x \ \forall \sigma \in U\}$$

Zeigen Sie: F^U ist ein Teilkörper von F, genannt *Fixkörper von* U.

(2) Sei K ein Körper, $\text{char}(K) = 0$, $f \in K[X]$ und Z ein Zerfällungskörper von f. Sei G die Galois-Gruppe von Z/K.

Zeigen Sie: $Z^G = K$.

5 Moduln und Algebren

Sei R ein Ring.

5.1 Definition: Ein *R-Modul* ist eine abelsche Gruppe $(M, +)$ mit einer R-Operation

$$R \times M \to M, \quad (r, m) \mapsto rm,$$

so dass

(1) $(r + s)m = rm + sm$

(2) $r(m + n) = rm + rn$

(3) $r(sm) = (rs)m$

(4) $1m = m$

für alle $r, s \in R$ und $m, n \in M$.
Eine *R-Algebra* ist ein R-Modul A mit einer Multiplikation

$$A \times A \to A, \quad (a, b) \mapsto a \cdot b,$$

so dass

(i) $(A, +, \cdot)$ ein Ring ist

(ii) $r(a \cdot b) = (ra) \cdot b = a \cdot (rb) \quad \forall a, b \in A, \forall r \in R.$

5.2 Konvention: Falls nicht ausdrücklich anders vermerkt, sind unsere Algebren alle kommutativ.

5.3 Bemerkung: Beachte, dass wir in unseren Axiomen dasselbe Symbol $+$ für **verschiedene** Additionen und im Falle von Algebren sogar drei verschiedene Multiplikationen haben.

R-Moduln und R-Algebren sind uns schon oft begegnet und werden uns immer wieder begegnen:

- Für einen Körper K sind die K-Moduln genau die K-Vektorräume.
- $\mathbb{Z}$-Moduln sind genau die abelschen Gruppen.
- R^n ist unter koordinatenweiser Addition und Multiplikation ein R-Modul.
- Ist $R \subset A$ eine Ringerweiterung, dann definieren die Addition und Multiplikation in A eine R-Algebrastruktur auf A.
- Ist $M_n(R)$ die Menge der $(n \times n)$-Matrizen über einem kommutativen Ring R, dann ist $M_n(R)$ mit der üblichen Matrizen-Addition und -Multiplikation eine **nicht-kommutative** R-Algebra.

Ein *R-Teilmodul* N eines R-Moduls M wird genauso definiert wie Untervektorräume. Dasselbe gilt für den *Quotientenmodul* M/N: Man nimmt die Faktorgruppe M/N und definiert

$$r\overline{m} = \overline{rm},$$

wobei $\overline{m} = m + N$ die Nebenklasse von m ist.

Die R-Teilmoduln des R-Moduls R^1 sind genau die Ideale von R.

Ist M ein R-Modul und $A \subset M$ eine Teilmenge, dann bezeichnen wir mit $\langle A \rangle_R$ den kleinsten R-Teilmodul von M, der A enthält. Er heißt der *von A erzeugte Teilmodul* von M und besteht aus allen endlichen R-Linearkombinationen von Elementen aus A. Wir nennen A ein *Erzeugendensystem* von $\langle A \rangle_R$, und M heißt *endlich erzeugt*, wenn es eine endliche Menge $A \subset M$ gibt, so dass $\langle A \rangle_R = M$.

5.4 Definition: Sei M ein R-Modul. Eine Teilmenge $A \subset M$ heißt *R-linear unabhängig*, falls für jede endliche Teilmenge $\{a_1, \ldots, a_n\} \subset A$ gilt

$$r_1 a_1 + \ldots + r_n a_n = 0 \quad \Rightarrow \quad r_1 = r_2 = \ldots = r_n = 0$$

(hier sind die $r_i \in R$). Eine *R-Basis* von M ist ein R-linear unabhängiges Erzeugendensystem.

Wie in der Linearen Algebra zeigt man: $A \subset M$ ist genau dann eine Basis, wenn jedes $m \in M$ eindeutig als endliche R-Linearkombination von Elementen aus A darstellbar ist.

5.5 Definition: Ein R-Modul M heißt *frei*, wenn er eine Basis A besitzt. Die Kardinalzahl $|A|$ von A heißt *Rang* von M.

5.6 Definition: Seien M und N R-Moduln. Eine Abbildung

$$f : M \to N,$$

heißt *R-linear*, wenn für alle $a, b \in M$ und alle $r \in R$ gilt

$$f(a+b) = f(a) + f(b) \quad \text{und} \quad f(ra) = rf(a).$$

Wie in der Linearen Algebra zeigt man

5.7 Satz: Sei M ein freier R-Modul mit Basis A, sei N ein beliebiger R-Modul und $f : A \to N$ eine beliebige Abbildung. Dann gibt es genau eine R-lineare Erweiterung $\overline{f} : M \to N$ von f.

5.8 Satz: Ist M ein freier R-Modul vom Rang $n < \infty$, dann ist M R-linear isomorph zu R^n.

Ist $f : M \to N$ eine R-lineare Abbildung und ist M frei mit Basis $\mathcal{B}_1 = \{a_1, \ldots, a_k\}$ und N frei mit Basis $\mathcal{B}_2 = \{b_1, \ldots, b_k\}$, dann wird f bzgl. dieser Basen durch eine $(l \times k)$-Matrix $\mathrm{Mat}_{\mathcal{B}_2}^{\mathcal{B}_1}(f) = (r_{ij})$ beschrieben, die durch

$$f(a_j) = \sum_{i=1}^{l} r_{ij} b_i$$

gegeben ist.
Während all dies aus der Linearen Algebra vertraut ist, ist das folgende Resultat weniger selbstverständlich.

5.9 Satz: Sei R ein Hauptidealring und F ein freier R-Modul von Rang $n < \infty$. Dann ist jeder Teilmodul $M \subset F$ frei vom Rang $\leq n$.

Beweis:: Induktion nach n.
Für $n = 0$ ist $F = M = \{0\}$
Schritt von $n-1$ nach n: Sei $\mathcal{B} = \{z_1, \ldots, z_n\}$ Basis von F und $T = \langle\{z_1, \ldots, z_{n-1}\}\rangle_R$. Dann ist $M \cap T$ ein Teilmodul von T und damit nach Induktionsannahme frei. Sei $\{y_1, \ldots, y_k\}$ Basis von $M \cap T$, $k \leq n-1$.

Ist $M = M \cap T$ sind wir fertig.
Ist $M \neq M \cap T$, dann gibt es ein $z \in M \backslash (M \cap T)$. Sei

$$z = r_1 z_1 + \ldots + r_{n-1} z_{n-1} + r_n z_n$$

$r_n \neq 0$, da sonst $z \in M \cap T$. Sei

$$J = \{r \in R;\ \exists y \in T,\ \text{so dass } r z_n + y \in M\}.$$

Man prüft leicht nach, dass J ein Ideal ist. Da R ein Hauptidealring ist, gibt es ein s, so dass $J = (s)$. Da $r_n \in J$ ist, ist $s \neq 0$. Da $s \in J$ ist, gibt es ein $v \in T$, so dass $y_{k+1} := s \cdot z_n + v \in M$.
Behauptung: $\{y_1, \ldots, y_{k+1}\}$ ist Basis von M.
Beweis: Sei $r_1 y_1 + \ldots + r_k y_k + r_{k+1} y_{k+1} = 0$
$y := r_1 y_1 + \ldots r_k y_k$ ist in $M \cap T$, und $r_{k+1} y_{k+1} = r_{k+1} s z_n + r_{k+1} v$. Nun ist $y + r_{k+1} v$ aus T, also Linearkombination von $z_1, \ldots, z_{n-1}$. Es folgt $r_{k+1} \cdot s = 0$, weil $z_1, \ldots, z_n$ eine Basis ist. Da $s \neq 0$ ist, ist $r_{k+1} = 0$. Da $y_1, \ldots, y_k$ Basis von $M \cap T$, folgt $r_1 = \ldots = r_k = 0$.
Also sind $y_1, \ldots, y_{k+1}$ linear unabhängig.
Behauptung: $M = \langle \{y_1, \ldots, y_{k+1}\} \rangle_R$
Sei $x \in M$. Da $\mathcal{B}$ Basis von F ist, besitzt x eine Darstellung.

$$x = r_1 z_1 + \ldots + r_n z_n = y + r_n z_n$$

mit $y = r_1 z_1 + \ldots r_{n-1} z_{n-1} \in T$. Da $x \in M$ ist, ist $r_n \in J$, also von der Form $r_n = q \cdot s$. Es folgt

$$x = q \cdot s \cdot z_n + y = q \cdot s \cdot z_n + q \cdot v + y - q \cdot v = q \cdot y_{k+1} + (y - q \cdot v).$$

Da $v \in T$ ist, ist $y - q \cdot v$ aus T. Da $x - q \cdot y_{k+1} \in M$, ist auch $y - q \cdot v \in M$. Also ist $y - q \cdot v \in M \cap T$ und damit Linearkombination von $y_1, \ldots, y_k$. $\square$
Wir benötigen noch eine Verschärfung dieses Resultat, das für Moduln über Hauptidealringen gilt, das wir aber nur für euklidische Ringe formulieren und beweisen.

5.10 Satz: Sei R ein euklidischer Ring, F ein freier R-Modul vom Rang n und M ein Teilmodul. Dann ist M frei vom Rang $m \leq n$, und es gibt eine Basis $\{u_1, \ldots, u_n\}$ von F und Elemente $\alpha_1, \ldots, \alpha_m \in R$, so dass $\{\alpha_1 u_1, \ldots, \alpha_m u_m\}$ Basis von M ist.

Beweis: Sei $\mathcal{B}_F$ eine Basis von F. Nach 5.9 besitzt M eine Basis $\mathcal{B}_M$ von m Elementen. Bzgl. dieser Basen wird die Inklusion $M \subset F$ durch eine $(n \times m)$-Matrix A gegeben. Ist $\{z_1, \ldots, z_n\}$ eine Basis, dann wissen wir aus der Linearen Algebra

(1) Ersetzen wir z_i durch rz_i, wobei $r \in R^*$ invertierbar ist, erhalten wir wieder eine Basis.

(2) Ersetzen wir z_i durch $z_i + rz_j$, wobei $i \neq j$ und $r \in R$ beliebig ist, erhalten wir wieder eine Basis.

Wenden wir diese Operation auf $\mathcal{B}_F$ an, erhalten wir die Inklusionsmatrix A' bzgl. der neuen Basis, indem wir die inversen Operationen auf ihre Zeilen anwenden, d.h. wir müssen bei (1) die i-te Zeile von A durch ihr r^{-1}-faches ersetzen und bei (2) das r-fache der i-ten Zeile von der j-ten abziehen. Wenden wir die Operationen auf $\mathcal{B}_M$ an, gilt das entsprechende für Spalten von A.

D.h. Zeilen- und Spaltenoperationen von A vom Typ (1) und (2) erhalten wir durch Basiswechsel in F und M.

Das Vertauschen von Zeilen und Spalten entspricht einer Umordnung der Basisvektoren in den Basen von F bzw. M.

Unser Ziel ist es, die Matrix $A = (a_{ij})$ auf die Form

$$D = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_m \\ \hline 0 & & 0 \end{pmatrix}$$

zu bringen. Ist $A = (0)$, dann ist $M = 0$, und wir haben nichts zu zeigen. Sonst bringen wir A auf die Form

$$C = \left(\begin{array}{c|ccc} \alpha_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & (c_{ij}) & \\ 0 & & & \end{array}\right)$$

und iterieren.

Durch Zeilen- und Spaltenvertauschung erreichen wir, dass $a_{11} \neq 0$ und von allen $a_{ij} \neq 0$ den kleinsten Grad hat. Sei $\delta : R\backslash\{0\} \to \mathbb{N}$ die Gradabbildung. Gibt es ein a_{1j} oder ein a_{i1} das nicht von a_{11} geteilt wird, etwa a_{1j}, dann teilen wir mit Rest

$$a_{1j} = q \cdot a_{11} + r_{1j} \quad \text{mit } \delta(r_{1j}) < \delta(a_{11}).$$

Dann ziehen wir das q-fache der ersten Spalte von der j-ten ab und vertauschen anschließend die erste mit der j-ten Spalte. Die neue Matrix hat r_{ij}

an Position $(1,1)$. Wir fahren fort, bis das Element an Position $(1,1)$ alle übrigen Elemente der ersten Zeile und Spalte teilt. Nach 2.9 wird das in endlich vielen Schritten erreicht, weil alle Elemente aus R von minimalem Grad invertierbar sind.

Ziehen wir jetzt geeignete Vielfache der ersten Zeile von den übrigen Zeilen und der ersten Spalte von den übrigen ab, erhalten wir eine Matrix der Form C. Wir wenden jetzt unser Verfahren auf die Teilmatrix (c_{ij}) von C an und fahren fort bis wir die Form D erhalten.

Sind $\{v_1, \ldots, v_m\}$ und $\{u_1, \ldots, u_n\}$ die Basen von M bzw. F bzgl. derer die Inklusion $i : M \subset F$ die Matrix D hat, dann gilt

$$v_i = i(v_i) = \alpha_i u_i.$$

□

6 Symmetrische Polynome

Sei R ein Ring und $R[X_1, \ldots, X_n]$ der Polynomring über R in den Unbestimmten $X_1, \ldots, X_n$.

6.1 Definition: Ein Polynom $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ heißt *symmetrisch*, wenn für jede Permutation $\tau \in \Sigma_n$ gilt

$$f(X_{\tau(1)}, \ldots, X_{\tau(n)}) = f(X_1 \ldots, X_n)$$

Beispiele sind:

6.2 Die elementarsymmetrischen Polynome: $p_1, \ldots, p_n \in R[X_1, \ldots, X_n]$. Dabei ist p_i die Summe aller Monome vom Totalgrad i, deren Faktoren alle verschieden sind:

$$\begin{aligned}
p_1 &= X_1 + X_2 + \ldots + X_n \\
p_2 &= \sum_{1 \le i < j \le n} X_i X_j = X_1X_2 + X_1X_3 + \ldots + X_1X_n + \ldots + X_{n-1}X_n \\
p_3 &= \sum_{1 \le i < j < k \le n} X_i X_j X_k \\
&\vdots \\
p_n &= X_1X_2X_3 \cdot \ldots \cdot X_n
\end{aligned}$$

Die Polynome $X_1 + 2X_2$ oder $X_1^2X_2$ aus $R[X_1, X_2]$ sind nicht symmetrisch.

6.3 Satz über symmetrische Polynome: Jedes symmetrische Polynom $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ lässt sich als Polynom in den elementarsymmetrischen Polynomen $p_1, \ldots, p_n$ mit Koeffizienten in R schreiben, d.h.

$$f \in R[p_1, \ldots, p_n] \subset R[X_1, \ldots, X_n].$$

Beweis: Wir ordnen die Monome $X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} \in R[X_1, \ldots, X_n]$, $i_k \in \mathbb{N}$ für $1 \leq k \leq n$ zunächst nach den Totalgraden

$$X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} > X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n}, \qquad (*)$$

wenn $i_1 + \ldots + i_n > j_1 + \ldots + j_n$. Sind die Totalgrade gleich, ordnen wir sie lexicographisch nach den Exponenten, d.h. $(*)$ gilt, wenn

$$i_1 = j_1, \ldots, i_k = j_k, \text{ aber } i_{k+1} > j_{k+1}.$$

Beispiel:

$$X_1 X_2^2 X_3^2 > X_1^2 X_2 X_3 > X_1 X_2^2 X_3 > X_2^2 X_3^2$$

Sei nun $X_1^{k_1} \ldots X_n^{k_n}$ das größte Monom in f mit einem Koeffizienten $c \neq 0$. Da f symmetrisch ist, enthält es alle Monome, die aus $X_1^{k_1} \ldots X_n^{k_n}$ hervorgehen, indem man die X_i vertauscht, etwa $X_1^{k_2} X_2^{k_3} X_3^{k_1} X_4^{k_4} \ldots X_n^{k_n}$ für $\tau = (1, 3, 2) \in \Sigma_n$.

Es folgt $k_1 \geq k_2 \geq \ldots \geq k_n$.

Sind $g_1 > g_2$ und $h_1 > h_2$ Monome, dann folgt

$$g_1 \cdot h_1 > g_2 \cdot h_2.$$

Das größte Monom in p_i ist $X_1 X_2 \ldots X_i$. Damit ist

$$X_1^{d_1 + \ldots + d_n} \cdot X_2^{d_2 + d_3 + \ldots + d_n} \cdot \ldots \cdot X_n^{d_n}$$

das größte Monom in $p_1^{d_1} p_2^{d_2} \cdot \ldots \cdot p_n^{d_n}$. Damit ist das größte Monom in

$$g = f - c \cdot p_1^{k_1 - k_2} \cdot p_2^{k_2 - k_3} \cdot \ldots \cdot p_n^{k_n}$$

kleiner als das größte Monom in f. Wir fahren nun mit dem größten Monom in g fort. Durch Abwärtsinduktion nach der Größe der Monome folgt der Satz. □

Der Beweis gibt uns eine konstruktive Methode, ein symmetrisches Polynom als Polynom in den elementarsymmetrischen Polynomen zu schreiben.

6.4 Beispiel: Die Monome des symmetrischen Polynoms

$$f = X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2$$

sind nach Größe geordnet. Wir haben $n = 3$, $k_1 = 2$, $k_2 = 1$, $k_3 = 0$ und $c = 1$. Damit ist

$$\begin{aligned} g = f - p_1 \cdot p_2 &= f - (X_1 + X_2 + X_3) \cdot (X_1X_2 + X_1X_3 + X_2X_3) \\ &= f - (X_1^2X_2 + X_1^2X_3 + X_1X_2X_3 + X_1X_2^2 + X_1X_2X_3 \\ &\qquad + X_2^2X_3 + X_1X_2X_3 + X_1X_3^2 + X_2X_3^2) \\ &= -3X_1X_2X_3 \\ &= -3p_3 \end{aligned}$$

Es folgt $f = p_1 \cdot p_2 - 3p_3$.

6.5 Folgerung: Sei $R \subset A$ eine Ringerweiterung und $f = X^n + a_1X^{n-1} + \ldots + a_n \in R[X]$, so dass f über A zerfällt, d.h.

$$f = \prod_{i=1}^{n}(X - \alpha_i) \quad \text{mit } \alpha_i \in A.$$

Dann gilt:

(1) $a_i = (-1)^i p_i(\alpha_1, \ldots, \alpha_n)$ (Beachte: a_i ist der Koeffizient von X^{n-i}.)

(2) Ist $g \in R[X_1, \ldots, X_n]$ symmetrisch, dann ist $g(\alpha_1, \ldots, \alpha_n) \in R$.

Beweis: (1) folgt durch Ausmultiplizieren von $\prod_{i=1}^{n}(X - \alpha_i)$ und Koeffizientenvergleich. Damit ist $p_i(\alpha_1, \ldots, \alpha_n) \in R$.
Teil (2) folgt aus 6.3. □

Teil II
Ringe ganzer Zahlen

7 Ganze Zahlen

7.1 Definition: Sei R ein Ring und A eine R-Algebra. Ein Element $a \in A$ heißt *ganz*, genauer *ganz algebraisch* über R, wenn es ein *normiertes* Polynom

$f \in R[X]$ gibt, so dass $f(a) = 0$ in A gilt. (Ist $f = \sum_{i=0}^{n} r_k X^i$, dann ist $f(a) = \sum_{i=0}^{n} r_i a^i \in A$, da A ein R-Modul ist.) Wir nennen die resultierende Gleichung

$$a^n + r_{n-1}a^{n-1} + \ldots + r_0 = 0$$

die *Ganzheitsgleichung* für $a \in A$ über R.

7.2 Beispiele: (1) Sind $K \subset F$ Körper, dann gilt für $a \in F$:

$$a \text{ ganz über } K \iff a \text{ algebraisch über } K.$$

(2) Seien $p_1, \ldots, p_n \in K[X_1, \ldots, X_n]$ die elementarsymmetrischen Polynome. Für die Ringerweiterung $K[p_1, \ldots, p_n] \subset K[X_1, \ldots, X_n]$ ist jedes X_i ganz über $K[p_1, \ldots, p_n]$.

Beweis: X_i ist Nullstelle des normierten Polynoms

$$f = \prod_{i=1}^{n} (X - X_i).$$

Nach 6.5 gilt

$$f = X^n + \sum_{i=1}^{n} (-1)^i p_i(X_1, \ldots, X_n) \cdot X^{n-i} \in K[p_1, \ldots, p_n][X].$$

□

7.3 Aufgabe: $d \in \mathbb{Z}$ heißt *quadratfrei*, falls $d \neq 0, 1$ und für jede Primzahl p gilt $p^2 \nmid d$. Sei d quadratfrei und

$$\mathcal{O}(\sqrt{d}) = \begin{cases} \{a + b\sqrt{d} \in \mathbb{C};\ a, b \in \mathbb{Z}\}, & \text{falls } d \not\equiv 1 \mod 4 \\ \{\frac{a+b\sqrt{d}}{2} \in \mathbb{C};\ a, b \in \mathbb{Z},\ a \equiv b \mod 2\}, & \text{falls } d \equiv 1 \mod 4 \end{cases}$$

Zeigen Sie:

(1) $\mathcal{O}(\sqrt{d})$ ist Teilring des Körpers $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$

(2) $\mathcal{O}(\sqrt{d})$ ist die Menge der über $\mathbb{Z}$ ganzen Elementen von $\mathbb{Q}(\sqrt{d})$.

Wir wollen nun einige wichtige Resultate über algebraische Elemente auf ganz algebraische Elemente erweitern.

7.4 Satz: Ist A eine R-Algebra, die als R-Modul endlich erzeugt ist, dann ist jedes Element $a \in A$ ganz über R.

Beweis: Sei $\{\beta_1, \ldots, \beta_n\}$ ein Erzeugendensystem von A als R-Modul. Indem wir eventuell $1 \in A$ hinzufügen, dürfen wir annehmen, dass $\beta_1 = 1$ ist. Indem wir R gegebenfalls durch sein Bild unter dem Ringhomomorphismus

$$\varphi : R \to A, \quad r \mapsto r \cdot 1$$

ersetzen, dürfen wir annehmen, dass $R \subset A$. Da $\{\beta_1, \ldots, \beta_n\}$ den R-Modul A erzeugt, haben wir für das gegebene a und jedes $1 \leq j \leq n$ eine Gleichung

$$a \cdot \beta_j = \sum_{k=1}^{n} r_{jk}\beta_k \quad \text{mit } r_{jk} \in R$$

und damit ein Gleichungssystem

$$\sum_{k=1}^{n}(r_{jk} - \delta_{jk}a) \cdot x_k = 0 \qquad 1 \leq j \leq n \tag{$*$}$$

mit dem Kroneckersymbol δ_{jk}. Das Gleichungssystem hat das Tupel $(\beta_1, \ldots, \beta_n)$ als nicht-trivale Lösung. Wäre A ein Körper, könnten wir daraus schließen, dass $\det(r_{jk} - a\delta_{jk}) = 0$. Damit wäre a Nullstelle des charakteristischen Polynoms $\det(r_{jk} - X\delta_{jk})$. Dieses Polynom ist normiert und hat Koeffizienten in R, weil die $r_{jk} \in R$ sind. Da A kein Körper ist, argumentieren wir wie folgt: Sei $C = (c_{jk}) = (r_{jk} - a\delta_{jk})$. Nach dem Laplace'schen Entwicklungsatz gilt

$$\det C \cdot E_n = C^* \cdot C,$$

wobei $C^* = (c_{ij}^*)$ die zu C adjungierte Matrix ist. Aus $(*)$ erhalten wir

$$0 = \sum_{j=1}^{n} c_{ij}^* \left(\sum_{k=1}^{n} c_{jk} \cdot \beta_k \right) = \sum_{k,j=1}^{n} c_{ij}^* \cdot c_{jk} \cdot \beta_k = \sum_{k=1}^{n} \det C \cdot \delta_{ik} \cdot \beta_k = \det C \cdot \beta_i.$$

Da $\beta_1 = 1$, folgt $\det C = 0$. Wir sind fertig. □

7.5 Definition: Eine Ringerweiterung $R \subset A$ heißt *ganz*, wenn jedes $a \in A$ ganz über R ist.
Die Ringerweiterung heißt *endlich*, wenn A als R-Modul endlich erzeugt ist.

7.6 Jede endliche Ringerweiterung ist nach 7.4 ganz.

7.7 Ganzheitskriterium: Seien $R \subset A$ Ringe. Für $a \in A$ sind äquivalent

(1) a ist ganz über R.

(2) $R[a] \subset A$ ist als R-Modul endlich erzeugt.

(3) Es gibt eine Unteralgebra $B \subset A$, die a enthält und als R-Modul endlich erzeugt ist.

Beweis: (1) $\Rightarrow$ (2): Nach Definition ist $R[a] = \{g(a); q \in R[X]\} \subset A$. Sei $f \in R[X]$ ein normiertes Polynom vom Grad n mit $f(a) = 0$ in A. Da f normiert ist, gibt es nach dem Divisionsalgorithmus Polynome $q, r \in R[X]$, so dass

$$g = q \cdot f + r \qquad r = 0 \text{ oder } \operatorname{grad} r < n.$$

Da $f(a) = 0$ ist, ist $g(a) = r(a)$, und somit ist $\{1, a, a^2, \ldots, a^{n-1}\}$ ein Erzeugendensystem von $R[a]$.
(2) $\Rightarrow$ (3): Nehme $B = R[a]$.
(3) $\Rightarrow$ (1): folgt aus 7.6. □

7.8 Satz: (vergl. 4.5) Sind $R \subset A$ und $A \subset B$ endliche Ringerweiterungen, dann ist auch $R \subset B$ endlich.

Beweis: Sei $A = Ra_1 + \ldots + Ra_k$ und $B = A \cdot b_1 + \ldots + A \cdot b_l$. Dann ist

$$B = Ra_1b_1 + \ldots + Ra_kb_1 + \ldots + Ra_1b_l + \ldots + Ra_kb_l.$$

□

7.9 Lemma: Für eine Ringerweiterung $R \subset A$ sind äquivalent

(1) Es gibt endlich viele Elemente $a_1, \ldots, a_n$ in A, die über R ganz sind, so dass $A = R[a_1, \ldots, a_n]$.

(2) $R \subset A$ ist endlich.

Beweis: (2) $\Rightarrow$ (1) ist klar: Ist $\{a_1, \ldots, a_n\}$ ein Erzeugendensystems des R-Moduls A, dann gilt $A = R[a_1, \ldots, \_n]$. Nach 7.6 ist jedes a_i ganz über R.
(1) $\Rightarrow$ (2): Vorsicht, $a_1, \ldots, a_n$ erzeugen A als Ring, nicht als R-Modul!
Wir beweisen diesen Teil durch Induktion nach n. Für $n = 0$ ist nichts zu zeigen. Sei also $n \geq 1$ und $B = R[a_1, \ldots, a_{n-1}]$. Dann ist $A = B[a_n]$, und a_n ist ganz über B. Nach 7.7.2 ist $B \subset A$ endlich. Nach Induktion ist $R \subset B$ endlich. Also ist auch $R \subset A$ endlich. □

7.10 Definition und Satz: Sei $R \subset A$ eine Ringerweiterung. Dann ist

$$C = \{a \in A;\ a \text{ ist ganz über } R\}$$

ein Unterring von A, der R umfasst. C heißt *ganzer Abschluss* von R in A.

Beweis: Offensichtlich gilt $R \subset C$. Sind $a, b \in C$, dann ist $R \subset R[a, b]$ nach 7.9 endlich, also sind $a \cdot b$ und $a \pm b$ ganz über R nach 7.6. □

7.11 Definition: Sei $R \subset A$ eine Ringerweiterung. R heißt *ganz abgeschlossen* in A, wenn R mit seinem ganzen Abschluss in A übereinstimmt.
Ist R ein **Integritätsring**, dann heißt R *ganz abgeschlossen*, wenn R in seinem Quotientenkörper ganz abgeschlossen ist.

7.12 Satz: Sei $R \subset A$ Ringerweiterung und C der ganze Abschluss von R in A, dann ist C ganz abgeschlossen in A.

Beweis: Sei $a \in A$ ganz über C und

$$a^n + c_{n-1}a^{n-1} + \ldots + c_0 = 0 \quad \text{mit} \quad c_i \in C$$

eine Ganzheitsgleichung für a über C. Dann ist a ganz über $R[c_0, \ldots, c_{n-1}]$. Da jedes c_i über R ganz ist, ist $R \subset R[c_0, \ldots, c_{n-1}]$ nach 7.9 endlich. Da $R[c_0, \ldots, c_{n-1}] \subset R[c_0, \ldots, c_{n-1}][a]$ nach 7.7 endlich ist, ist auch $R \subset R[c_0, \ldots, c_{n-1}][a]$ endlich. Nach 7.6 ist a ganz über R, also $a \in C$. □

7.13 Satz: Für Ringe $R \subset A \subset B$ gilt:

$$R \subset A \text{ ganz und } A \subset B \text{ ganz} \iff R \subset B \text{ ganz.}$$

Beweis: Sei C der ganze Abschluss von R in B.
"$\Rightarrow$": Da $R \subset A$ ganz ist, folgt $A \subset C$. Da $A \subset B$ ganz ist, ist auch $C \subset B$ ganz. Aber C ist ganz abgeschlossen in B, so dass $C = B$. Also ist $R \subset B$ ganz.
"$\Leftarrow$": trivial, dann jedes $b \in B$ ist ganz über R. □

7.14 Lemma: Sei R Unterring eines Körpers F. Sei $a \in F$ algebraisch über dem Quotientenkörper K von R (beachte, die Inklusion $R \subset F$ erweitert zu einem Monomorphismus $K \subset F$). Dann gibt es ein $r \neq 0$ aus R, so dass $r \cdot a$ ganz über R ist.

Beweis: Sei $f = X^n + c_{n-1}X^{n-1} + \ldots + c_0$ aus $K[X]$ das Minimalpolynom von a. Sei r das Produkt der Nenner der c_i. Dann ist $r \cdot c_i \in R$ für $i = 0, \ldots, n-1$. Multiplizieren wir die Gleichung $f(a) = 0$ mit r^n, erhalten wir

$$0 = (ra)^n + r \cdot c_{n-1}(ra)^{n-1} + r^2 c_{n-2}(ra)^{n-2} + \ldots + r^n \cdot c_0.$$

Dies ist die Ganzheitsgleichung für $r \cdot a$. □

7.15 Satz: Jeder faktorielle Ring R ist ganz abgeschlossen.

Beweis: Sei K der Quotientenkörper von R und $\frac{r}{s} \in K$ Nullstelle eines normierten Polynoms $f \in R[X]$. Nach dem Satz von Vieta gilt $s|1$, d.h. s ist eine Einheit in R und $\frac{r}{s} = r \cdot s^{-1} \in R$. □

7.16 Sei $R \subset A$ eine Ringerweiterung und $f : A \to B$ ein Ringhomomorphismus. Ist $a \in A$ ganz über R, dann ist $f(a)$ ganz über $f(R)$.

Beweis: Wende f auf die Ganzheitsgleichung von a an. □

7.17 Satz: Sei K der Quotientenkörper eines Integritätsringes R und $K \subset F$ eine endliche Körpererweiterung. Sei $a \in F$ ganz über R und R ganz abgeschlossen. Dann liegt das Minimalpolynom $f \in K[X]$ von a bereits in $R[X]$.

Beweis: Sei Z Zerfällungskörper von f, und $f = \prod_{i=1}^{n}(X - a_i)$ in $Z[X]$, wobei $a_1 = a$. Nach 4.9 gibt es Erweiterungen von id_K zu Körperhomomorphismen

$$\varphi_i : K(a) \to Z, \quad a \mapsto a_i.$$

Nach 7.16 ist a_i ganz über $\varphi_i(R) = R$. Ist $f = X^n + c_{n-1}X^{n-1} + \ldots + c_0$, so gilt nach 6.5

$$c_{n-i} = (-1)^i p_i(a_1, \ldots, a_n),$$

wobei p_i das i-te symmetrische Polynom ist. Nach 7.10 sind damit alle c_i ganz über R. Da $c_i \in K$ und R ganz abgeschlossen in K ist, sind alle $c_i \in R$, also $f \in R[X]$. □

7.18 Aufgabe: (1) Zeigen Sie: Sei R ganz abgeschlossener Integritätsring und K sein Quotientenkörper. Sei $f \in R[X]$ normiert und seien $g, h \in K[X]$ normierte Polynome, so dass

$$f = g \cdot h \quad \text{in } K[X].$$

Dann gilt $g, h \in R[X]$.

(2) Beweisen Sie 7.17 mit Hilfe von (1).

7.19 Satz: Sei $R \subset F$ ganze Ringerweiterung und F ein Körper. Dann ist auch R ein Körper.

Beweis: Sei $a \neq 0$ aus R. Da $\frac{1}{a} \in F$ ganz über R ist, erfüllt es eine Ganzheitsgleichung mit Koeffizienten $c_i \in R$

$$\left(\frac{1}{a}\right)^n + c_{n-1}\left(\frac{1}{a}\right)^{n-1} + \ldots + c_0 = 0.$$

Wir multiplizieren mit a^{n-1} und erhalten

$$\frac{1}{a} = -c_{n-1} - ac_{n-2} - \ldots - c_0 a^{n-1} \in R.$$

□

8 Norm und Spur

Sei R ein Ring, A eine nicht notwendig kommutative R-Algebra und M ein A-Modul. Dann ist M auch ein R-Modul vermöge des Ringhomomorphismus

$$\varphi : R \to A, \quad r \mapsto r \cdot 1.$$

8.1 Jedes $\alpha \in A$ definiert eine R-lineare Abbildung

$$\alpha_{M/R} : M \to M, \quad x \mapsto \alpha \cdot x.$$

Wenn wir $\alpha_{M/R}$ studieren, wollen wir stets annehmen, dass M ein endlich erzeugter **freier** R-Modul ist. Ist $\mathcal{B} = \{e^1, \ldots, e^n\}$ eine R-Basis von M, dann wird $\alpha_{M/R}$ bzgl. $\mathcal{B}$ durch eine Matrix $C(\alpha) = (c_{ik})$ mit $c_{ik} \in R$ gegeben. Mit Hilfe von $C(\alpha)$ kann man das charakteristische Polynom, die Spur und die Determinante von $\alpha_{M/R}$ definieren (s. 8.3). Sie sind unabhängig von der Wahl der Basis.

Ist R ein Körper und damit M ein endlichdimensionaler Vektorraum, besitzt $\alpha_{M/R}$ auch ein Minimalpolynom. Es ist das eindeutig gegebene normierte Polynom in $R[X]$, das den Kern der Einsetzabbildung

$$R[X] \to \mathrm{End}_R M, \quad p \mapsto p(\alpha_{M/R})$$

erzeugt. Hier steht $\mathrm{End}_R M$ für die (nicht kommutative) R-Algebra der R-linearen Abbildungen $M \to M$ mit der Komposition als Algebramultiplikation.

8.2 Definition: Wir bezeichnen das charakteristische Polynom von $\alpha_{M/R}$ mit $P_{M/R}(\alpha)$ und definieren

$$S_{M/R}(\alpha) := \mathrm{Spur}(\alpha_{M/R}), \quad N_{M/R}(\alpha) = \det(\alpha_{M/R}).$$

Wir nennen $S_{M/R}(\alpha)$ die *Spur* und $N_{M/R}(\alpha)$ die *Norm* von α.

8.3 Aus der Linearen Algebra sollte bekannt sein (wir benutzen die Bezeichnungen von 8.1):

$$\begin{aligned} P_{M/R}(\alpha; X) &= \det(X \cdot E_n - C(\alpha)) = X^n + r_{n-1}X^{n-1} + \ldots + r_1 X + r_0 \in R[X] \\ S_{M/R}(\alpha) &= -r_{n-1} = \sum_{i=1}^{n} c_{ii} \\ N_{M/R}(\alpha) &= (-1)^n r_0 = \det C(\alpha). \end{aligned}$$

Ist R ein Körper und $\mu(\alpha; X)$ das Minimalpolynom von $\alpha_{M/R}$, dann ist $\mu(\alpha; X)$ Teiler von $P_{M/R}(\alpha; X)$, und jeder Primteiler von $P_{M/R}(\alpha; X)$ ist Teiler von $\mu(\alpha; X)$.

8.4 Elementare Eigenschaften: In der gegebenen Situation gilt

(1) $S_{M/R}(\alpha + \beta) = S_{M/R}(\alpha) + S_{M/R}(\beta)$

(2) $S_{M/R}(r \cdot \alpha) = r \cdot S_{M/R}(\alpha), \quad r \in R.$

(3) $A \times A \to R$, $(\alpha, \beta) \mapsto S_{M/R}(\alpha \cdot \beta)$ ist eine symmetrische Bilinearform.

(4) $N_{M/R}(\alpha \cdot \beta) = N_{M/R}(\alpha) \cdot N_{M/R}(\beta)$

(5) $S_{M/R}(\alpha)$ und $N_{M/R}(\alpha)$ sind aus R.

Beweis: Für die Matrizen zur gewählten Basis gilt $C(\alpha+\beta) = C(\alpha)+C(\beta)$ und $C(r \cdot \alpha) = r \cdot C(\alpha)$. Damit folgen (1) und (2) aus 8.3. Dasselbe gilt für die Bilinearität von (3) und für (5). Weiter gilt $C(\alpha \cdot \beta) = C(\alpha) \cdot C(\beta)$. Damit folgt (4), und es gilt

$$\begin{aligned} S_{M/R}(\alpha \cdot \beta) &= \sum_{i=1}^{n} c_{ii}^{\alpha\cdot\beta} = \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^{\alpha} \cdot c_{ji}^{\beta} \\ &= \sum_{j=1}^{n}\sum_{i=1}^{n} c_{ji}^{\beta} \cdot c_{ij}^{\alpha} = \sum_{j=1}^{n} c_{jj}^{\beta\alpha} \\ &= S_{M/K}(\beta \cdot \alpha) \end{aligned}$$

Also ist die Form (3) auch symmetrisch. □

8.5 Satz: Ist in unserer Situation $N \subset M$ ein A-Teilmodul und sind N und $\overline{M} = M/N$ endlich erzeugte freie R-Module, dann gilt für $\alpha \in A$

(1) $S_{M/R}(\alpha) = S_{N/R}(\alpha) + S_{\overline{M}/R}(\alpha)$

(2) $N_{M/R}(\alpha) = N_{N/R}(\alpha) \cdot N_{\overline{M}/R}(\alpha)$

(3) $P_{M/R}(\alpha; X) = P_{N/R}(\alpha; X) \cdot P_{\overline{M}/R}(\alpha; X)$

Beweis: Ist $x_1, \ldots, x_m$ Basis von N und sind $y_1, \ldots, y_n \in M$ Elemente, so dass $\overline{y}_1, \ldots, \overline{y}_n$ eine Basis von $\overline{M}$ bilden, dann ist $x_1, \ldots, x_m, y_1, \ldots, y_n$ Basis von M.

(i) Ist $z \in M$, dann gibt es eine R-Linearkombination für $\overline{z} \in \overline{M}$

$$\overline{z} = r_1\overline{y}_1 + \ldots + r_n\overline{y}_n.$$

Da z und $r_1y_1 + \ldots + r_ny_n$ in derselben Restklasse liegen, ist $z - (r_1y_1 + \ldots + r_ny_n) \in N$, d.h. es gibt $s_1, \ldots, s_m \in R$, so dass

$$z - (r_1y_1 + \ldots + r_ny_n) = s_1x_1 + \ldots + s_mx_m.$$

Also erzeugen $x_1, \ldots, x_m, y_1, \ldots, y_n$ ganz M.

(ii) Sei $\underbrace{s_1x_1 + \ldots + s_mx_m}_{=:x} + \underbrace{r_1y_1 + \ldots + r_ny_n}_{=:y} = 0, \quad s_ir_i \in R$

Da $x \in N$ ist, folgt $r_1\overline{y}_1 + \ldots + r_n\overline{y}_n = 0$ in $\overline{M}$, also $r_1, \ldots, r_n = 0$. Damit folgt auch $s_1, \ldots, s_m = 0$.
Die R-lineare Abbildung

$$\alpha_M : M \to M, \quad x \mapsto \alpha \cdot x$$

bildet N nach N ab, da N ein A-Untermodul ist, und definiert daher R-lineare Abbildungen

$$\alpha_N : N \to N, \quad \alpha_{\overline{M}} : \overline{M} \to \overline{M}.$$

Bzgl. unserer Basis hat $C(\alpha)$ die Form

$$C(\alpha) = \begin{pmatrix} C(\alpha|N) & * \\ 0 & C_2(\alpha) \end{pmatrix},$$

wobei $C_2(\alpha)$ die Matrix für $\alpha_{\overline{M}}$ ist bzgl. $\{\overline{y}_1, \ldots, \overline{y}_n\}$. Die Aussagen folgen nun. $\square$

8.6 Satz: Sei B eine R-Unteralgebra von A, die als R-Modul frei und endlich erzeugt ist. A sei als B-Modul frei und endlich erzeugt. Dann ist A als R-Modul frei und endlich erzeugt, und es gilt für $\beta \in B$

$$P_{A/R}(\beta; X) = P_{B/R}(\beta; X)^m \qquad m = \mathrm{Rang}_B(A.$$

$$S_{A/R}(\beta) = m \cdot S_{B/R}(\beta) \quad \text{und} \quad N_{A/R}(\beta) = N_{B/R}(\beta)^m.$$

Beweis: Wir haben einen Isomorphismus von B-Moduln

$$A \cong B^m.$$

Da $B \cong R^n$, falls $\mathrm{Rang}_R B = n$ ist, folgt $A \cong R^{m \cdot n}$ als R-Modul. Aus 8.5 folgt für $M \cong M_1 \oplus M_2$ als R-Modul

$$P_{M/R}(\alpha; X) = P_{M_1/R}(\alpha, X) \cdot P_{M_2/R}(\alpha; X)$$

und induktiv das entsprechende Resultat für m Summanden. □

8.7 Satz: Sei A eine R-Algebra, die als R-Modul frei und endlich erzeugt ist. Dann gilt

$$\alpha \in A^* \iff N_{A/R}(\alpha) \in R^*.$$

Beweis: Existiert α^{-1}, so gilt nach 8.4.4

$$N(\alpha) \cdot N(\alpha^{-1}) = N(\alpha \cdot \alpha^{-1}) = N(1) = 1.$$

Ist umgekehrt $N(\alpha) = \det(\alpha_{A/R})$ invertierbar, dann ist $\alpha_{A/R}$ nach dem Laplace'schen Entwicklungssatz invertierbar. Insbesondere gibt es ein $x \in A$, so dass $1 = \alpha_{A/R}(x) = \alpha \cdot x$. Es folgt $1 = N(\alpha) \cdot N(x)$. Also ist $N(x)$ invertierbar. Damit gibt es wie eben ein $y \in A$, so dass $x \cdot y = 1$. Es folgt $y = (\alpha \cdot x) \cdot y = \alpha$. Also ist $x = \alpha^{-1}$. □

Für uns ist die erheblich schönere Situation einer **endlichen Körpererweiterung** $K \subset F$ von besonderem Interesse.

8.8 Satz: Sei F/K endliche Körpererweiterung und $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ aus $K[X]$ das Minimalpolynom von $\alpha \in F$. Dann gilt mit $m = [F : K(\alpha)]$

(1) $P_{K(\alpha)/K}(\alpha; X) = f(X)$

(2) $S_{K(\alpha)/K}(\alpha) = -a_{n-1}$

(3) $N_{K(\alpha)/K}(\alpha) = (-1)^n a_0$

(4) $P_{F/K}(\alpha; X) = f(X)^m$

(5) $S_{F/K}(\alpha) = -ma_{n-1}$

(6) $N_{F/K}(\alpha) = (-1)^{m \cdot n} \cdot a_0^m$

Beweis: $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ ist nach 4.3 eine K-Basis für $K(\alpha)$. Bzgl. dieser Basis hat $\alpha_{K(\alpha)/K} : K(\alpha) \to K(\alpha)$ die Matrix

$$C(\alpha) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}, \quad P_{K(\alpha)/K}(\alpha) = \det(X \cdot E_n - C(\alpha)) = f$$

Damit ist (1) gezeigt, und (2), (3) folgen.
Wir wenden nun 8.6 auf $K \subset K(\alpha) \subset F$ an. □

Norm und Spur lassen sich auch über die Operation der Galois-Gruppe einer Körpererweiterung bestimmen. Dazu eine Vorbereitung:

8.9 Satz: Sei F/K endliche separable Körpererweiterung. Sei $\overline{K}$ ein algebraischer Abschluss von K und G die Menge aller K-Homomorphismen $F \to \overline{K}$. Dann gilt für $\alpha \in F$

$$S_{F/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \qquad N_{F/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Beweis: Wir dürfen $F \subset \overline{K}$ voraussetzen. Sei $n = [K(\alpha) : K]$ und seien $\alpha = \alpha_1, \ldots, \alpha_n$ die n **verschiedenen** Nullstellen des Minimalpolynoms $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ von α. Dann gibt es noch 4.9 genau n verschiedene K-Homomorphismen

$$\rho_i : K(\alpha) \to \overline{K}, \quad \alpha \mapsto \alpha_i.$$

Da $f = \prod_{i=1}^n (X - \alpha_i)$ in $\overline{K}$, gilt

$$\begin{aligned} S_{K(\alpha)/K}(\alpha) &= -a_{n-1} = \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \rho_i(\alpha) \\ N_{K(\alpha)/K}(\alpha) &= (-1)^n a_0 = \prod_{i=1}^n \alpha_i = \prod_{i=1}^n \rho_i(\alpha) \end{aligned}$$

Nach dem folgenden Lemma gibt es $m = [F : K(\alpha)]$ verschiedene Erweiterungen von ρ_i zu einem Homomorphismus $F \to \overline{K}$. Es folgt nach 8.8

$$\begin{aligned}\sum_{\sigma\in G}\sigma(\alpha) &= m\cdot\sum_{i=1}^{n}\rho_i(\alpha) = mS_{K(\alpha)/K}(\alpha) = S_{F/K}(\alpha)\\ \prod_{\sigma\in G}\sigma(\alpha) &= \left(\prod_{i=1}^{n}\rho_i(\alpha)\right)^m = (N_{K(\alpha)/K}(\alpha))^m = N_{F/K}(\alpha).\end{aligned}$$

□

8.10 Lemma: Sei F/K eine endliche separable Körpererweiterung, $\overline{K}$ ein algebraischer Abschluss von K und $\varphi : K \to \overline{K}$ ein Homomorphismus. Dann gibt es genau $[F : K]$ verschiedene Erweiterungen $\sigma : F \to \overline{K}$ von φ.

Beweis: Nach 4.18 ist F/K einfach, d.h. es gibt ein $a \in F$, so dass $F = K(a)$. Ist $f \in K[X]$ das Minimalpolynom von a, gilt $[F : K] = \operatorname{grad} f$. Da f separabel ist, hat es nur einfache Nullstellen in $\overline{K}$. Damit gibt es nach 4.9 genau $\operatorname{grad}(f)$ viele verschiedene Erweiterungen $\sigma : F \to \overline{K}$ von φ. □

8.11 Schachtelungsformel: Sei F/K endliche, separable Erweiterung und $K \subset L \subset F$ ein Zwischenkörper. Dann gilt für $\alpha \in F$

$$S_{F/K}(\alpha) = S_{L/K}(S_{F/L}(\alpha)), \quad N_{F/K}(\alpha) = N_{L/K}(N_{F/L}(\alpha)).$$

Beweis: Sei $\overline{K}$ ein algebraischer Abschluss von K. Wir dürfen annehmen, dass $F \subset \overline{K}$. Wie im Beweis von 8.9 gezeigt, gibt es $n = [L : K]$ verschiedene K-Homomorphismen $\rho_i : L \to \overline{K}$, und jedes ρ_i hat $m = [F : L]$ Erweiterungen

$$\sigma_{i,j} : F \to \overline{K}, \quad j = 1, \ldots, m.$$

Dann haben wir vermöge $\sigma_{i,1}$ Teilkörper

$$\rho_i(L) = \sigma_{i,1}(L) \subset \sigma_{i,1}(F) \subset \overline{K}.$$

Die weiteren $\rho_i(L)$-Homomorphismen $\sigma_{i,1}(F) \to \overline{K}$ sind dann

$$\sigma_{i,j} \circ \sigma_{i,1}^{-1} : \sigma_{i,1}(F) \to \overline{K}.$$

Wir erhalten

$$\begin{aligned}S_{F/K}(\alpha) &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sigma_{i,j}(\alpha) = \sum_{i=1}^{n}\sum_{j=1}^{m}\sigma_{i,j}\circ\sigma_{i,1}^{-1}(\sigma_{i,1}(\alpha))\\ &= \sum_{i=1}^{n} S_{\sigma_{i1}F/\rho_i L}(\sigma_{i,1}(\alpha)) \overset{(*)}{=} \sum_{i=1}^{n}\sigma_{i,1}(S_{F/L}(\alpha))\\ &\overset{(**)}{=} \sum_{i=1}^{n}\rho_i(S_{F/L}(\alpha)) = S_{L/K}(S_{F/L}(\alpha))\end{aligned}$$

$(*)$ gilt, weil $\sigma_{i,1} : (F, L) \to (\sigma_{i,1}F, \rho_i L)$ ein Isomorphismus von Paaren ist.
$(**)$ gilt, weil $S_{F/L}(\alpha) \in L$ und $\sigma_{i1}|L = \rho_i$ ist.
Für die Norm ist der Beweis analog. □

8.12 Satz: Sei R ein ganz abgeschlossener Integritätsring und K sein Quotientenkörper. Sei F/K endliche Körpererweiterung und $\alpha \in F$ ganz über R. Dann folgt

$$S_{F/K}(\alpha) \in R \quad \text{und} \quad N_{F/K}(\alpha) \in R.$$

Beweis: Nach 7.17 liegt das Minimalpolynom von α über K in $R[X]$. Damit folgt der Satz aus 8.8. □

8.13 Satz: Sei F/K endliche separable Erweiterung vom Grad $[F : K] = n$. Dann gilt

(1) Die Spurabbildung

$$S_{F/K} : F \to K$$

ist surjektiv.

(2) Die Bilinearform

$$F \times F \to K, \quad (\alpha, \beta) \mapsto S_{F/K}(\alpha \cdot \beta)$$

auf dem K-Vektorraum F ist nicht entartet.

Beweis: (1) Gibt es ein $\alpha \in F$ mit $S_{F/K}(\alpha) = r \neq 0$, dann folgt für ein beliebiges $q \in K$, dass $S_{F/K}((q \cdot r^{-1}) \cdot \alpha) = q \cdot r^{-1} \cdot r = q$ nach 8.4.2.
Da $S_{F/K}(1) = n$, ist 1 ein solches α, falls $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) \nmid n$. Ist das nicht der Fall, beziehen wir uns auf Aufgabe 8.16: Gilt

$$S_{F/K}(\alpha) = \sum_{\sigma} \sigma(\alpha) = 0$$

für alle K-Morphismen $\sigma : F \to \overline{K}$ und alle α, dann wären die σ linear abhängig im Widerspruch zu 8.16.
(2) Wir müssen zeigen, dass für festes $\alpha \neq 0$ die Abbildung

$$F \to K, \quad \beta \mapsto S_{F/K}(\alpha \cdot \beta)$$

nicht die Nullabbildung ist. Wäre das der Fall, dann wäre $S_{F/K}$ die Nullabbildung, weil F ein Körper ist. Das widerspricht aber Teil (1). □

8.14 Sei $\mathbb{Q} \subset K$ eine endliche Erweiterung und $\mathcal{O}_K \subset K$ der Teilring der über $\mathbb{Z}$ ganzen Zahlen. Nach 8.12 sind Norm und Spur Abbildungen von Paaren

$$S_{K/\mathbb{Q}}, N_{K/\mathbb{Q}} : (K, \mathcal{O}_K) \to (\mathbb{Q}, \mathbb{Z}).$$

8.15 Beispiel: Sei d quadratfrei. Wir wollen Norm und Spur für die quadratische Erweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt{d})$ bestimmen. Nach 4.9 gibt es genau zwei $\mathbb{Q}$-Morphismen $\mathbb{Q}(\sqrt{d}) \to \overline{\mathbb{Q}}$, nämlich die Identität und

$$\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \subset \overline{\mathbb{Q}}, \quad \sqrt{d} \mapsto -\sqrt{d}.$$

Es folgt für $\alpha = a + b\sqrt{d}$

$$\begin{aligned} S_{K/\mathbb{Q}}(a + b\sqrt{d}) &= \mathrm{id}(\alpha) + \sigma(\alpha) = a + b\sqrt{d} + a - b\sqrt{d} = 2a \\ N_{K/\mathbb{Q}}(a + b\sqrt{d}) &= \mathrm{id}(\alpha) \cdot \sigma(\alpha) = (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - db^2. \end{aligned}$$

8.16 Aufgabe: Sei M ein Monoid und K ein Körper. Sei $\mathcal{F}$ eine Menge von verschiedenen Homomorphismen $f : M \to K^*$. Dann ist $\mathcal{F}$ linear unabhängig im K-Vektorraum $\mathrm{Abb}(M, K)$.

(Hinweise: $\mathcal{F}$ heißt linear unabhängig, wenn jede endliche Teilmenge von $\mathcal{F}$ linear unabhängig ist. Angenommen $\{f_1, \ldots, f_n\}$ mit verschiedenen $f_i \in \mathcal{F}$ ist linear abhängig, wähle unter allen nicht-trivialen Linearkombinationen $c_1 \cdot f_1 + \ldots c_n \cdot f_n = 0$ eine mit minimaler Anzahl von $c_i \neq 0$. Konstruiere daraus unter Ausnutzung, dass die f_i verschieden sind, eine nicht-triviale Linearkombination mit wenigeren $c_i \neq 0$.)

9 Die Diskriminante

9.1 Definition: Sei R ein kommutativer Ring und A eine R-Algebra, die als R-Modul frei vom Rang n ist. Dann definieren wir für Elemente $\alpha_1, \ldots, \alpha_n$ aus A die *Diskriminante*

$$D_{A/R}(\alpha_1, \ldots, \alpha_n) = \det(S_{A/R}(\alpha_i \cdot \alpha_j)) \in R.$$

9.2 Ist $(\beta_1, \ldots, \beta_n)$ ein n-Tupel aus A, so dass $\beta_i = \sum_{j=1}^{n} r_{ij} \cdot \alpha_j$ mit $r_{ij} \in R$, dann gilt

$$D_{A/R}(\beta_1, \ldots, \beta_n) = \det(r_{ij})^2 \cdot D_{A/R}(\alpha_1, \ldots, \alpha_n)$$

Denn $$\begin{aligned} S_{A/R}(\beta_i \cdot \beta_j) &= S_{A/R}((\sum_{k=1}^{n} r_{ik}\alpha_k) \cdot (\sum_{l=1}^{n} r_{jl}\alpha_l)) \\ &= \sum_{k,l} r_{ik} \cdot S_{A/R}(\alpha_k, \alpha_l) \cdot r^t_{lj}, \end{aligned}$$

wobei (r_{lj}^t) die Transponierte von (r_{lj}) ist. In Matrizenschreibweise erhalten wir

$$(S_{A/R}(\beta_i \cdot \beta_j)) = (r_{ij}) \cdot (S_{A/R}(\alpha_i, \alpha_j)) \cdot (r_{ij})^t.$$

9.3 Für eine $\mathbb{Z}$-Algebra A definieren wir die *Diskriminante* durch

$$\mathrm{disc}(A/\mathbb{Z}) = D_{A/\mathbb{Z}}(\alpha_1, \ldots, \alpha_n),$$

wobei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Z}$-Basis von A ist. Nach 9.2 ist $\mathrm{disc}(A/\mathbb{Z})$ unabhängig von der Wahl der Basis. Denn sind $(\beta_1, \ldots, \beta_n)$ und $(\alpha_1, \ldots, \alpha_n)$ zwei Basen, ist die Transformationsmatrix (r_{ij}) invertierbar und damit $\det(r_{ij}) \in \mathbb{Z}^*$, so dass $\det(r_{ij})^2 = 1$ ist. Für allgemeinere Ringe ist $\mathrm{disc}(A/R)$ nur bis auf Multiplikation mit Quadraten von Einheiten aus R eindeutig bestimmt. Daher definiert man in diesen Fällen $\mathrm{disc}(A/R)$ als das Ideal in R, das von allen $D_{A/R}(\alpha_1, \ldots, \alpha_n)$, $\{\alpha_1, \ldots, \alpha_n\}$ eine R-Basis von A, erzeugt wird.

9.4 Satz: Sei R ein Integritätsring. Sei A eine R-Algebra, die als R-Modul frei vom Rang n ist. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine R-Basis von A und $D_{A/R}(\alpha_1, \ldots, \alpha_n) \neq 0$. Dann ist $\{\beta_1, \ldots, \beta_n\}$ genau dann eine R-Basis von A, wenn

$$D_{A/R}(\beta_1, \ldots, \beta_n) = \mu^2 \cdot D_{A/R}(\alpha_1, \ldots, \alpha_n) \quad \text{mit} \quad \mu \in R^*.$$

Beweis: Sei $\beta_i = \sum r_{ij} \cdot \alpha_j$ mit $r_{ij} \in R$. Dann gilt

$$D_{A/R}(\beta_1, \ldots, \beta_n) = \det(r_{ij})^2 \cdot D_{A/R}(\alpha_1, \ldots, \alpha_n)$$

$\{\beta_1, \ldots, \beta_n\}$ ist genau dann R-Basis von A, wenn $\det(r_{ij})$ invertierbar ist. Da R Integritätsring ist, entspricht $\det(r_{ij})^2$ dem μ^2. □

Wieder interessiert uns besonders der Fall von endlichen Körpererweiterungen F/K.

9.5 Satz: Ist F/K endliche separable Körpererweiterung von Grad n und sind $\sigma_i : F \to \overline{K}$ die n verschiedenen K-Morphismen, dann gilt für $\alpha_1, \ldots, \alpha_n \in F$

$$D_{F/K}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Beweis:

$$\begin{aligned} D_{F/K}(\alpha_1, \ldots, \alpha_n) &= \det(S_{F/K}(\alpha_i \cdot \alpha_j)) = \det(\textstyle\sum_k \sigma_k(\alpha_i \cdot \alpha_j)) \\ &= \det(\textstyle\sum_k \sigma_k(\alpha_i) \cdot \sigma_k(\alpha_j)) = \det((\sigma_k(\alpha_i))_{i,k} \cdot (\sigma_k(\alpha_j))_{k,j}) \\ &= \det(\sigma_k(\alpha_j))^2. \end{aligned}$$

□

Der Beriff “Diskriminante” tritt auch im Zusammenhang mit Polynomen auf:

9.6 Definition: Sei $f \in K[X]$ ein Polynom vom Grad n und Leitkoeffizient c. Sei $f = c \cdot \prod_{i=1}^{n}(X - \alpha_i)$ seine Faktorisierung in Linearfaktoren in $\overline{K}[X]$, dann nennt man

$$D(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

die *Diskriminante* von f.

Wir wollen uns jetzt mit der Verbindung von $D(f)$ und $D_{F/K}$ beschäftigen.

9.7 Satz: Sei $F = K(\alpha)$, $\alpha \in F$ separabel über K, sei $f \in K[X]$ das Minimalpolynom von α und $\operatorname{grad}(f) = n$. Dann gilt

$$D_{F/K}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = D(f).$$

Beweis: Da α separabel ist, hat f verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n$ in $\overline{K}$, und wir haben n verschiedene K-Morphismen.

$$\sigma_i : F \to \overline{K}, \quad \alpha \mapsto \alpha_i.$$

Es folgt: $\sigma_i(\alpha^j) = \alpha_i^j$ und mit 9.5

$$D_{F/K}(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_i(\alpha^{j-1}))^2 = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}^2$$

Die rechte Seite ist das Quadrat der Vandermonde-Determinante. Aus Übungsaufgaben kennt man diesen Wert: $(\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j))^2$. □

9.8 Satz: Unter den Voraussetzungen von 9.7 gilt

$$D_{F/K}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n \cdot (n-1)/2} \cdot N_{F/K}(f'(\alpha)).$$

Beweis: $f = \prod_{j=1}^{n}(X - \alpha_i)$, $f' = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \ne j}}^{n}(X - \alpha_i)$. Also $f'(\alpha_j) = \prod_{\substack{i=1 \\ i \ne j}}^{n}(\alpha_j - \alpha_i)$

$$N_{F/K}(f'(\alpha)) = \prod_{j=1}^{n} \sigma_j(f'(\alpha)) = \prod_{j=1}^{n} f'(\sigma_j(\alpha)) = \prod_{j=1}^{n} f'(\alpha_j) = \prod_{1 \le i \ne j \le n} (\alpha_j - \alpha_i)$$

In diesem Ausdruck kommt der Faktor $(\alpha_i - \alpha_j)$ für $i < j$ genau zweimal auf, nämlich als $(\alpha_i - \alpha_j)$ und $(\alpha_j - \alpha_i) = -(\alpha_i - \alpha_j)$. Wir erhalten für jedes Paar $i < j$ also $-((\alpha_i - \alpha_j)^2$. Es gibt aber davon $\frac{n^2-n}{2} = \frac{n(n-1)}{2}$. Also

$$\begin{aligned} N_{F/K}(f'(\alpha)) &= (-1)^{n(n-1)/2} \cdot \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \cdot D_{F/K}(1, \alpha, \ldots, \alpha^{n-1}) \end{aligned}$$

□

9.9 Folgerung: Ist $K \subset F$ endliche separable Erweiterung und $\{\beta_1, \ldots, \beta_n\}$ eine K-Basis von F, dann ist

$$D_{F/K}(\beta_1, \ldots, \beta_n) \neq 0.$$

Beweis: Nach 4.18 ist $K \subset F$ einfach, d.h. es gibt ein $\alpha \in F$, so dass $F = K(\alpha)$. Nach 4.3 ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ eine K-Basis von F. Das Minimalpolynom f von α ist separabel und hat daher nur verschiedene Nullstellen. Es folgt direkt aus der Definition, dass $D(f) \neq 0$. Aus 9.7 folgt $D_{F/K}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \neq 0$ und nach 9.4 auch $D_{F/K}(\beta_1, \ldots, \beta_n) \neq 0$. □

Wir wollen nun eine Methode zur Berechnung von $D_{F/K}(1, \alpha, \ldots, \alpha^{n-1})$ angeben, für die man α nicht explizit zu kennen braucht.

9.10 Satz: Sei $F = K(\alpha)$, α separabel über K mit Minimalpolynom $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. Dann gilt

$$D_{F/K}(1, \alpha, \ldots, \alpha^{n-1}) = \det \begin{pmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{pmatrix}$$

wobei $p_k = \alpha_1^k + \alpha_2^k + \ldots + \alpha_n^k$ und $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f sind.

Beweis: Sei V die Vandermonde-Matrix aus den Beweis von 9.7. Dann gilt $D_{F/K}(1, \ldots, \alpha^{n-1}) = \det(V^t \cdot V)$, aber

$$V^t \cdot V = \begin{pmatrix} n & \sum \alpha_i & \sum \alpha_i^2 & \cdots & \sum \alpha_i^{n-1} \\ \sum \alpha_i & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ \sum \alpha_i^{n-1} & & & & \sum \alpha_i^{2n-2} \end{pmatrix}.$$

□

9.11 Die p_k lassen sich rekursiv wie folgt berechnen

$$\begin{aligned} p_0 = n \qquad\qquad (n-k)a_{n-k} &= \sum_{j=0}^{k} a_{n-j}p_{k-j} \qquad 0 \le k \le n \\ p_1 = -a_{n-1} \qquad\qquad 0 &= \sum_{j=0}^{k} a_{n-j}p_{k-j} \qquad k > n. \end{aligned}$$

Beweis: $f' = \sum_{i=0}^{n} i \cdot a_i \cdot X^{i-1} = \sum_{k=1}^{n} \prod_{i \neq k} (X - \alpha_i)$. Es folgt wegen $f = \prod_{i=1}^{n}(X - \alpha_i)$

$$\frac{f'}{f} = \sum_{k=1}^{n} \frac{1}{X - \alpha_k} = \sum_{k=1}^{n} \frac{1}{X} \cdot \frac{1}{1 - \frac{\alpha_k}{X}} = \sum_{k=1}^{n} \sum_{j=0}^{\infty} \frac{\alpha_k^i}{X^{j+1}}$$

Also

$$\sum_{i=0}^{n} i a_i X^{i-1} = \left(\sum_{i=0}^{n} a_i X^i \right) \cdot \left(\sum_{j=0}^{\infty} \frac{\alpha_1^j + \alpha_2^j + \ldots + \alpha_n^j}{X^{j+1}} \right) = \left(\sum_{i=0}^{n} a_i X^i \right) \cdot \left(\sum_{j=0}^{\infty} \frac{p_j}{X^{j+1}} \right).$$

Umkehren der Summationsreihenfolge gibt

$$\sum_{i=0}^{n} (n-i) a_{n-i} X^{n-i-1} = \sum_{i=0}^{n} \left(\sum_{j+k=i} a_{n-k} \cdot p_j \right) \cdot X^{n-i-1}$$

Koeffizientenvergleich ergibt

$$\begin{aligned} (n-i)a_{n-i} &= \sum_{k=0}^{i} a_{n-k} \cdot p_{i-k} \qquad 0 \le i \le n \\ 0 &= \sum_{k=0}^{i} a_{n-k} \cdot p_{i-k} \qquad i > n. \end{aligned}$$

□

9.12 Aufgabe: Berechnen Sie nach dieser Methode für $a \neq 0$

$$D(aX^2 + bX + c) \quad \text{und} \quad D(X^3 + bX + c).$$

9.13 Beispiel: Sei $f = X^n + bX + c$ aus $K[X]$ irreduzibel und separabel. Dann gilt

$$D(f) = (-1)^{\frac{n(n-1)}{2}} (n^n c^{n-1} + (-1)^{n-1}(n-1)^{n-1} b^n).$$

Beweis: Sei β Nullstelle von f und $\gamma = f'(\beta) = n\beta^{n-1} + b$ in $\overline{K}$. Gesucht wird $D(f) = D_{F/K}(1, \beta, \ldots, \beta^{n-1}) = (-1)^{n(n-1)/2} N_{F/K}(\gamma)$
Aus der Gleichung $\beta^n + b\beta + c = 0$ erhalten wir

$$n \cdot \beta^{n-1} + nb + nc\beta^{-1} = 0, \text{ also}$$

$$\gamma = -nc\beta^{-1} - nb + b = -(n-1)b - nc\beta^{-1}, \text{ also } \beta = \frac{-nc}{\gamma + (n-1)b}.$$

Es folgt $K(\beta) = K(\gamma)$. Damit hat das Minimalpolynom von γ ebenfalls den Grad n. Wir schreiben

$$f\left(\frac{-nc}{X + (n-1)b}\right) = \frac{(-nc)^n}{(X + (n-1)b)^n} + \frac{-ncb}{X + (n-1)b} + c = \frac{P(X)}{Q(X)}$$

mit $\begin{aligned} P(X) &= (X + (n-1)b)^n - nb(X + (n-1)b)^{n-1} + (-1)^n \cdot n^n \cdot c^{n-1} \text{ und} \\ Q(X) &= \frac{1}{c}(X + (n-1)b)^n \end{aligned}$

Dann gilt $P(\gamma)/Q(\gamma) = f(\beta) = 0$. Also $P(\gamma) = 0$. Damit ist P das Minimalpolynom von γ. Es folgt

$$\begin{aligned} N_{F/K}(\gamma) &= (-1)^n \cdot ((n-1)^n b^n - nb(n-1)^{n-1} b^{n-1} + (-1)^n n^n c^{n-1}) \\ &= n^n \cdot c^{n-1} + (-1)^{n-1}(n-1)^{n-1} \cdot b^n. \end{aligned}$$

□

10 Ganze Basen

10.1 Konvention: Für das Weitere sei R ein ganz abgeschlossener Integritätsring, K sein Quotientenkörper und $K \subset F$ eine endliche separable Erweiterung. Weiter sei B der ganze Abschluss von R in F.

Man erhält sofort

10.2 $R = B \cap K, \quad S_{F/K}(x) \in R, \quad N_{F/K}(x) \in R \quad \forall x \in B$

$R = B \cap K$, denn R ist ganz abgeschlossen. Nach 7.17 ist das Minimalpolynom von x aus $R[X]$. Damit folgt der Rest.

10.3 Lemma: Sei $\{\alpha_1, \ldots, \alpha_n\} \subset B$ eine K-Basis von F mit Diskriminate d. Dann gilt (beachte $d \neq 0$ nach 9.9)

$$R \cdot \alpha_1 + \ldots + R \cdot \alpha_n \subset B \subset R \cdot \left(\frac{\alpha_1}{d}\right) + \ldots + R \cdot \left(\frac{\alpha_n}{d}\right).$$

Beweis: Sei $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \in B$ mit $a_i \in K$ und seien $\sigma_j : F \to \overline{K}$, $j = 1, \ldots, n$ die n K-Homomorphismen von F nach $\overline{K}$. Dann gilt

$$\sigma_j(\alpha) = \sum_{i=1}^{n} a_i \cdot \sigma_j(\alpha_i). \qquad (*)$$

D.h. $(a_1, \ldots, a_n)$ ist eine Lösung des Gleichungssytem $(*)$. Da nach 9.5 $\det(\sigma_j(\alpha_i))^2 = D_{F/K}(\alpha_1, \ldots, \alpha_n) = d \neq 0$, können wir die Cramer'sche Regel anwenden. Ist $\delta = \det(\sigma_j(\alpha_i))$, so gibt es Elemente $\beta_i \in \overline{K}$, so dass

$$a_i = \frac{\beta_i}{\delta}.$$

Es folgt $\beta_i \cdot \delta = a_i \cdot d \in K$, also $d \cdot \alpha = \sum\limits_{i=1}^{n} da_i\alpha_i = \sum\limits_{i=1}^{n}(\beta_i \cdot \delta)\alpha_i$, da $\delta^2 = d$.
Da die α_i ganz über R sind, sind die $\sigma_j(\alpha_i)$ ganz über R. Die β_k sind die Determinante der Matrix $(\sigma_i(\alpha_j))$ mit der Spalte der $\sigma_i(\alpha_k)$ ersetzt durch die $\sigma_i(\alpha)$. Damit sind die $\beta_k \in \overline{K}$ ganz über R und damit auch $\beta_k \cdot \delta$. Da $\beta_k \cdot \delta \in K$, folgt $\beta_k \cdot \delta \in R$ für alle k. Wir erhalten die zweite Inklusion. Die erste Inklusion ist klar. □

10.4 Definition: $\{\beta_1, \ldots, \beta_n\} \subset B$ heißt *ganze Basis* von B über R oder *R-Basis* von B, wenn $\{\beta_1, \ldots, \beta_n\}$ eine Basis des R-Moduls B ist (insbesondere ist B frei und endlich erzeugt).

Ganze Basen brauchen nicht zu existieren. In den uns interessierenden Fällen ist B aber frei.

10.5 Satz: Unter der Konvention 10.1 gilt

(1) B ist Untermodul eines freien R-Moduls vom Rang $m = [F : K]$.

(2) Ist R Hauptidealring, dann ist B frei vom Rang $m = [F : K]$.

Beweis: Sie $\{\beta_1, \ldots, \beta_m\}$ eine K-Basis von F. Nach 7.14 gibt es ein $r \in R$, $r \neq 0$, so dass $\{r\beta_1, \ldots, r\beta_m\} \subset B$. Da $\{r\beta_1, \ldots, r\beta_m\}$ eine K-Basis von F ist, dürfen wir o.B.d.A. annehmen, dass $\{\beta_1, \ldots, \beta_m\} \subset B$. Aus Lemma 10.3 folgt dann

$$R \cdot \beta_1 + \ldots + R \cdot \beta_m \subset B \subset R \cdot \left(\frac{\beta_1}{d}\right) + \ldots + R \cdot \left(\frac{\beta_m}{d}\right) \qquad (*)$$

Linke und rechte Seite sind freie R-Moduln vom Rang $m = [F : K]$. Ist nun R ein Hauptidealring und B Untermodul eines freien R-Moduls M von Rang n, dann ist B selbst ein freier R-Modul vom Rang $\leq n$ nach 5.9. Also folgt in diesem Fall aus $(*)$, dass B ein freier R-Modul vom Rang m ist. □

10.6 Folgerung: Ist R Hauptidealring, dann ist jede R-Basis von B eine K-Basis von F.

10.7 Definition: Ein *algebraischer Zahlkörper* K ist eine endliche Erweiterung $\mathbb{Q} \subset K$.

Als faktorieller Ring ist $\mathbb{Z}$ ganz abgeschlossen nach 7.15. Ist K ein Zahlkörper, dann ist $\mathbb{Q} \subset K$ endlich und separabel. Wir sind in der Situation unserer Konvention 10.1.

10.8 Bezeichnung: Ist K ein Zahlkörper, dann bezeichne $\mathcal{O}_K$ den ganzen Abschluss von $\mathbb{Z}$ in K. Wir nennen den Ring $\mathcal{O}_K$ den *Ring der ganzen Zahlen* in K. Wir nennen $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$ die *Diskriminante von* K und bezeichnen sie oft mit δ_K.

Nach 10.5 hat $\mathcal{O}_K$ stets eine ganze Basis. Unser Problem ist es, $\mathcal{O}_K$ zu bestimmen. Selbst für quadratische Erweiterungen ist das nicht völlig trivial (vergl. Aufgabe 7.3). Das Problem ist mit dem Auffinden einer ganzen Basis gelöst. Hier hilft

10.9 Satz: Sei K ein algebraischer Zahlkörper, $[K : \mathbb{Q}] = n$. Seien $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ und $\{\beta_1, \ldots, \beta_n\} \subset \mathcal{O}_K$ $\mathbb{Q}$-Basen von K und $\{\alpha_1, \ldots, \alpha_n\}$ sei **ganz** (d.h. Basis von $\mathcal{O}_K$). Sei $G \subset \mathcal{O}_K$ die von $\{\beta_1, \ldots, \beta_m\}$ erzeugte Untergruppe von $(\mathcal{O}_K, +)$. Dann gilt

(1) $D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = |\mathcal{O}_K/G|^2 .\ D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$

(2) $\{\beta_1, \ldots, \beta_n\}$ ist ganz $\iff D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$

(3) $D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$ und $D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) \equiv \left\{ \begin{array}{l} 0 \\ 1 \end{array} \right.$ oder $\mod 4$

10.10 Stickelbergers Theorem: $\delta_K \equiv \left\{ \begin{array}{l} 0 \\ 1 \end{array} \right.$ oder $\mod 4$

Beweis: Nach 10.6 ist jede $\mathbb{Z}$-Basis von $\mathcal{O}_K$ eine $\mathbb{Q}$-Basis von K. Damit folgt 10.10 aus 10.9.3. □

Beweis von 10.9: $\mathcal{O}_K$ ist ein freier $\mathbb{Z}$-Modul und $G \subset \mathcal{O}_K$ ist ein freier Teilmodul vom Rang n. Nach 5.10 gibt es eine Basis $\{\alpha'_1, \ldots, \alpha'_n\}$ von $\mathcal{O}_K$ und Zahlen $a_1, \ldots, a_n \in \mathbb{Z}$, so dass $\{\beta'_1, \ldots, \beta'_n\}$ mit $\beta'_i = a_i \cdot \alpha'_i$ Basis von G ist. Es folgt

$$\mathcal{O}_K/G \cong \mathbb{Z}/a_1 \times \ldots \times \mathbb{Z}/a_n.$$

Aus 9.2 folgt

$$D_{K/\mathbb{Q}}(\beta'_1,\ldots,\beta'_n) = (\prod_{i=1}^{n} a_i^2)\cdot D_{K/\mathbb{Q}}(\alpha'_1,\ldots,\alpha'_n) = |\mathcal{O}_K/G|^2\cdot D_{K/\mathbb{Q}}(\alpha'_1,\ldots,\alpha'_n).$$

Die Transformationsmatrizen T_1 zwischen den Basen $\{\beta_1,\ldots,\beta_n\}$ und $\{\beta'_1,\ldots,\beta'_n\}$ und T_2 zwischen den Basen $\{\alpha_1,\ldots,\alpha_n\}$ und $\{\alpha'_1,\ldots,\alpha'_n\}$ sind ganzzahlige invertierbare Matrizen, so dass $\det(T_i) \in \mathbb{Z}^*$, also $(\det T_i)^2 = 1$. Es folgt

$$D_{K/\mathbb{Q}}(\beta_1,\ldots,\beta_n) = D_{K/\mathbb{Q}}(\beta'_1,\ldots,\beta'_n)$$

und

$$D_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n) = D_{K/\mathbb{Q}}(\alpha'_1,\ldots,\alpha'_n)$$

Damit ist (1) gezeigt, Teil (2) folgt direkt aus (1).

(3) Sei $\overline{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$. Wir dürfen voraussetzen, dass $K \subset \overline{\mathbb{Q}}$. Seien $\sigma_i : K \to \overline{\mathbb{Q}}$, $i = 1,\ldots,n$ die verschiedenen $\mathbb{Q}$-Morphismen. Nach 4.18 gibt es ein $\gamma \in K$, so dass $K = \mathbb{Q}(\gamma)$. Sei Z der Zerfällungskörper des Minimalpolynoms f von γ. Nach 4.9 ist $\sigma_i(\gamma)$ eine Nullstelle von f, so dass $\sigma_i(K) \subset Z$. Daher fassen wir die σ_i als $\mathbb{Q}$-Morphismen $K \to Z$ auf. Wir schreiben

$$\det(\sigma_j(\beta_i)) = \sum_{\pi\in\Sigma_n} \operatorname{sign}(\pi)\cdot\sigma_{\pi 1}(\beta_1)\cdot\ldots\cdot\sigma_{\pi n}(\beta_n) = P - N,$$

wobei P die Summe über die geraden Permutationen π und N die über die ungeraden ist.

Sei $\sigma \in \mathrm{Gal}(Z/\mathbb{Q})$. Da $\sigma_j(K) \subset Z$, ist $\sigma\circ\sigma_j$ eines der σ_i. Da σ ein Körperhomomorphismus ist, folgt

$$\sigma(\det(\sigma_j(\beta_i))) = \det(\sigma\circ\sigma_j(\beta_i)).$$

Damit ist $\sigma(\det(\sigma_j(\beta_i)))$ die Determinante einer Spaltenpermutation der Ausgangsmatrix, d.h. es gibt ein $\tau \in \Sigma_n$, so dass mit $a_{ij} = \sigma_j(\beta_i)$ gilt

$$\begin{aligned}\sigma(\det(a_{ij})) &= \sum_{\pi\in\Sigma_n} \operatorname{sign}(\pi)\cdot a_{1,\pi\tau(1)}\cdot\ldots\cdot a_{n,\pi\tau(n)} \qquad \text{setze } \pi\circ\tau = \lambda \\ &= \sum_{\lambda\in\Sigma_n} \operatorname{sign}(\lambda\circ\tau^{-1})\cdot a_{1,\lambda(1)}\cdot\ldots\cdot a_{n,\lambda(n)}.\end{aligned}$$

Ist $\operatorname{sign}(\tau) = 1$, erhalten wir $\sigma(P) = P$ und $\sigma(N) = N$, ist $\operatorname{sign}(\tau) = -1$, erhalten wir $\sigma(P) = N$ und $\sigma(N) = P$. Also haben wir in beiden Fällen

$$\sigma(P+N) = P+N \quad \text{und} \quad \sigma(P\cdot N) = P\cdot N.$$

Damit liegen $P+N$ und $P\cdot N$ im Fixkörper der Galoisgruppe, also nach 4.23 in $\mathbb{Q}$. Da aber alle β_i ganz sind, sind alle $\sigma_j(\beta_i)$ ganz, also auch P und N. Es folgt $P+N\in\mathbb{Z}$ und $P\cdot N\in\mathbb{Z}$, und damit

$$D_{K/\mathbb{Q}}(\beta_1,\ldots,\beta_n)=(P-N)^2=(P+N)^2-4PN\in\mathbb{Z}.$$

Weiter gilt

$$(P+N)^2-4PN\equiv(P+N)^2\equiv 0 \text{ oder } 1 \mod 4,$$

weil 0 und 1 die einzigen Quadrate $\mod 4$ sind. □

10.11 Warnung: Wir haben gezeigt, dass $(\det(\sigma_j(\beta_i)))^2\in\mathbb{Z}$, aber nicht, dass $\det(\sigma_j(\beta_i))\in\mathbb{Z}$.

10.12 Beispiel: Sei $m\in\mathbb{Z}$ quadratfrei. Dann ist $\{1,\sqrt{m}\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\sqrt{m}]=K$ aus ganzen Elementen.

$$D_{K/\mathbb{Q}}(1,\sqrt{m})=D(X^2-m)=4m.$$

Es folgt $\delta_K=m$ oder $4m$. Denn ist G die von $\{1,\sqrt{m}\}$ erzeugte Untergruppe, gilt $D_{K/\mathbb{Q}}(1,\sqrt{m})=|\mathcal{O}_K/G|^2\cdot\delta_K$. Ist $\{1,\sqrt{m}\}$ nicht ganz, dann ist $\mathcal{O}_K\neq G$, so dass $D_{K/\mathbb{Q}}(1,\sqrt{m})$ einen quadratischen Faktor enthält. Da m quadratfrei ist, kann das höchstens die 4 sein.

Ist $m\equiv 2,3 \mod 4$, kann nach Stickelbergers Theorem nur $4m$ die Diskriminante sein. Nach 9.4 ist dann $\{1,\sqrt{m}\}$ eine **ganze** Basis.

Ist $m\equiv 1 \mod 4$, können wir so nicht schließen. Es könnte sein, daß $|\mathcal{O}_K/G|=2$ ist. Nach 5.10 gibt es eine Basis $\{\alpha_1,\alpha_2\}$ von $\mathcal{O}_K$, so dass $\{\alpha_1,2\cdot\alpha_2\}$ eine Basis von G ist. Wir probieren es mit $\alpha_2=\frac{1+\sqrt{m}}{2}$:

$$\frac{1+\sqrt{m}}{2}=-\frac{p}{2}+\frac{\sqrt{p^2-4q}}{2},\quad \text{falls } p=-1 \text{ und } m=1-4q.$$

Da $m\equiv 1 \mod 4$, gibt es ein solches $q\in\mathbb{Z}$. Also ist $\frac{1+\sqrt{m}}{2}$ als Nullstelle von X^2-X+q ganz über $\mathbb{Z}$. Da $2\cdot\left(\frac{1+\sqrt{m}}{2}\right)$ aus G ist, folgt nach 10.9, dass $\{1,\frac{1+\sqrt{m}}{2}\}$ eine ganze Basis von $\mathcal{O}_K$ ist.

10.13 Weitere Beispiele

(1) Sei α Nullstelle des irreduziblen Polynoms X^3+X+1 in seinem Zerfällungskörper. Dann ist $\{1,\alpha,\alpha^2\}$ $\mathbb{Q}$-Basis von $K=\mathbb{Q}(\alpha)$. Nach 9.13 gilt

$$D_{K/\mathbb{Q}}(1,\alpha,\alpha^2)=D(X^3+X+1)=(-1)^{3\cdot 2/2}(3^3+(-1)^2\cdot 2^2)=-31.$$

Da -31 quadratfrei ist, ist dies eine **ganz** Basis nach 10.9.1. Also folgt

$$\mathcal{O}_K = \mathbb{Z}[\alpha]$$

.

(2) $f = X^3 - X - 1$. Wieder ist $\{1, \alpha, \alpha^2\}$ ganze Basis, da

$$D(f) = (-1)^{3\cdot 2/2}(3^3(-1)^2 + (-1)^2 \cdot 2^2 \cdot (-1)^3) = -23.$$

$\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(3) $f = X^5 - X - 1$

$D(f) = (-1)^{5\cdot 4/2}(5^5 \cdot (-1)^4 + (-1)^4 \cdot 4^4 \cdot (-1)^5) = 3125 - 256 = 2869$

$D(f) = 19 \cdot 151$. Also ist $D(f)$ wieder quadratfrei, so dass $\mathcal{O}_K = \mathbb{Z}[\alpha]$ mit ganzer Basis $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$.

Die Beispiele belegen, dass es ohne den Einsatz theoretischer Überlegungen oft schwierig sein kann, ganze Basen zu finden. Das folgende Ergebnis soll dabei helfen.

10.14 Satz: Ist K ein algebraischer Zahlkörper, dann ist $\mathcal{O}_K$ der größte Unterring von K, der als abelsche Gruppe unter $+$ endlich erzeugt ist.

Beweis: Wir wissen, dass $\mathcal{O}_K$ freie abelsche Gruppe vom Rang $[K : \mathbb{Q}]$ ist. Sie nun A ein Unterring von K, der als abelsche Gruppe endlich erzeugt ist. Nach 7.4 ist jedes $a \in A$ ganz über $\mathbb{Z}$, da $\mathbb{Z} \subset A$ endlich ist. Also ist $A \subset \mathcal{O}_K$. □

Teil III
Die Idealklassengruppe

11 Historische Vorbemerkungen

Den Mathematikern des 19. und 20. Jahrhunderts war es ein Dorn im Auge, dass sie keinen Beweis für die Fermat-Vermutung fanden:

$$x^n + y^n = z^n$$

hat keine nicht-triviale Lösung in $\mathbb{N}^3$, falls $n \geq 3$.

Für kleine n wurde das z.T. mit großem Aufwand gezeigt, wobei die Zerlegungsmethode eine zentrale Rolle spielte. Ich demonstriere sie an folgendem Beispiel.

11.1 Beispiel: Gesucht werden die Lösungen der diophantischen Gleichung

$$x^2 = y^4 + 8$$

d.h. alle ganzzahligen Lösungen.

Ist $(x, y) \in \mathbb{Z}^2$ eine Lösung, dann sind $(\pm x, \pm y)$ in allen Kombinationen von $\pm$ ebenfalls Lösungen. Es genügt also, die Lösungen in $\mathbb{N}^2$ zu bestimmen. Seien also $x, y \in \mathbb{N}$.

$$x^2 = y^4 + 8 \iff 8 = x^2 - y^4 = (x - y^2) \cdot (x + y^2).$$

Jetzt nutzen wir die eindeutige Primfaktorzerlegung von 8 in $\mathbb{N}$ aus: Es gibt keine Lösung mit $y = 0$. Also ist

$$0 < x - y^2 < x + y^2.$$

(Da $x + y^2 > 0$, muss auch $x - y^2 > 0$ sein). Damit haben wir zwei Fälle:

1. Fall: $x - y^2 = 1$ und $x + y^2 = 8$,

2. Fall: $x - y^2 = 2$ und $x + y^2 = 4$.

Addieren wir die beiden Gleichungen im 1.Fall, erhalten wir $2x = 9$, eine Gleichung, die in $\mathbb{N}$ keine Lösung hat. Im 2. Fall erhalten wir $2x = 6$, also $x = 3$, und damit $y^2 = 1$. Es folgt $(x, y) = (3, 1)$ ist die einzige Lösung in $\mathbb{N}^2$.

Gabriel Lamé (1795-1870), der 1839 mit großem Einfallsreichtum einen Beweis der Fermat-Vermutung für $n = 7$ gefunden hatte, trug 1847 vor den Mitgliedern der Pariser Akademie der Wissenschaften einen allgemeinen Beweis der Fermat-Vermutung vor, indem er die Fermat-Gleichung im Ring ganzer Zahlen $\mathcal{O}_K$ eines geeigneten Kreisteilungskörpers K zerlegte und dann ähnlich, wenn auch erheblich komplexer, wie wir im Beispiel 11.1 argumentierte. Dabei benutzte er natürlich implizit, dass $\mathcal{O}_K$ ein faktorieller Ring ist. Am Ende seiner Rede dankte er Joseph Liouville, dass er ihn auf die Idee gebracht habe, eine solche Faktorisierung mit Hilfe der komplexen Zahlen zu versuchen. Liouville holte Lamé in die Wirklichkeit zurück, indem er ihn auf die entscheidende Lücke im Beweis hinwies: Woher wusste er, dass die Faktorisierung eindeutig war.

Lamé konnte diese Lücke nicht schließen. Beschämt schrieb er seinem Freund Dirichlet: “Wenn Du nur in Paris gewesen wärest, oder ich in Berlin, dann wäre dies alles nicht geschehen”.

In der Tat hätte Dedekind ihn auf eine Arbeit von Ernst Eduard Kummer (1810-1893) aus dem Jahre 1844 in der völlig unbekannten Gratulationsschrift der Universität Breslau zur Jubelfeier der Universität Königsberg hinweisen können, in der Kummer bewies, dass die eindeutige Primfaktorzerlegung nicht in allen Ringen von ganzen Zahlen von Kreisteilungskörpern gilt.

Ein Beispiel dafür, das Ringe ganzer Zahlen nicht faktoriell zu sein brauchen, haben wir in der Einführung kennen gelernt, auf das wir jetzt nochmals eingehen wollen.

11.2 Beispiel: Im Körper $K = \mathbb{Q}(\sqrt{-5})$ ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z} \cdot \sqrt{-5}$ nach 7.3 oder 10.12. Es gilt in $\mathcal{O}_K$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 + \sqrt{-5}) \qquad (11.2*)$$

Die Zahlen $2, 3, 1 \pm \sqrt{-5}$ sind irreduzibel. Dies folgt sofort aus Normbetrachtungen:

$$N_{K/\mathbb{Q}}(2) = 4, \quad N_{K/\mathbb{Q}}(3) = 9, \quad N_{K/\mathbb{Q}}(1 + \sqrt{-5}) = 6.$$

Die Norm eines beliebigen Elementes in $\mathcal{O}_K$ ist positiv und damit in $\mathbb{N}$.

Nach 8.7 ist $x \in \mathcal{O}_K$ damit genau dann eine Einheit, wenn $N_{K/\mathbb{Q}}(x) = 1$. Wären $2, 3, 1 \pm \sqrt{-5}$ reduzibel, gäbe es Elemente $x, y \in \mathcal{O}_K$ mit $N_{K/\mathbb{Q}}(x) = 2$ bzw. $N_{K/\mathbb{Q}}(y) = 3$. Da aber

$$N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

ist das unmöglich. Aus demselben Grund sind $2, 3$ und $1 + \pm\sqrt{-5}$ nicht assoziiert.

Wäre $\mathcal{O}_K$ faktoriell, dann hätten wir zwei grundsätzlich verschiedene Faktorisierungen von 6 in Primelemente, denn in faktoriellen Ringen sind irreduzible Elemente prim.

Angeregt durch die Zahlbereichserweiterungen wie der damals gerade erfundenen komplexen Zahlen, hatte Eduard Kummer die Idee, Ringe ganzer Zahlen $\mathcal{O}_K$ durch sogenannte "ideale Zahlen" zu erweitern, so dass sich die Elemente aus $\mathcal{O}_K$ **eindeutig** als Produkte idealer Zahlen schreiben lassen. In unserem Beispiel müßte es dann "ideale Zahlen" x_1, x_2 mit Norm 2 und y_1, y_2 mit Norm 3 geben, so dass

$$1 + \sqrt{-5} = x_1 \cdot y_1, \quad 1 - \sqrt{-5} = x_2 \cdot y_2, \quad 2 = x_1 \cdot x_2, \quad 3 = y_1 \cdot y_2,$$

und das Problem mit Gleichung 11.2 $*$ wäre aufgelöst.

Aus den "idealen Zahlen" hat Richard Dedekind (1831-1916) die Idealtheorie entwickelt. Das ist nicht überraschend: Ist x "ideale Zahl", so soll sie Teiler einer Zahl $a \in \mathcal{O}_K$ sein, sie soll die Teilbarkeitsregeln erfüllen.

$$x|a \text{ und } x|b \Rightarrow x|a \pm b \text{ und } x|t \cdot a \quad \forall a, b, t \in \mathcal{O}_K.$$

Außerdem soll sie durch die Menge der Zahlen, die sie teilt, also durch

$$\{a \in \mathcal{O}_K;\ x|a\}$$

eindeutig bestimmt sein. Aber diese Menge ist das "von x erzeugte Ideal".

Kummer konnte sein Programm für viele, aber nicht für alle Ringe $\mathcal{O}_K$ durchführen.

12 Dedekind-Ringe

12.1 Definition: Ein R-Modul heißt *noethersch*, wenn jeder Teilmodul endlich erzeugt ist. Ein Ring R heißt *noethersch*, wenn er als R-Modul noethersch ist.

12.2 Da die Untermoduln des R-Moduls R genau die Ideale von R sind, ist ein Ring noethersch, wenn jedes Ideal als R-Modul endlich erzeugt ist.

Wir verschaffen uns jetzt einige Werkzeuge für noethersche R-Moduln.

12.3 Satz: Für einen R-Modul M sind äquivalent

(1) M ist noethersch.

(2) M erfüllt die *aufsteigende Kettenbedingung*, d.h. jede Kette von Teilmoduln
$$N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq \ldots$$
von M ist endlich.

(3) M erfüllt die *Maximalitätsbedingung*, d.h. jede nicht-leere Familie von Teilmoduln von M besitzt einen maximalen Teilmodul.

Beweis: (1) $\Rightarrow$ (2): Setze $N = \bigcup N_i$. Damit ist N ein Teilmodul von M, also endlich erzeugt, etwa $N = Rx_1 + \ldots + Rx_n$. Da jedes x_i in einem der Teilmoduln N_k liegt, gibt es ein N_k, das alle enthält. Also $N = N_k$.

(2) $\Rightarrow$ (3): Sei $\mathcal{F}$ eine nicht-leere Familie von Teilmoduln von M. Wähle ein $N_0 \in \mathcal{F}$. Ist N_0 nicht maximal in $\mathcal{F}$, gibt es einen größeren Teilmodul $N_0 \subsetneqq N_1$ aus $\mathcal{F}$. Diesen können wir nach (2) nur endlich oft finden.

(3) $\Rightarrow$ (1): Sei N ein Teilmodul von M und $\mathcal{F}$ die Familie aller endlich erzeugten Teilmoduln $N' \subset N$. Sei $L \in \mathcal{F}$ ein maximales Element. Ist $L \neq N$, gibt es ein $x \in N \backslash L$. Dann ist aber $L + R \cdot x$ ein endlich erzeugter Teilmodul von N, der größer als L ist. $\square$

12.4 Satz: Sei M ein R-Modul und $N \subset M$ ein Teilmodul. Dann gilt

$$M \text{ noethersch} \iff N \text{ und } M/N \text{ sind noethersch.}$$

Beweis: „$\Rightarrow$“ Offensichtlich ist N noethersch. Sei nun $p : M \to M/N$ die Projektion und $U \subset M/N$ ein Teilmodul. Dann ist $p^{-1}(U)$ ein endlich erzeugter Teilmodul: $p^{-1}(U) = Rx_1, \ldots Rx_n$. Es folgt $U = R \cdot \overline{x}_1 + \ldots + R \cdot \overline{x}_n$ mit $\overline{x}_i = p(x_i)$.

„$\Leftarrow$“ Sei $U \subset M$ ein Teilmodul. Dann gilt

$$U/U \cap N \cong (U + N)/N \subset M/N.$$

Also ist $U/U \cap N$ endlich erzeugt, etwa von $\overline{u}_1, \ldots, \overline{u}_k$. Auch $U \cap N$ ist endlich erzeugt, etwa von $v_1, \ldots, \ v_l$. Dann ist U von $u_1, \ldots, u_k, v_1, \ldots, v_l$ erzeugt. (vergl. Beweis von 8.5). $\square$

12.5 Aufgabe: Zeigen Sie: Jeder Hauptidealring ist noethersch.

Folgendes Resultat ist der Grund dafür, uns mit noetherschen Ringen und Moduln zu beschäftigen.

12.6 Satz: Ist K ein algebraischer Zahlkörper, dann ist $\mathcal{O}_K$ noethersch, ganz abgeschlossen, und jedes Primideal $\mathfrak{p} \neq 0$ ist ein maximales Ideal.

Beweis: Wir haben es mit $\mathbb{Z}$-Moduln, also abelschen Gruppen zu tun. $(\mathcal{O}_K, +)$ ist freie abelsche Gruppe vom Rang $[K : \mathbb{Q}]$, also endlich erzeugt, und jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt. Als ganzer Abschluss von $\mathbb{Z}$ in K ist $\mathcal{O}_K$ nach 7.12 ganz abgeschlossen, denn nach 7.14 ist K der Quotientenkörper von $\mathcal{O}_K$.

Sei nun $\mathfrak{p} \neq 0$ ein Primideal. Wir zeigen gleich, dass $\mathfrak{p} \cap \mathbb{Z} = (p)$, p prim, gilt. Es folgt, dass $\mathbb{F}_p = \mathbb{Z}/(p)$ ein Unterring von $\mathcal{O}_K/\mathfrak{p}$, ist. Da $(p) \subset \mathfrak{p}$, ist $\mathcal{O}_K/\mathfrak{p}$ ein Quotient von $\mathcal{O}_K/(p) \cong (\mathbb{F}_p)^n$, $n = [K : \mathbb{Q}]$. Also ist $\mathcal{O}_K/\mathfrak{p}$ ein endlicher Integritätsring. Aber endliche Integritätsringe sind Körper. Also ist $\mathfrak{p}$ maximal. $\square$

12.7 Lemma: (1) Sind $R \subset A$ Ringe, $J \subset A$ ein Ideal und $x \in J$ Nullstelle des Polynoms $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in R[X]$, dann ist $a_0 \in J \cap R$.

(2) Ist K ein Zahlkörper und $J \neq 0$ Ideal in $\mathcal{O}_K$, dann ist $J \cap \mathbb{Z} \neq \{0\}$.

(3) Ist $\mathfrak{p} \neq 0$ ein Primideal in $\mathcal{O}_K$, dann ist $\mathbb{Z} \cap \mathfrak{p} = (p)$, p prim.

Beweis: (1) $a_0 = -a_n \cdot x^n - a_{n-1} x^{n-1} - \ldots - a_1 x$. Die rechte Seite liegt in J.
(2) Sei $x \neq 0$ aus J. Dann erfüllt x eine Ganzheitsgleichung.

$$x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \quad a_i \in \mathbb{Z},\ a_0 \neq 0.$$

(3) $\mathbb{Z} \cap \mathfrak{p}$ ist ein Ideal in $\mathbb{Z}$. Nach (2) ist es nicht $\{0\}$. Da $\mathbb{Z}/\mathbb{Z} \cap \mathfrak{p}$ ein Teilring von $\mathcal{O}_K/\mathfrak{p}$ ist, ist $\mathbb{Z}/\mathbb{Z} \cap \mathfrak{p}$ ein Integritätsring, also $\mathbb{Z} \cap \mathfrak{p}$ ein Primideal in $\mathbb{Z}$. □

Die Teilbarkeitslehre der Ideale in $\mathcal{O}_K$ macht nur von den Eigenschaften aus 12.6 Gebrauch. Sie wurde von Dedekind entwickelt. Daher macht man folgende Definition.

12.8 Definition: Ein *Dedekindring* ist ein noetherscher, ganz abgeschlossener Integitätsring, in dem jedes von 0 verschiedene Primideal maximal ist und der kein Körper ist.

12.9 Satz: Jeder Hauptidealring ist eine Dedekindring.

Beweis: Ein Hauptidealring ist noethersch nach 12.5, als faktorieller Ring nach 7.15 ganz abgeschlossen und jedes von 0 verschiedene Primideal ist maximal nach 2.5. □

Dedekindringe sind die natürliche Verallgemeinerung von Hauptidealringen, wie folgender zentraler Satz zeigt.

12.10 Satz: Ist R ein Dedekindring, dann besitzt jedes nicht-triviale Ideal J eine bis auf Reihenfolge eindeutige Zerlegung

$$J = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$$

in Primideale $\mathfrak{p}_i$ von R. (Nicht-trivial bedeutet $J \neq 0$, $J \neq R$.)

Das ist ein Satz, wie ihn Kummer sich wünschte. Sein Beweis ist nicht einfach und wird uns eine Weile beschäftigen. Als vorgezogene Anwendung beweisen wir eine Umkehrung von 12.9.

12.11 Satz: Jeder faktorielle Dedekindring R ist ein Hauptidealring.

Beweis: Sei zunächst $\mathfrak{p} \subset R$ ein nicht triviales Primideal, $a \neq 0$ aus $\mathfrak{p}$ und

$$a = p_1 \cdot \ldots \cdot p_k$$

seine Primfaktorzerlegung. Da $\mathfrak{p}$ ein Primideal ist, liegt mindestens einer der Faktoren, etwa p_1 in $\mathfrak{p}$, also $(p_1) \subset \mathfrak{p}$. Da (p_1) aber maximal ist, folgt $(p_1) = \mathfrak{p}$. Ist nun J ein beliebiges nicht-triviales Ideal und $J = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ seine Zerlegung in Primideale $\mathfrak{p}_i = (p_i)$, dann folgt $J = (p_1 \cdot p_2 \cdot \ldots \cdot p_r)$. □

Dem Beweis von 12.10 schicken wir zwei Hilfssätze voraus:

12.12 Lemma: Ist J ein nicht-triviales Ideal in einem noetherschen Ring R, dann gibt es von 0 verschiedene Primideale $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, so dass

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subset J.$$

el

Beweis: Angenommen, dies ist falsch. Wir betrachten die Familie $\mathcal{F}$ aller Ideale von R, für die der Satz nicht gilt. Da R noethersch ist, gibt es ein maximales Gegenbeispiel J. Dieses kann kein Primideal sein, d.h. es gibt Elemente $x, y \in R$, so dass $x \cdot y \in J$, aber $x \notin J$ **und** $y \notin J$. Dann gilt

$$J \subsetneqq J + (x), \quad J \subsetneqq J + (y) \quad \text{und} \quad (J + (x)) \cdot (J + (y)) \subset J + (x \cdot y) = J.$$

Da J ein maximales Gegenbeispiel ist, enthalten $J+(x)$ und $J+(y)$ Produkte von Primidealen $\neq 0$ und damit aber auch J, ein Widerspruch. □

12.13 Lemma: Sei $\mathfrak{p}$ Primideal in einem Dedekindring R. Sei K der Quotientenkörper von R und

$$\mathfrak{p}^{-1} = \{x \in K; x \cdot \mathfrak{p} \subset R\}.$$

Dann gilt:

(1) $\mathfrak{p}^{-1}$ ist ein R-Modul.

(2) Ist $J \subset R$ ein Ideal, dann ist $J \cdot \mathfrak{p}^{-1} := \{\sum_{i=1}^{n} a_i \cdot x_i;\ n \in \mathbb{N},\ a_i \in J,\ x_i \in \mathfrak{p}^{-1}\}$ ebenfalls ein R-Modul, und es gilt $J \cdot \mathfrak{p}^{-1} \neq J$, falls $J \neq 0$.

Beweis: Die Modulstruktur ist in beiden Fällen klar. Sei nun $a \neq 0$ aus $\mathfrak{p}$. Nach 12.12 gibt es Primideale $\mathfrak{p}_i \neq 0$, $i = 1, \ldots, r$, so dass

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

Wir wählen eine Zerlegung mit minimalem r. Da $\mathfrak{p}$ prim ist, liegt mindestens einer der Faktoren, etwa $\mathfrak{p}_1$ in $\mathfrak{p}$. Wegen der Maximalität von $\mathfrak{p}$, folgt $\mathfrak{p}_1 = \mathfrak{p}$. Wegen der Minimalität von r ist $\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \ldots \cdot \mathfrak{p}_r \not\subset (a)$, d.h. es gibt ein b aus $\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \ldots \cdot \mathfrak{p}_r$, so dass $b \notin (a) = R \cdot a$, also $a^{-1} \cdot b \notin R$. Da aber $b \cdot \mathfrak{p} \subset (a) = R \cdot a$, ist $a^{-1} \cdot b \cdot \mathfrak{p} \subset R$, also $a^{-1} \cdot b \in \mathfrak{p}^{-1}$. Es folgt

$$\mathfrak{p}^{-1} \not\subset R. \qquad (*)$$

Sei nun $J \neq 0$ ein Ideal von R. Da J Teilmodul von R ist, ist J als R-Modul endlich erzeugt, etwa von $\alpha_1, \ldots \alpha_n$. Wir nehmen an, dass $J \cdot \mathfrak{p}^{-1} = J$. Dann haben wir für jedes $x \in \mathfrak{p}^{-1}$ Gleichungen

$$x \cdot \alpha_i = \sum_{j=0}^{n} r_{ij} \alpha_j \quad r_{ij} \in R.$$

Also

$$\sum_{j=0}^{n} (x \cdot \delta_{ij} - r_{ij}) \alpha_j = 0,$$

wobei δ_{ij} das Kronecker-Symbol ist. Sei $A = (x \cdot \delta_{ij} - r_{ij})_{i,j}$. Dann ist

$$A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0, \quad \text{also} \quad 0 = A^* \cdot A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \det(A) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Ist $d = \det A$, so folgt $d \cdot \alpha_1 = d\alpha_2 = \ldots = d\alpha_n = 0$. Da $\alpha_1, \ldots, \alpha_n$ ein Erzeugendensystem von $J \neq 0$ ist, sind nicht alle $\alpha_i = 0$. Da ein Dedekindring nullteilerfrei ist, ist $d = 0$. Damit ist x Nullstelle des normierten Polynoms

$$f(X) = \det(X \cdot E_n - (r_{ij})) \in R[X],$$

d.h. x ist ganz über R und damit in R, weil R ganz abgeschlossen ist. Es folgt $\mathfrak{p}^{-1} \subset R$, im Widerspruch zu $(*)$. □

12.14 Aufgabe: Ermitteln Sie die Aussagen des Zorn'schen Lemmas und des Auswahlaxioms. Finden Sie heraus, was die beiden miteinander zu tun haben.

Beweisen Sie mit Hilfe des Zorn'schen Lemmas: Jedes Ideal eines Ringes R ist in einem maximalen Ideal enthalten.

Beweis von 12.10 *Existenz:* Sei $\mathcal{F}$ die Familie aller von (0) und R verschiedenen Ideale, die keine Primzerlegung besitzen. Ist $\mathcal{F}$ nicht leer, besitzt

es maximale Elemente J, da R noethersch ist. Nach 12.14 liegt J in einem maximalen Ideal $\mathfrak{p}$. Als maximales Ideal ist $\mathfrak{p}$ prim. Aus der Definition von $\mathfrak{p}^{-1}$ folgt sofort, dass $R \subset \mathfrak{p}^{-1}$. Also gilt

$$J = J \cdot R \subset J \cdot \mathfrak{p}^{-1} \subset \mathfrak{p} \cdot \mathfrak{p}^{-1} \subset R,$$

letzteres nach Definition von $\mathfrak{p}^{-1}$. Nach 12.13 gilt $J \subsetneqq J\mathfrak{p}^{-1}$ und $\mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1}$. Da $\mathfrak{p}$ ein maximales Ideal ist und $\mathfrak{p}\mathfrak{p}^{-1}$ als Teil-R-Modul von R ein Ideal ist, folgt $\mathfrak{p}\mathfrak{p}^{-1} = R$. Da $J \neq J\mathfrak{p}^{-1}$ und $J\mathfrak{p}^{-1}$ als Untermodul von R ein Ideal ist, folgt aus der Maximalität von J, dass $J\mathfrak{p}^{-1}$ eine Primzerlegung $J\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ besitzt. Es folgt

$$J = J \cdot R = J\mathfrak{p}^{-1} \cdot \mathfrak{p} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \cdot \mathfrak{p}$$

ein Widerspruch.

Eindeutigkeit: Seien

$$J = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$$

zwei Primzerlegungen von J. Da $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s \subset \mathfrak{p}_1$ und $\mathfrak{p}_1$ ein Primideal ist, ist ein Faktor $\mathfrak{q}_i$, nach Umordnen $\mathfrak{q}_1$, in $\mathfrak{p}_1$ enthalten: $\mathfrak{q}_1 \subset \mathfrak{p}_1$. Da $\mathfrak{q}_1$ prim ist, ist $\mathfrak{q}_1$ maximal, also $\mathfrak{q}_1 = \mathfrak{p}_1$. Wir multiplizieren mit $\mathfrak{p}_1^{-1}$ und nutzen aus, dass $\mathfrak{p} \cdot \mathfrak{p}^{-1} = R$ ist für jedes Primideal $\mathfrak{p} \neq 0$. Es folgt

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_2 \cdot \mathfrak{q}_3 \cdot \ldots \cdot \mathfrak{q}_s.$$

Durch Induktion folgt das Ergebnis. □

12.15 Aus dem Beweis halten wir fest:
(1) Ist $\mathfrak{p}$ ein Primideal, dann gilt $R \subset \mathfrak{p}^{-1}$
(2) Ist $\mathfrak{p} \neq 0$ ein Primideal, dann gilt $\mathfrak{p} \cdot \mathfrak{p}^{-1} = R$

13 Gebrochene Ideale

Sei R ein Dedekindring und K sein Quotientenkörper. Die Ergebnisse von §12 erlauben es uns, in R eine Teilertheorie ähnlich wie in Hauptidealringen zu betreiben, nur dass wir Elemente durch Ideale ersetzen müssen. Da $J \cdot R = J$, verhält sich R wie die 1, ganz im Sinne der Gleichheit $R = (1)$. Wir schreiben oft auch:

$J_1 | J_2$, wenn $J_2 \subset J_1$, dies entspricht $a|b \iff (b) \subset (a)$
J_1, J_2, *teilerfremd,* wenn $J_1 + J_2 = (1) = R$

usw.

Ist $\mathfrak{p}$ ein Primideal in R, dann verhält sich der R-Modul $\mathfrak{p}^{-1} \subset K$ wie ein Inverses, denn $\mathfrak{p} \cdot \mathfrak{p}^{-1} = R$, wie wir im Beweis von 12.10 gesehen haben. Diese Beobachtung wolle wir vertiefen:

13.1 Definition: Ein *gebrochenes Ideal* von K ist ein endlich erzeugter R-Untermodul $J \neq 0$ von K. Die Ideale von R nennen wir *ganze Ideale* von K. (Da R noethersch ist, sind Ideale in R endlich erzeugte R-Teilmoduln von K.)

13.2 Sei $M \neq 0$ ein R-Teilmodul von K. Dann gilt

$$M \text{ ist gebrochenes Ideal} \iff \text{es gibt ein } r \neq 0 \text{ in } R, \text{ so dass } r \cdot M \subset R.$$

Beweis: Sei M ein gebrochenes Ideal, $M = Rx_1 + \ldots + Rx_n \subset K$ mit $x_i = \frac{r_i}{s_i}$, $r_i, s_i \in R$. Sei $r = s_1 \cdot \ldots \cdot s_n$. Dann ist $r \cdot M \subset R$. Sei umgekehrt $M \subset K$ ein R-Modul, so dass $r \cdot M \subset R$ für ein $r \neq 0$ aus R. Dann ist $r \cdot M$ ein R-Teilmodul von R und damit endlich erzeugt, weil R noethersch ist. Ist $r \cdot M = R \cdot r_1 + \ldots + R \cdot r_n$ mit $r_i \in R$, dann folgt $M = R \cdot \frac{r_1}{r} + \ldots + R \cdot \frac{r_n}{r}$. □

Gebrochene Ideale multiplizieren wir wie ganze Ideal:

$$J_1 \cdot J_2 = \left\{ \sum_{i=1}^{n} a_i \cdot b_i;\ n \in \mathbb{N},\ a_i \in J_1,\ b_i \in J_2 \right\}.$$

Offensichtlich ist $J_1 \cdot J_2$ wieder ein endlich erzeugter R-Untermodul von K und $J_1 \cdot J_2 \neq 0$. Also ist $J_1 \cdot J_2$ wieder ein gebrochenes Ideal.

13.3 Satz: Die gebrochenen Ideale J bilden eine abelsche Gruppe $\mathcal{J}_K$, die *Idealgruppe* von K. Das Einselement ist $(1) = R$, das Inverse zu J ist

$$J^{-1} = \{x \in K;\ x \cdot J \subset R\}.$$

Beweis: Assoziativität und Kommutativität unter der Multiplikation sind klar. Ebenfalls klar ist, dass $J \cdot R = J$, da $1 \in R$.

Für ein Primelement $\mathfrak{p} \neq 0$ haben wir bereits gezeigt, dass $\mathfrak{p} \cdot \mathfrak{p}^{-1} = R$. Ist nun $J = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ ein ganzes Ideal, folgt, dass $J' = \mathfrak{p}_1^{-1} \cdot \ldots \cdot \mathfrak{p}_r^{-1}$ ein Inverses ist. Aus $J' \cdot J = R$ folgt $x \cdot J \subset R$ für alle $x \in J'$, also $J' \subset J^{-1}$. Umgekehrt gilt für $x \in J^{-1}$, dass $x \cdot J \subset R$, also $x \cdot R = x \cdot J \cdot J' \subset R \cdot J' = J'$, so dass $x \in J'$. Also ist $J' = J^{-1}$.

Sei nun J ein gebrochenes Ideal und $r \neq 0$ aus R, so das $r \cdot J \subset R$. Aus der Definition von J^{-1} folgt leicht, dass $(r \cdot J)^{-1} = r^{-1} \cdot J^{-1}$ ist. Es folgt

$$J \cdot J^{-1} = r \cdot r^{-1} \cdot J \cdot J^{-1} = (r \cdot J) \cdot (r^{-1} \cdot J^{-1}) = (r \cdot J) \cdot (r \cdot J)^{-1} = R.$$

□

13.4 Folgerung: Sei $\mathcal{P}$ die Menge der Primideale $\mathfrak{p} \neq 0$ von R. Dann besitzt jedes gebrochene Ideal J von K eine eindeutige Produktdarstellung

$$J = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\nu_\mathfrak{p}} \quad \nu_\mathfrak{p} \in \mathbb{Z}, \text{ fast alle } \nu_\mathfrak{p} = 0.$$

Damit ist $\mathcal{J}_K$ die durch die Primideale $\mathfrak{p} \neq 0$ von R erzeugte freie abelsche Gruppe.

Beweis: Sei J ein gebrochenes Ideal und $r \neq 0$ aus R, so dass $I := r \cdot J \subset R$. Dann ist I ein Ideal in R und $J = (r)^{-1} \cdot I$. Die ganzen Ideale I und (r) besitzen eine eindeutige Primfaktorisierung. Damit folgt 13.4. □

13.5 Definition: Sei $a \neq 0$ aus K, dann nennen wir $(a) := R \cdot a$ ein *gebrochenes Hauptideal*.

13.6 Für gebrochene Hauptideale (a) und (b) gilt offensichtlich

$$(a) \cdot (b) = (a \cdot b).$$

Damit bilden sie eine Untergruppe $\mathcal{H}_K$ von $\mathcal{J}_K$.

13.7 Definition: Die Faktorgruppe $\mathcal{C}l_K = \mathcal{J}_K / \mathcal{H}_K$ heißt *Idealklassengruppe* oder kurz *Klassengruppe* von K.

13.8 Wir haben eine exakte Sequenz abelscher Gruppen

$$1 \xrightarrow{f_0} R^* \xrightarrow{f_1} K^* \xrightarrow{f_2} \mathcal{J}_K \xrightarrow{f_3} \mathcal{C}l_K \xrightarrow{f_4} 1$$

d.h. Bild f_i = Kern f_{i+1} für $i = 0, 1, 2, 3$. Hier ist $f_2(a) = (a)$ und f_3 die Projektion.

$\mathcal{C}l_K$ beschreibt damit die Erweiterung, die beim Übergang vom Bereich der Zahlen K^* zu (gebrochenen) Idealen in $\mathcal{J}_K$ erzielt wird, R^* beschreibt den Verlust an Information. Daher sind beide Gruppen R^* und $\mathcal{C}l_K$ für die Entwicklung der Zahlentheorie von fundamentaler Bedeutung.

13.9 Bemerkung: Ein Dedekindring R ist genau dann ein Hauptidealring, wenn $\mathcal{C}l_K = \{1\}$.

Beweis: Ist R ein Hauptidealring und J ein gebrochenes Ideal, dann gibt es ein $r \neq 0$ aus R, so dass $r \cdot J \subset R$. Da $r \cdot J$ ein Ideal in R ist, gibt es ein $a \in R$, so dass $r \cdot J = (a)$. Es folgt $J = \left(\frac{a}{r}\right)$, d.h. J ist ein gebrochenes Hauptideal und repräsentiert 1 aus $\mathcal{C}l_K$.

Ist $\mathcal{C}l_K = \{1\}$ und $J \neq 0$ ein Ideal in R, dann ist J ein gebrochenes Hauptideal $J = R \cdot a$ mit $a \in K$. Da $1 \in R$, ist a ganz, d.h. $J = (a)$ mit $a \in R$. $\square$

Man kann zeigen, dass jede abelsche Gruppe als Klassengruppe eines Dedekindringes auftreten kann. Beschränkt man sich nur auf Zahlringe $\mathcal{O}_K$ gibt es aber wichtige Endlichkeitsbeschränkungen.

14 Gitter

Rechnet man mit Ringen ganzer Zahlen $\mathcal{O}_K$ für quadratische Körper $\mathbb{Q}(\sqrt{m})$, ist es oft günstig in $\mathbb{C}$ zu rechnen. Diese Betrachtungsweise hat Hermann Minkowski (1864-1909) auf beliebige Zahlkörper ausgedehnt und sehr erfolgreich eingesetzt. Für die Entwicklung dieser Theorie müssen wir uns zunächst mit Gittern beschäftigen.

14.1 Definition: Ein *Gitter* in einem n-dimensionalen $\mathbb{R}$-Vektorraum V ist eine Untergruppe von $(V, +)$ der Form

$$\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren $v_1, \ldots, v_m$. Wir nennen $\{v_1, \ldots, v_m\}$ eine *Basis* und die Menge

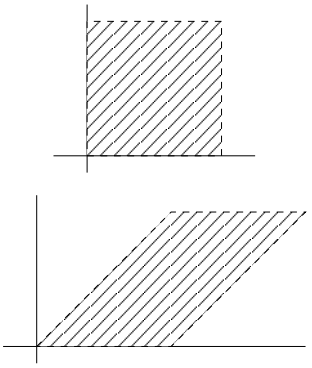
$$\Phi := \{r_1v_1 + \ldots + r_mv_m;\ r_i \in \mathbb{R},\ 0 \leq r_i < 1\}$$

eine *Grundmasche* des Gitters Γ. Ein Gitter heißt *vollständig* oder $\mathbb{Z}$-*Struktur* auf V, wenn $m = n$ ist.

14.2 Ein Gitter $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ ist somit eine freie abelsche Gruppe vom Rang m, aber nicht jede freie abelsche Gruppe vom Rang m bildet ein Gitter in V.

Beispiel: $\mathbb{Z} + \mathbb{Z} \cdot \sqrt{2} \subset \mathbb{R}$ ist eine freie abelsche Gruppe vom Rang 2, aber **kein** Gitter in $\mathbb{R}$.

14.3 Beispiel: $\mathbb{Z} \cdot \binom{0}{1} + \mathbb{Z} \cdot \binom{1}{0} \subset \mathbb{R}^2$ ist das Gitter, das aus allen Punkten in $\mathbb{Z} \times \mathbb{Z} \subset \mathbb{R} \times \mathbb{R}$ besteht. Das Einheitsquadrat ist eine Grundmasche.



Dieses Gitter ist vollständig.
Da sich $\binom{m}{n} \in \mathbb{Z}^2$ aber auch in der Form

$$\binom{m}{n} = (m-n)\binom{1}{0} + n \cdot \binom{1}{1}$$

darstellen läßt, ist dieses Gitter auch durch $\mathbb{Z} \cdot \binom{1}{0} + \mathbb{Z} \cdot \binom{1}{1}$ mit nebenstehender Grundmasche gegeben.

Wir suchen nun eine Charakterisierung eines Gitters, die von der Wahl einer Basis unabhängig ist.

14.4 Definition: Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und $\varphi : V \to \mathbb{R}^n$ ein linearer Isomorphismus. Eine Untergruppe $\Gamma < (V, +)$ heißt *diskret*, wenn $\varphi(\Gamma) \cap \mathbb{B}^n(r)$ für jedes $r \in \mathbb{R}$ nur endlich viele Elemente hat. Hier bezeichnet $\mathbb{B}^n(r) = \{r \in \mathbb{R}^n;\ ||x|| \leq r\}$ den Ball von Radius r um 0.

Man macht sich leicht klar, dass diese Definition von der Wahl von φ unabhängig ist.

14.5 Sei $\Gamma < (V, +)$ ein Gitter mit Basis $\{v_1, \ldots, v_m\}$ und Grundmasche Φ. Dann gilt

$$\bigcup_{\gamma \in \Gamma} \gamma + \Phi = \mathbb{R} \cdot v_1 + \ldots + \mathbb{R} \cdot v_m.$$

Insbesondere ist Γ genau dann vollständig, wenn

$$V = \bigcup_{\gamma \in \Gamma} \gamma + \Phi$$

ist.

Beweis: Sei $W = \mathbb{R} \cdot v_1 + \ldots + \mathbb{R} \cdot v_m$ der von $\{v_1, \ldots, v_m\}$ aufgespannte Teilraum von V. Dann liegen Φ und Γ in W, also auch $\bigcup_{\gamma \in \Gamma} \gamma + \Phi$. Ist umgekehrt $w = r_1 \cdot v_1 + \ldots + r_m \cdot v_m$ aus W, dann ist $r_i = q_i + s_i$ mit $q_i \in \mathbb{Z}$ und $0 \leq s_i < 1$. Also ist

$$w = \underbrace{q_1 \cdot v_1 + \ldots + q_m v_m}_{\in \Gamma} + \underbrace{s_1 \cdot v_1 + \ldots + s_m v_m}_{\in \Phi}$$

Es folgt $W = \bigcup_{\gamma \in \Gamma} \gamma + \Phi$. □

14.6 Satz: Eine Untergruppe Γ von $(V, +)$ ist genau dann ein Gitter, wenn Γ diskret ist.

Beweis: Sei $\Gamma < (V,+)$ diskret und $V_0 \subset V$ der von Γ aufgespannte Untervektorraum von V, $\dim V_0 = m$. Da $V_0 = \mathrm{Span}(\Gamma)$, besitzt V_0 eine Basis $\{u_1, \ldots, u_m\}$ von Elementen in Γ. Wir erhalten ein vollständiges Gitter

$$\Gamma_0 = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m \subset \Gamma$$

von V_0.

Behauptung: $|\Gamma/\Gamma_0| < \infty$

Beweis: Sei $\{\gamma_i \in \Gamma\}$ ein Repräsentantensystem für die Nebenklassen in Γ/Γ_0. Sei Φ_0 die Grundmasche von Γ_0. Da Γ_0 in V_0 vollständig ist, ist

$$V_0 = \bigcup_{\gamma \in \Gamma_0} \gamma + \Phi_0.$$

Da außerdem $\Gamma \subset V_0$, ist jedes γ_i von der Form $\gamma_i = \gamma_{0i} + x_i$ mit $\gamma_{0i} \in \Gamma_0$ und $x_i \in \Phi_0$. Ist $\varphi : V \to \mathbb{R}^n$ ein linearer Isomorphismus, dann ist $\varphi(\Phi_0)$ beschränkt. Also enthält Φ_0 nur endlich viele Elemente aus Γ. Da $x_i = \gamma_i - \gamma_{0i} \in \Gamma$, gibt es nur endlich viele x_i dieser Form. Da $x_i \sim \gamma_i \mod \Gamma_0$, ist Γ/Γ_0 endlich.

Ist $|\Gamma/\Gamma_0| = q \in \mathbb{N}$, dann ist $q \cdot \gamma \in \Gamma_0$ für alle $\gamma \in \Gamma$. Es folgt $q \cdot \Gamma \subset \Gamma_0$, also (wir rechnen in $(V,+)$)

$$\Gamma \subset \frac{1}{q} \cdot \Gamma_0 = \mathbb{Z} \cdot \left(\frac{1}{q} \cdot u_1\right) + \ldots + \mathbb{Z} \cdot \left(\frac{1}{q} \cdot u_m\right)$$

Da Untergruppen freier abelscher Gruppen frei sind, hat Γ eine $\mathbb{Z}$-Basis $\{v_1, \ldots, v_r\}$, $r \leq m$, also $\Gamma = \mathbb{Z} \cdot v_1 + \ldots + \mathbb{Z} \cdot v_r$. Da $v_1, \ldots, v_r$ den Vektorraum V_0 aufspannen, folgt $r = m$ und die lineare Unabhängigkeit von $v_1, \ldots, v_r$.

Die umgekehrte Richtung des Satzes ist trivial: Ist Γ ein Gitter mit Basis $\{v_1, \ldots, v_m\}$ in V, dann ergänzen wir $v_1, \ldots, v_m$ zu einer Basis $v_1, \ldots, v_n$ von V. Diese Basis definiert einen linearen Isomorphismus $V \xrightarrow{\varphi} \mathbb{R}^n$, so dass $\varphi(\Gamma)$ nur Punkte mit ganzzahligen Koordinaten enthält. □

14.7 Lemma: Ein Gitter Γ in V ist genau dann vollständig, wenn es einen linearen Isomorphismus $\varphi : V \to \mathbb{R}^n$ und eine Menge $M \subseteq V$ gibt, so dass $\varphi(M)$ beschränkt ist und $V = \bigcup_{\gamma \in \Gamma} \gamma + M$.

14.8 Bemerkung: Sind $\varphi, \psi : V \to \mathbb{R}^n$ und $M \subset V$ wie in 14.7, dann ist auch $\psi(M)$ für jeden anderen linearen Isomorphismus $\psi : V \to \mathbb{R}^n$ beschränkt.

Beweis von 14.7: Sei $\{v_1, \ldots, v_m\}$ Basis von Γ. Wir ergänzen diese zu einer Basis $v_1, \ldots, v_n$ von V, die einen linearen Isomorphismus $\varphi : V \to \mathbb{R}^n$ definiert durch $\varphi(v_i) = e_i$, wobei e_i der i-te Einheitsvektor ist. Ist Γ vollständig, können wir für M das Urbild des Einheitswürfels nehmen, d.h. die abgeschlossene Grundmasche.

Ist umgekehrt Γ nicht vollständig und $\varphi(M)$ beschränkt, dann gibt es ein $k \in \mathbb{N}$, so dass $(x_1, \ldots, x_n) \notin \varphi(M)$ für $x_n \geq k$. Da $\varphi(\Gamma) \subset \mathbb{R}^m \times 0$ mit $m < n$, ist $k \cdot e_n$ nicht im Bild von $\bigcup_{\gamma \in \Gamma} \gamma + M$. Also $\varphi(\bigcup_{\gamma \in \Gamma} \gamma + M) \neq \mathbb{R}^n = \varphi(V)$, d.h. $V \neq \bigcup_{\gamma \in \Gamma} \gamma + M$. □

Sei nun V ein euklidischer Raum, d.h. hier ein $\mathbb{R}$-Vektorraum endlicher Dimension mit einem Skalarprodukt

$$\langle -, - \rangle : V \times V \to \mathbb{R}.$$

Jede Orthonormalbasis $\{e_1, \ldots, e_n\}$ von V definiert eine *Isometrie*

$$\varphi : V \to \mathbb{R}^n$$

mit dem Standardskalarprodukt auf dem $\mathbb{R}^n$. Damit erhalten wir in V einen sinnvollen Volumenbegriff:

(i) der Einheitswürfel bzgl. $\{e_1, \ldots, e_n\}$ in V hat das Volumen 1,

(ii) das von n Vektoren $v_1, \ldots, v_n$ aufgespannte Parallelepiped

$$\Phi := \{x_1 \cdot v_1 + \ldots + x_n \cdot v_n;\ 0 \leq x_i < 1\}$$

hat das Volumen

$$\mathrm{vol}(\Phi) = |\det(\varphi(v_1), \ldots, \varphi(v_n))|.$$

Wie man aus der linearen Algebra weiß, hängt dieser Volumenbegriff nicht von der Wahl der Orthonormalbasis ab. Ist nämlich T die Transformationsmatrix zwischen zwei Orthonormalbasen, dann ist T eine orthogonale Matrix, ihre Determinante also $\det T = \pm 1$.

14.9 Definition: Sei Γ ein vollständiges Gitter in V mit Basis $\{v_1, \ldots, v_n\}$. Wir definieren

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = |\det(\varphi(v_1), \ldots, \varphi(v_n))|.$$

14.10 $\mathrm{vol}(\Gamma)$ ist unabhängig von der Basiswahl, denn ist $\{w_1, \ldots, w_n\}$ eine andere Basis, dann ist die Transformationsmatrix T eine ganzzahlige invertierbare Matrix, also $|\det T| = 1$.

14.11 Definition: Eine Teilmenge X eines $\mathbb{R}$-Vektorraumes V heißt *zentralsymmetrisch*, wenn mit x auch $-x$ in X liegt, und *konvex*, wenn mit $x, y \in X$ auch die Strecke $\{tx + (1-t) \cdot y;\ 0 \leq t \leq 1\}$ in X liegt.

14.12 Gittersatz (Minkowski 1896): Sei Γ ein vollständiges Gitter in einem n-dimensionalen euklidischen Raum V und X eine zentralsymmetrische, konvexe Teilmenge von V. Ist

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma),$$

dann enthält X mindestens einen Punkt $\gamma \neq 0$ aus Γ.

14.13 Bemerkung: Die Wahl einer orthonormalen Basis in V definiert eine Isometrie $\varphi : V \cong \mathbb{R}^n$, wie oben gesehen. Dann definieren wir $\mathrm{vol}(X)$ als das übliche Volumen im $\mathbb{R}^n$ von $\varphi(X)$, wir setzen dabei voraus, dass $\varphi(X)$ Lebesgue-messbar ist. Nach dem Transformationssatz für das Lebesgue-Maß ist $\mathrm{vol}(X)$ von der Wahl der Isometrie unabhängig.

Beweis 14.12: *Behauptung:* Es gibt $\gamma_1 \neq \gamma_2 \in \Gamma$, so dass $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$.
Das genügt. Denn ist z aus diesem Durchschnitt, dann gibt es $x_1, x_2 \in X$ mit

$$z = \frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2.$$

Dann ist $0 \neq \gamma := \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$ ein Gitterpunkt, der Mittelpunkt der Strecke zwischen x_2 und $-x_1$ ist und damit in X liegt.
Angenommen, die Behauptung ist falsch. Dann sind die Mengen $\frac{1}{2}X + \gamma$, $\gamma \in \Gamma$, paarweise disjunkt. Für die Grundmasche Φ folgt dann

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right) \qquad (*)$$

Da das Lebesgue-Maß translationsinvariant ist, gilt für die Translation mit $-\gamma$:

$$\mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right) = \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right)$$

Da Γ ein vollständiges Gitter ist, gilt $V = \bigcup_{\gamma \in \Gamma} \Phi - \gamma$. Also ist $(*)$

$$\begin{aligned} \mathrm{vol}(\Phi) &\geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\Phi \cap \left(\tfrac{1}{2}X + \gamma\right)\right) = \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \tfrac{1}{2}X\right) \\ &\geq \mathrm{vol}((\bigcup_{\gamma \in \Gamma} \Phi - \gamma) \cap \tfrac{1}{2}X) \\ &= \mathrm{vol}(V \cap \tfrac{1}{2}X) = \mathrm{vol}(\tfrac{1}{2}X) = \tfrac{1}{2^n}\,\mathrm{vol}(X) \end{aligned}$$

im Widerspruch zur Voraussetzung. □

Bevor wir mit der Theorie fortfahren, geben wir zwei Anwendungsbeispiele für den Gittersatz.

14.14 Satz: Sei $p > 2$ eine Primzahl. Dann gilt

$$p \text{ ist Summe zweier Quadrate} \iff p \equiv 1 \mod 4.$$

Beweis: „⇒“ Sei $p = a^2 + b^2$. Da 0 und 1 die einzigen Quadrate $\mod 4$ sind, gilt $a^2 + b^2 \equiv 0, 1$ oder 2. Im Falle $p \equiv 0$ oder $2 \mod 4$, wäre aber p gerade. Also muß $p \equiv 1 \mod 4$ sein.

„⇐“ $p = 4k + 1$ für ein $k \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p)^*$ eine zyklische Gruppe der Ordnung $p - 1 = 4k$ nach 4.21. Also gibt es ein $u \in \mathbb{N}$, $0 < u < p$, dessen Restklasse $\overline{u} \mod p$ die multiplikative Ordnung 4 hat. Da $-\overline{1}$ das einzige Element der multiplikativen Ordnung 2 ist (denn $\mathbb{Z}/p$ ist ein Körper), gilt

$$u^2 \equiv -1 \mod p.$$

Sei $\Gamma \subset \mathbb{R} \times \mathbb{R}$ das von $(p, 0)$ und $(u, 1)$ erzeugte Gitter. Die Grundmasche Φ hat das Volumen

$$\mathrm{vol}(\Phi) = \left|\det \begin{pmatrix} p & 0 \\ u & 1 \end{pmatrix}\right| = p, \quad \text{d.h. } \mathrm{vol}(\Gamma) = p.$$

Sei $X \subset \mathbb{R}^2$ der Kreis um $(0, 0)$ mit Radius $r = \sqrt{\frac{3}{2}p}$. Dann gilt

$$\mathrm{vol}(X) = \pi r^2 = \pi \cdot \frac{3}{2}p > 4p = 2^2 \cdot \mathrm{vol}(\Gamma).$$

Nach dem Gittersatz gibt es ein $\gamma \neq 0$ aus $\Gamma \cap X$, $\gamma = \alpha(p, 0) + \beta(u, 1) = (a, b)$ mit $\alpha, \beta \in \mathbb{Z}$. Es folgt

$$0 < a^2 + b^2 \leq \frac{3}{2}p < 2p \quad (\text{da } (a, b) \in X) \qquad (*)$$

$$a^2 + b^2 = (\alpha p + \beta u)^2 + \beta^2 \equiv \beta^2 \cdot u^2 + \beta^2 \equiv -\beta^2 + \beta^2 \equiv 0 \mod p.$$

Also ist $a^2 + b^2$ ein Vielfaches von p. Aus $(*)$ folgt somit $a^2 + b^2 = p$. □

Fermat erwähnte dieses Resultat in einem Brief 1640 an Mersenne und schickte 1659 eine Beweisskizze an Carcavi. Der erste veröffentlichte und vollständige Beweis wird Euler zugeschrieben (1754).

Auch der nächste Satz hat Geschichte. Wieder wurde er von Fermat behauptet, Euler plagte sich 40 Jahre erfolglos mit einem Beweis, der dann 1770 Lagrange gelang.

14.15 Satz: Jedes $x \in \mathbb{N}$ ist Summe von 4 Quadraten.

Beweis: (1) Sind x und y aus $\mathbb{N}$ Summen von 4 Quadraten, dann auch $x \cdot y$.
Beweis: Sei $x = x_1^2 + x_2^2 + x_3^2 + x_4^2$ und $y = y_1^2 + y_2^2 + y_3^2 + y_4^2$. Dann gilt

$$\begin{aligned} x \cdot y &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad +(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_2)^2 \end{aligned}$$

Da $0 = 0^2 + 0^2 + 0^2 + 0^2$ und $2 = 1^2 + 1^2 + 0^2 + 0^2$ genügt es nach (1) den Satz für Primzahlen $p \geq 3$ zu beweisen.

(2) Es gibt $m, n \in \mathbb{Z}$, so dass $m^2 + n^2 + 1 \equiv 0 \mod p$.

Beweis: Da $\mathbb{Z}/p$ ein Körper und $p > 2$ ist, hat die Gleichung $x^2 \equiv a^2 \mod p$ für $a^2 \neq 0$ genau zwei Lösungen, nämlich $\pm\overline{a}$, damit gibt es genau $\frac{p+1}{2}$ verschiedene Quadrate (hier wird 0 mitgezählt), d.h. m^2 kann genau $\frac{p+1}{2}$ verschiedene Werte $\mod p$ annehmen. Dasselbe gilt dann für $-n^2 - 1$. Falls kein m^2-Wert mit dem Wert von $-n^2 - 1$ übereinstimmt ($\mod p$), gibt es $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$ verschiedene Elemente in $\mathbb{Z}/p$, ein Widerspruch.
Sei (m, n) eine Lösung von (2) und $\Gamma \subset \mathbb{R}^4$ das Gitter mit Basis $v_1 = (1, 0, m, -n)$, $v_2 = (0, 1, n, m)$, $v_3 = (0, 0, p, 0)$, $v_4 = (0, 0, 0, p)$. Dann gilt

$$\mathrm{vol}(\Gamma) = \left| \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ m & n & p & 0 \\ -n & m & 0 & p \end{pmatrix} \right| = p^2.$$

Also ist Γ vollständing. Die vierdimensionale Kugel X um 0 mit Radius $r = \sqrt{1,9p}$ hat bekanntlich (?) das Volumen

$$\mathrm{vol}(X) = \frac{\pi^2}{2} r^4 = \frac{\pi^2}{2} \cdot 1,9^2 \cdot p^2 > \frac{9 \cdot 1,9^2}{2} \cdot p^2 = \frac{32,49}{2} \cdot p^2 > 2^4 \cdot p^2 = 2^4 \cdot \mathrm{vol}(\Gamma).$$

Nach dem Gittersatz gibt es also $(a, b, c, d) \neq 0$ aus Γ, so dass $(a, b, c, d) \in X$, also $a^2 + b^2 + c^2 + d^2 < 1,9 \cdot p$.

$$\begin{aligned} (a, b, c, d) \in \Gamma &\iff \exists k, l \in \mathbb{Z} \text{ mit } c = am + bn + kp \text{ und} \\ &\quad d = -a \cdot n + bm + l \cdot p \\ &\iff c \equiv am + bn \mod p \text{ und } d \equiv bm - an \mod p \end{aligned}$$

Also mit (2)

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + a^2m^2 + 2abmn + b^2n^2 + b^2m^2 - 2abmn + a^2n^2 \\ &\equiv a^2(1 + m^2 + n^2) + b^2(1 + n^2 + m^2) \equiv 0 \mod p \end{aligned}$$

Da $0 < a^2 + b^2 + c^2 + d^2 < 2p$, folgt $a^2 + b^2 + c^2 + d^2 = p$. $\square$

15 Minkowski-Theorie

Minkowski-Theorie wird auch die Geometrie der Zahlen genannt. Sei $K/\mathbb{Q}$ eine algebraische Erweiterung vom Grad n und seien

$$\tau_i : K \to \mathbb{C}, \quad i = 1, \ldots, n$$

die n verschiedenen Einbettungen, die nach 8.10 existieren. Wir erhalten eine Abbildung

$$j : K \to K_{\mathbb{C}} := \mathbb{C}^n, \quad x \mapsto (\tau_1(x), \ldots, \tau_n(x)).$$

Die Galois-Gruppe $(\mathbb{C}/\mathbb{R})$ wird durch die komplexe Konjugation erzeugt. Sie operiert auf jedem Faktor $\mathbb{C}$, aber auch auf der Menge $\{\tau_1, \ldots, \tau_n\}$, indem τ_i auf $\overline{\tau}_i \in \{\tau_1, \ldots, \tau_n\}$ abgebildet wird. Es empfiehlt sich daher, die Koordinaten von $K_{\mathbb{C}}$ durch die $\tau \in T = \{\tau_1, \ldots, \tau_n\}$ zu induzieren. Dann definiert die komplexe Konjugation eine Abbildung

$$F : K_{\mathbb{C}} \to K_{\mathbb{C}}, \quad (Fz)_\tau = \overline{z}_{\overline{\tau}}$$

d.h. die τ-te Koordinate von Fz ist das komplex-konjugierte der $\overline{\tau}$-Koordinate von z.

Die übliche hermitesche Form auf $\mathbb{C}^n$ definiert eine hermitesche Form auf $K_{\mathbb{C}}$

$$\langle x, y \rangle = \sum_{\tau \in T} x_\tau \cdot \overline{y}_\tau.$$

Die komplexere Konjugation F erhält das Skalarprodukt, d.h. genauer

15.1 $F\langle x, y \rangle = \langle Fx, Fy \rangle$.

15.2 Wir haben eine lineare *Spurabbildung*

$$Tr : K_{\mathbb{C}} \to \mathbb{C}, \quad Tr(x)_\tau = \sum_{\tau \in T} x_\tau.$$

Nach 8.9 gilt

15.3 Ist $a \in K$, so ist $S_{K/\mathbb{Q}}(a) = Tr(j(a))$.

Uns interessiert der $\mathbb{R}$-Vektorraum $K_{\mathbb{R}}$, der unter der Operation von F punktweise festgelassen wird, d.h.

$$(x_\tau) \in K_{\mathbb{R}} \iff x_{\overline{\tau}} = \overline{x}_\tau.$$

Nach Definiton ist $\overline{\tau}(a) = \overline{\tau(a)}$ für $a \in K$, also bildet j bereits nach $K_{\mathbb{R}}$ ab.

15.4 $j : K \to K_{\mathbb{R}}$.

Schränken wir die hermitesche Form auf $K_{\mathbb{R}}$ ein, erhalten wir ein Skalarprodukt

$$\langle -, - \rangle = K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R},$$

denn für $x, y \in K_{\mathbb{R}}$ gilt

$$\overline{\langle x, y \rangle} = F\langle x, y \rangle = \langle Fx, Fy \rangle = \langle x, y \rangle.$$

15.5 Definition: $K_{\mathbb{R}}$ heißt *Minkowski*-Raum und das Skalarprodukt seine *kanonische Metrik*.

Für die Spurabbildung gilt $F \circ Tr = Tr \circ F$. Also erhalten wir eine $\mathbb{R}$-lineare Spur, für die weiterhin 15.3 gilt

15.6 $Tr : K_{\mathbb{R}} \to \mathbb{R}$.

15.7 Explizite Beschreibung von $K_{\mathbb{R}}$

Von den Einbettungen $\tau : K \to \mathbb{C}$ liegen einige, etwa

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}$$

bereits in $\mathbb{R}$, während andere komplex sind, d.h. nicht nach $\mathbb{R}$ einbetten. Komponiert man letztere mit der komplexen Konjugation, erhält man eine weitere Einbettung, d.h. die komplexen Einbettungen kommen in Paaren

$$\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$$

$n = r + 2s$. Wir erhalten somit

$$K_{\mathbb{R}} = \{(z_\tau)_{\tau \in T} \in \mathbb{C}^n;\ z_\rho \in \mathbb{R},\ z_{\overline{\sigma}} = \overline{z_\sigma}\},$$

d.h. die $z_{\overline{\sigma}}$ sind bereits durch die z_σ bestimmt. Hier steht ρ für die Familie $\{\rho_1, \ldots, \rho_r\}$ und σ für die Familie $\{\sigma_1, \ldots \sigma_s\}$. Wir werden diese Kurzschreibweise auch im Weiteren benutzen. Wir wählen uns aus jedem Paar $\sigma_i, \overline{\sigma}_i$ einen Vertreter und erhalten

15.8 Satz: Die Abbildung

$$f : K_{\mathbb{R}} \to \prod_{\tau \in T} \mathbb{R} = \mathbb{R}^{r+2s}, \quad (z_\tau) \to (x_\tau)$$

mit $x_\rho = z_\rho$, $x_\sigma = \mathrm{Re}(z_\sigma)$, $x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma)$ ist ein $\mathbb{R}$-linearer Isomorphimus. Er überführt die kanonische Metrik in das Skalarprodukt

$$(x, y) = \sum_{\tau \in T} a_\tau \cdot x_\tau \cdot y_\tau \quad \text{mit } a_\tau = \begin{cases} 1 & \tau \text{ reell} \\ 2 & \tau \text{ komplex} \end{cases}$$

Beweis: Die Isomorphie ist nach Konstruktion klar: $K_{\mathbb{R}}$ ist durch die z_ρ und die ausgewählten z_σ festgelegt, f zerlegt diese ausgewählten z_σ in Real- und Imaginärteil.

Sei nun $z_\tau = x_\tau + iy_\tau$, $z'_\tau = x'_\tau + iy'_\tau$ mit x_τ, $y_\tau \in \mathbb{R}$. Dann gilt

$$\langle z, z' \rangle = \sum_\rho z_\rho \cdot \overline{z'}_\rho + \sum_\sigma (z_\sigma \cdot \overline{z'}_\sigma + z_{\overline{\sigma}} \cdot \overline{z'}_{\overline{\sigma}}) = \sum_\rho x_\rho \cdot x'_\rho + 2 \sum_\sigma (x_\sigma \cdot x'_\sigma + x_{\overline{\sigma}} \cdot x'_{\overline{\sigma}})$$

denn

$$\begin{aligned} z_\sigma \cdot \overline{z}'_\sigma + z_{\overline{\sigma}} \cdot \overline{z}'_{\overline{\sigma}} &= z_\sigma \cdot \overline{z}'_\sigma + \overline{z}_\sigma \cdot z'_\sigma = z_\sigma \cdot \overline{z}'_\sigma + \overline{z_\sigma \cdot \overline{z}'_{\overline{\sigma}}} = 2 \cdot \mathrm{Re}(z_\sigma \cdot \overline{z}'_\sigma) \\ &= 2 \cdot (x_\sigma \cdot x'_\sigma + y_\sigma \cdot y'_\sigma) = 2(x_\sigma \cdot x'_\sigma + x_{\overline{\sigma}} \cdot x'_{\overline{\sigma}}) \end{aligned}$$

Damit geht $\langle z, z' \rangle$ in (x, x') über. □

15.9 Vorsicht! Durch f wird auf $\mathbb{R}^{r+2s}$ eine andere als die übliche euklidische Metrik definiert. Damit unterscheidet sich dieses *kanonische* Volumen vom Lebegue-Maß: Für messbare Mengen gilt

$$\mathrm{vol}_{\mathrm{kanon}}(X) = 2^s \cdot \mathrm{vol}_{\mathrm{Lebesgue}}(X).$$

15.10 Satz: Ist $J \neq 0$ ein Ideal von $\mathcal{O}_K$, dann ist das Bild Γ von J unter der Abbildung j aus 15.4 ein vollständiges Gitter in $K_{\mathbb{R}}$ mit

$$\mathrm{vol}(\Gamma) = |\mathcal{O}_K / J| \cdot \sqrt{|\delta_K|}.$$

Wir erinnern daran, dass $\delta_K = \mathrm{disc}(\mathcal{O}_K / \mathbb{Z})$ ist.

Beachte zunächst

15.11 Ist $J \neq 0$ ein Ideal von $\mathcal{O}_K$, dann ist $(J, +)$ eine freie abelsche Gruppe vom Rang $n = [K : \mathbb{Q}]$.

Denn $(J, +) \subset (\mathcal{O}_K, +)$, also ist $(J, +)$ frei vom Rang $\leq$ Rang $\mathcal{O}_K$. Ist $x \neq 0$ aus J, dann definiert

$$\mathcal{O}_K \to J, \quad \alpha \mapsto \alpha \cdot x$$

einen Monomorphismus abelscher Gruppen. Also ist Rang $\mathcal{O}_K \leq$ Rang J.

Beweis 15.10: Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von J, so das

$$\Gamma = \mathbb{Z} \cdot j(\alpha_i) + \ldots + \mathbb{Z} \cdot j(\alpha_n).$$

Seien $\tau_i : K \to \mathbb{C}$, $i = 1, \ldots, n$ wieder die n verschiedenen Einbettungen, und sei $A = (\tau_j(\alpha_i))$. Dann gilt (vergl. 9.5 und 10.9)

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \det(A)^2 = |\mathcal{O}_K / J|^2 \cdot \delta_K$$

und

$$\mathrm{vol}(\Gamma) = |\det(j(\alpha_1), \ldots, j(\alpha_n))| = |\det A| = |\mathcal{O}_K/J| \cdot \sqrt{|\delta_K|}$$

□

Mit dem Gittersatz erhalten wir

15.12 Satz: Sei $J \neq 0$ ein Ideal in $\mathcal{O}_K$ und $T = \{\tau : K \to \mathbb{C}\}$ die Menge der Einbettungen von K in $\mathbb{C}$. Weiter seien $c_\tau > 0$ aus $\mathbb{R}$, $\tau \in T$, so dass $c_\tau = c_{\overline{\tau}}$ und $\prod_{\tau \in T} c_\tau > A \cdot |\mathcal{O}_K/J|$, wobei

$$A = \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|} \qquad s = \text{ Anzahl der komplexen } \tau.$$

Dann gibt es ein $a \in J$, $a \neq 0$, so dass $|\tau(a)| < c_\tau \ \forall \tau \in T$.

Beweis: $X = \{(z_\tau) \in K_{\mathbb{R}};\ |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Wir ermitteln das (kanonische) Volumen von X mit Hilfe der Abbildung f aus 15.8 und der durch f induzierten Metrik auf $\mathbb{R}^{r+2s}$:

$$f(X) = \{(x_\tau) \in \prod_{\tau \in T} \mathbb{R};\quad |x_\rho| < c_\rho,\ x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\}$$

Es folgt

$$\mathrm{vol}(X) = 2^s \cdot \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)) = 2^s \cdot \prod_\rho (2c_\rho) \cdot \prod_\sigma (\pi c_\sigma^2) = 2^{r+s} \cdot \pi^s \cdot \prod_{\tau \in T} c_\tau$$

(Hier schreiben wir $c_\sigma^2 = c_\sigma \cdot c_{\overline{\sigma}}$). Es folgt nach Voraussetzung

$$\mathrm{vol}(X) > 2^{r+s} \cdot \pi^s \cdot \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|} \cdot |\mathcal{O}_K/J| = 2^n \cdot \mathrm{vol}(\Gamma).$$

Nach dem Gittersatz gibt es ein $a \in J$, $a \neq 0$, so dass $j(a) \in X$. Nach Definition von X und j folgt

$$|\tau(a)| < c_\tau.$$

□

15.13 Multiplikative Minkowski-Theorie

Statt $(K, +)$ betrachten wir $(K^*, \cdot)$. Die Abbildung j ist auch multiplikativ, wir haben einen Monomorphismus

$$j : K^* \to K_{\mathbb{C}}^* := \prod_{\tau \in T} \mathbb{C}^*.$$

Jetzt wird die Spur durch die **Norm** ersetzt:

15.14 $N : K_{\mathbb{C}}^* \to \mathbb{C}^*, \quad (z_\tau)_{\tau\in T} \mapsto \prod_{\tau\in T} z_\tau.$

Es folgt

15.15 Für $a \in K^*$ gilt $N_{K/\mathbb{Q}}(a) = N(j(a))$.

Um Gittertheorie auch im multiplikativen Fall zu nutzen, müssen wir zu additiven Gruppen übergehen. Bekanntlich wird das durch den Logarithmus bewerkstelligt. Sei also

$$l : \mathbb{C}^* \to \mathbb{R}, \quad z \mapsto \log|z|.$$

Dann definiert l einen surjektiven Homomorphismus

$$l : K_{\mathbb{C}}^* \to \prod_{\tau\in T} \mathbb{R},$$

so dass

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \Pi_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \hookrightarrow & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R} \end{array}$$

kommutiert. Wieder haben wir eine Operation durch die komplexe Konjugation F auf diesen Gruppen, und zwar die triviale auf K^* und die auf $K_{\mathbb{C}}^*$ wie zuvor. Auf $\Pi_\tau\mathbb{R}$ ist sie durch Koordinatenvertauschung gegeben

$$(FX)_\tau = x_{\overline{\tau}}.$$

Wir erhalten analog zu additiven Teil

15.16 $F \circ j = j, \quad F \circ l = l \circ F, \quad N \circ F = F \circ N, \quad Tr \circ F = Tr.$

Damit erhalten die Abbildungen im Diagramm die Operation von F. Gehen wir zu den Fixpunktmengen unter dieser Operation über, erhalten wir ein kommutatives Diagramm

15.17

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\Pi_{\tau\in T}\mathbb{R}]^+ \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \hookrightarrow & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array}$$

15.18 Explizite Beschreibung von $[\Pi_{\tau\in T}\mathbb{R}]^+$:
Mit den Bezeichnungen aus 15.7 gilt

$$[\Pi_{\tau\in T}\mathbb{R}]^+ = \prod_{\rho}\mathbb{R}\times\prod_{\sigma}[\mathbb{R}\times\mathbb{R}]^+.$$

Der Faktor $[\mathbb{R}\times\mathbb{R}]^+$ ist die Fixpunktmenge unter der Koordinatenvertauschung, d.h. $[\mathbb{R}\times\mathbb{R}]^+ = \{(x,x); x\in\mathbb{R}\}$. Um mit den $2s$ komplexen Einbettungen kompatibel zu bleiben, identifizieren wir

$$[\mathbb{R}\times\mathbb{R}]^+ \cong \mathbb{R}, \quad (x,x)\mapsto 2x \quad !$$

Wir erhalten einen Isomorphismus

$$f^* : \left[\prod_{\tau\in T}\mathbb{R}\right]^+ \cong \mathbb{R}^{r+s}.$$

Weil wir den Faktor 2 für die komplexen Einbettungen eingeführt haben, geht

$$Tr : \left[\prod_{\tau\in T}\mathbb{R}\right]^+ \to \mathbb{R} \quad \text{in} \quad Tr : \mathbb{R}^{r+s}\to\mathbb{R},$$

die Koordinatensumme, über.

Sind $\rho_1,\dots,\rho_r$ die reellen, $\sigma_1,\overline{\sigma}_1,\dots,\sigma_s,\overline{\sigma}_s$ die komplexen Einbettungen, dann gilt

15.19 $f^*([(x_\tau)]) = (x_{\rho_1},\dots,x_{\rho_r},2x_{\sigma_1},\dots,2x_{\sigma_s})$

$f^*\circ l : K_{\mathbb{R}}^* \to \mathbb{R}^{r+s}, \quad (x_\tau)\longmapsto(\log|x_{\rho_1}|,\dots,\log|x_{\rho_r}|,\log|x_{\sigma_1}|^2,\dots,\log|x_{\sigma_s}|^2).$

16 Die Klassenzahl

Ziel dieses Abschnitts ist es zu zeigen, dass die Idealklassengruppe $\mathcal{C}l_K$ eines algebraischen Zahlkörpers endlich ist.

16.1 Definition: Sei $0\neq J\subset\mathcal{O}_K$ ein Ideal. Dann definieren wir die *Absolutnorm* $\mathfrak{N}(J)$ von J durch

$$\mathfrak{N}(J) = |\mathcal{O}_K/J| \in \mathbb{N}.$$

Beachte: Nach 10.9 ist $\mathfrak{N}(J)$ endlich!
Diese Norm wird uns helfen, Ideale zu zählen.

16.2 Ist $\alpha \in \mathcal{O}_K$ und (α) das von α erzeugte Hauptideal, dann gilt

$$|N_{K/\mathbb{Q}}(\alpha)| = \mathfrak{N}(\alpha).$$

Denn ist $\beta_1, \ldots, \beta_n$ eine ganze Basis, d.h. $\mathcal{O}_K = \mathbb{Z} \cdot \beta_1 + \ldots + \mathbb{Z} \cdot \beta_n$. Dann ist $(\alpha) = \mathcal{O}_K \cdot \alpha = \mathbb{Z} \cdot \beta_1\alpha + \ldots + \mathbb{Z} \cdot \beta_n\alpha$. Also ist $\beta_1\alpha + \ldots + \beta_n\alpha$ $\mathbb{Z}$-Basis von (α). Sei A die Übergangsmatrix von $\{\beta_1, \ldots, \beta_n\}$ nach $\{\alpha\beta_1, \ldots, \alpha\beta_n\}$, d.h.

$$\alpha \cdot \beta_i = \sum a_{ij}\beta_j,$$

dann gilt, wie in 10.9 gezeigt, $|\det A| = |\mathcal{O}_K/(\alpha)|$. Anderseits gilt nach Definition 8.2

$$N_{K/\mathbb{Q}}(\alpha) = \det A.$$

16.3 Satz: $\mathfrak{N}$ ist multiplikativ: Sind $J_1 \neq 0$ und $J_2 \neq 0$ Ideale in $\mathcal{O}_K$, dann gilt

$$\mathfrak{N}(J_1 \cdot J_2) = \mathfrak{N}(J_1) \cdot \mathfrak{N}(J_2).$$

Beweis: Sei $J = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r}$ die Primidealfaktorisierung des Ideals $J \neq 0$ aus $\mathcal{O}_K$. Es genügt zu zeigen, dass

$$\mathfrak{N}(J) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdot \ldots \cdot \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}.$$

Nun sind $\mathfrak{p}_i^{\nu_i}$ und $\mathfrak{p}_j^{\nu_j}$ coprim. Es folgt

$$\mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r} = \bigcap_{j=1}^{r} \mathfrak{p}_j^{\nu_j}.$$

Wir können den chinesischen Restesatz anwenden und erhalten

$$\mathcal{O}_K/J \cong \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \times \ldots \times \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}$$

und damit

$$\mathfrak{N}(J) = \mathfrak{N}(\mathfrak{p}_1^{\nu_1}) \cdot \ldots \cdot \mathfrak{N}(\mathfrak{p}_r^{\nu_r}).$$

Sei nun $\mathfrak{p}$ ein Primideal. In der Kette

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \ldots \supset \mathfrak{p}^r$$

ist $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ wegen der eindeutigen Primidealzerlegung. Da $\mathfrak{p} \subset \mathcal{O}_K$ maximal ist, ist $\mathcal{O}_K/\mathfrak{p}$ ein Körper, und

$$\mathcal{O}_K/\mathfrak{p} \times \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}, \quad \overline{r} \cdot \overline{x} = \overline{r \cdot x}$$

macht $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ zum $\mathcal{O}_K/\mathfrak{p}$-Vektorraum. Diese Skalarmultiplikation ist wohldefiniert, denn

$$(r+\mathfrak{p})\cdot(x+\mathfrak{p}^{i+1}) = r\cdot x + \mathfrak{p}\cdot x + r\mathfrak{p}^{i+1} + \mathfrak{p}^{i+2} \subset r\cdot x + \mathfrak{p}^{i+1},$$

weil $x\cdot\mathfrak{p} \in \mathfrak{p}^{i+1}$ für $x \in \mathfrak{p}^i$.
Die $(\mathcal{O}_K/\mathfrak{p})$-Dimension von $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist 1: Jedes $a \in \mathfrak{p}^i\backslash\mathfrak{p}^{i+1}$ erzeugt den Vektorraum, denn

$$\mathfrak{p}^{i+1} \subsetneqq \mathcal{O}_K\cdot a + \mathfrak{p}^{i+1} \subset \mathfrak{p}^i,$$

so dass $\mathfrak{p}^i = \mathcal{O}_K\cdot a + \mathfrak{p}^{i+1}$ wegen der eindeutigen Primzerlegung (ist I das Ideal in der Mitte, so gilt $\mathfrak{p}^i|I$ und $I|\mathfrak{p}^{i+1}$). Es folgt

$$\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}.$$

Wir erhalten $\mathfrak{N}(\mathfrak{p}^r) = |\mathcal{O}_K/\mathfrak{p}^r| = |\mathcal{O}_K/\mathfrak{p}^1|\cdot|\mathfrak{p}/\mathfrak{p}^2|\cdot\ldots\cdot|\mathfrak{p}^{r-1}/\mathfrak{p}^r| = \mathfrak{N}(\mathfrak{p})^r$. □
Aus 13.4 folgt sofort, dass die abelsche Gruppe $\mathcal{J}_K$ aller gebrochenen Ideale die Gruppenkompletierung des Monoids der ganzen Ideale $\neq 0$ ist. Damit erweitert der Homomorphismus $\mathfrak{N}$ zu einem Gruppenhomomorphismus

16.4 $\mathfrak{N} : \mathcal{J}_K \to (\mathbb{Q}_+^*, \cdot)$.

16.5 Lemma: Jedes Ideal $J \neq 0$ in $\mathcal{O}_K$ enthält ein Element $a \neq 0$, so dass

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}\cdot\mathfrak{N}(J).$$

Beweis: Zu $\varepsilon > 0$ wählen wir positive reelle Zahlen $c_\tau > 0$, $\tau \in T = \{\tau : K \to \mathbb{C}\}$, so dass $c_\tau = c_{\overline{\tau}}$ und $\Pi_{\tau\in T} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}\cdot\mathfrak{N}(J) + \varepsilon$. Nach 15.12 gibt es ein $a \neq 0$ in J, so dass $|\tau(a)| < c_\tau\ \forall\tau \in T$. Es folgt

$$|N_{K/\mathbb{Q}}(a)| = |\Pi_{\tau\in T}\tau(a)| < \Pi_{\tau\in T} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}\cdot\mathfrak{N}(J) + \varepsilon.$$

Da es zu jedem $\varepsilon > 0$ ein solches a gibt und $|N_{K/\mathbb{Q}}(a)|$ eine natürliche Zahl ist, gibt es ein $a \neq 0$ in J mit

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}\cdot\mathfrak{N}(J).$$

□

16.6 Definition und Satz: Die Idealklassengruppe $\mathcal{C}l_K = \mathcal{J}_K/\mathcal{H}_K$ ist endlich. Ihre Ordnung $h_K = |\mathcal{C}l_K|$ heißt *Klassenzahl* von K.

Beweis: Sei $\mathfrak{p} \neq 0$ ein Primideal in $\mathcal{O}_K$, dann gibt es nach 12.7 eine Primzahl $p \in \mathbb{N}$, so dass $\mathfrak{p} \cap \mathbb{Z} = p \cdot \mathbb{Z}$. Da $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und $F = \mathcal{O}_K/\mathfrak{p}$ Körper sind, ist $\mathbb{F}_p \subset F$ eine endliche Erweiterung vom Grad n (beachte: $\mathcal{O}_K$ hat eine endliche $\mathbb{Z}$-Basis, also ist $\mathbb{F}_p \subset F$ endlich). Es folgt

$$\mathfrak{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathbb{F}_p^n| = p^n. \qquad (*)$$

Zu festen $p \in \mathbb{N}$ gibt es nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p$, da $(p) \subset \mathfrak{p}$, also $\mathfrak{p}|p$, und p eindeutig in Primideale zerlegbar ist. Also gibt es zu einer vorgegebenen Schranke $N \in \mathbb{R}_+$ nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{N}(\mathfrak{p}) \leq N$ wegen $(*)$. Ist nun $J \neq 0$ ein Ideal, $J = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r}$, dann ist

$$\mathfrak{N}(J) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdot \ldots \cdot \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}.$$

Also gibt es nur endlich viele Ideale J in $\mathcal{O}_K$ mit $\mathfrak{N}(J) \leq N$. Es genügt daher, ein $N \in \mathbb{R}_+$ zu finden, so dass in jeder Nebenklasse $[J] \in \mathcal{C}l_K$ ein ganzes Ideal J liegt mit $\mathfrak{N}(J) \leq N$.

Wir setzen $N = \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}$. Sei nun $[M]$ eine Nebenklasse in $\mathcal{C}l_K$ mit einem gebrochenen Ideal M. Dann ist auch M^{-1} ein gebrochenes Ideal. Nach 13.2 gibt es ein $r \in \mathcal{O}_K$, $r \neq 0$, so dass $J := r \cdot M^{-1} \in \mathcal{O}_K$.

Nach 16.5 gibt es ein $a \neq 0$ in J, so dass

$$|N_{K/\mathbb{Q}}(a)| \leq N \cdot \mathfrak{N}(J).$$

Es folgt: $\mathfrak{N}(a \cdot J^{-1}) = \mathfrak{N}((a) \cdot J^{-1}) = \mathfrak{N}((a)) \cdot \mathfrak{N}(J^{-1}) = |N_{K/\mathbb{Q}}(a)| \cdot \mathfrak{N}(J)^{-1} \leq N$.

Da $J^{-1} = \{x \in K; x \cdot J \subset \mathcal{O}_K\}$ und $a \in J$, folgt $a \cdot J^{-1} \subset \mathcal{O}_K$, d.h. $a \cdot J^{-1}$ ist ganz.

Da $a \cdot J^{-1} = a \cdot r^{-1} \cdot M$, unterscheidet sich das ganze Ideal $a \cdot J^{-1}$ vom gebrochenen Ideal M nur um das gebrochene Hauptideal $\left(\frac{a}{r}\right)$, d.h. $a \cdot J^{-1}$ ist in der Nebenklasse von M. □

16.7 Bemerkung: Im Beweis von 16.6 haben wir erheblich mehr gezeigt: Jede Nebenklasse in $\mathcal{C}l_K$ hat als Repräsentanten ein ganzes Ideal J, so dass

$$\mathfrak{N}(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}.$$

16.8 Bemerkung: Rechnet man etwas sorgfältiger, läßt sich 16.7 verbessern: Jede Nebenklasse in $\mathcal{C}l_K$ enthält ein ganzes Ideal J mit

$$\mathfrak{N}(J) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\delta_K|} =: M.$$

Die Zahl M heißt *Minkowski'sche Zahl.*

16.9 Beispiel: $K = \mathbb{Q}[i]$. Da $\mathcal{O}_K = \mathbb{Z}[i]$ ein Hauptidealring ist, folgt $h_K = 1$. Das erhalten wir auch aus 16.7: $\delta_K = -4$ nach 10.12 und $s = 1$. Also

$$N = \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|} = \frac{4}{\pi} < 2.$$

Damit werden die Nebenklassen in $\mathcal{C}l_K$ durch ganze Ideale mit Absolutnorm 1 repräsentiert. Es gibt aber nur eines, nämlich $\mathcal{O}_K$. Also ist $h_K = 1$. □

16.10 Lemma: Sei $J \neq 0$ ein Ideal in $\mathcal{O}_K$. Dann gilt

(1) $\mathfrak{N}(J) = 1 \iff J = \mathcal{O}_K$.

(2) $\mathfrak{N}(J)$ prim $\Rightarrow J$ ist Primideal.

(3) $\mathfrak{N}(J) \in J \cap \mathbb{Z}$, insbesondere gilt $\mathfrak{N}(J) \in J$, also $J|\mathfrak{N}(J)$ in $\mathcal{O}_K$.

Beweis: (1) Ist J nicht prim und $J \neq \mathcal{O}_K$, dann ist es Produkt von mehreren Primidealen. Also kann $\mathfrak{N}(J)$ nicht prim sein.
(2) Da $\mathfrak{N}(J) = |\mathcal{O}_K/J|$, gilt für jede Restklasse $\overline{x} \in \mathcal{O}_K/J$ mit $x \in \mathcal{O}_K$, dass $\mathfrak{N}(J) \cdot \overline{x} = \overline{0}$ und damit $\mathfrak{N}(J) \cdot x \in J$. Für $x = 1$ folgt $\mathfrak{N}(J) \in J$. □

16.11 Beispiel: $K = \mathbb{Q}[\sqrt{-5}]$. Wir wissen, dass $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring ist, so dass $h_K \geq 2$. Hier gilt $\delta_K = -20$ nach 10.12 und $s = 1$. Also

$$\left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|} = \frac{2}{\pi} \cdot \sqrt{20} < \frac{2}{\pi}\sqrt{\frac{81}{4}} = \frac{9}{\pi} < 3.$$

Neben dem durch $\mathcal{O}_K$ mit $\mathfrak{N}(\mathcal{O}_K) = 1$ repräsentierten neutralen Element muss es also Klassen geben, die durch Ideale J mit $\mathfrak{N}(J) = 2$ repräsentiert werden. Nach 16.10 ist J prim und $J|2$.

Wir suchen daher nach der Primfaktorisierung des Hauptideals (2).

Behauptung: $(2) = \mathfrak{p}^2$, wobei $\mathfrak{p} = (2, 1 + \sqrt{-5})$.

Beweis: $\mathfrak{p} = \mathcal{O}_K \cdot 2 + \mathcal{O}_K \cdot (1 + \sqrt{-5})$. Da $\{1, 1 - \sqrt{-5}\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ ist, erhalten wir

$$\begin{aligned} \mathfrak{p} &= (\mathbb{Z} + \mathbb{Z} \cdot (1 - \sqrt{-5})) \cdot 2 + (\mathbb{Z} + \mathbb{Z} \cdot (1 - \sqrt{-5}))(1 + \sqrt{+5}) \\ &= \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot 2 \cdot (1 - \sqrt{-5}) + \mathbb{Z}(1 + \sqrt{-5}) + \mathbb{Z} \cdot 6 \end{aligned}$$

Da $\mathbb{Z} \cdot 6 \subset \mathbb{Z} \cdot 2$, besteht $\mathfrak{p}$ aus allen Elementen der Form

$$\begin{aligned} z &= 2a + 2b(1 - \sqrt{-5}) + c \cdot (1 + \sqrt{+5}) \qquad a, b, c \in \mathbb{Z} \text{ beliebig} \\ &= x \cdot 1 + y \cdot (1 - \sqrt{-5}) \in \mathbb{Z} + \mathbb{Z} \cdot (1 - \sqrt{-5}) = \mathcal{O}_K. \end{aligned}$$

Wir ermitteln x und y:

$$x + y = 2a + 2b + c \qquad\qquad - y = -2b + c.$$

Es folgt $x = 2(a + c)$, $y = 2b - c$, wobei $a, b, c \in \mathbb{Z}$ beliebig sind.
Also ist $\{2, 1 - \sqrt{-5}\}$ eine $\mathbb{Z}$-Basis von $\mathfrak{p}$ und somit

$$\mathfrak{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = 2.$$

Da $2^2 \in (2)$, $(1 - \sqrt{-5}) \cdot 2 \in (2) = \mathcal{O}_K \cdot 2$, und $(1 - \sqrt{-5})^2 = (-4 - 2\sqrt{5}) = (-2 - \sqrt{5}) \cdot 2 \in (2)$,ist $\mathfrak{p}^2 \subset (2)$. Da weiterhin $\mathfrak{N}((2)) = N_{K/\mathbb{Q}}(2) = 4$, folgt

$$\mathfrak{p}^2 = (2).$$

Da (2) ein Hauptideal ist, repräsentiert (2) das neutrale Element. Wir erhalten

$$\mathcal{C}l_{\mathbb{Q}[\sqrt{-5}]} \cong \mathbb{Z}/2, \text{ erzeugt von } \mathfrak{p} = (2, 1 + \sqrt{-5}).$$

□

Im nächten Kapitel werden wir Methoden kennen lernen, die uns 16.11 einfacher beweisen lassen.

Die Klassenzahl misst, was man beim Übergang von Zahlen zu Idealen an Information "verliert". Im günstigsten Fall hat man $h_K = 1$ und damit die eindeutige Primzerlegung auf Zahlenniveau. In den meisten Fällen ist aber $h_K > 1$.

16.12 Historische Bemerkungen: Für imaginär quadratische Zahlkörper $\mathbb{Q}(\sqrt{m})$, $m < 0$ quadratfrei, gilt

$$h_K = 1 \iff m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Für reell-quadratische Zahlkörper gibt es keine entsprechende Klassifikation.

Vermutung: Es gibt unendlich viele reell-quadratische Zahlkörper K mit $h_K = 1$. Es gibt unendlich viele Zahlkörper K mit $h_K = 1$.

Im Zusammenhang mit Fermat's letztem Satz hat die Klassenzahl von Kreisteilungskörpern, die wir im Abschnitt 21 behandeln werden, eine große Bedeutung. Ist $p > 2$ prim, so untersucht man die Lösbarkeit von

$$x^p + y^p = z^p.$$

Ist ζ eine primitive p-te Einheitswurzel, dann gilt in $\mathbb{Z}[\zeta]$

$$y^p = z^p - x^p = (z - x) \cdot (z - \zeta x) \cdot \ldots \cdot (z - \zeta^{p-1} x).$$

Falls $\mathbb{Z}[\zeta]$ faktoriell ist, erhält man zwei verschiedene Faktorisierungen in Primelemente und damit einen Widerspruch. Das war die Grundlage von Lamé's "Beweis" von 1847, der fälschlich annahm, dass $\mathbb{Z}[\zeta]$ ein Hauptidealring ist.

Kummer (1850) machte diesen Fehler nicht und konnte Fermat's letzten Satz für *reguläre Primzahlen* zeigen, d.h. für solche p, für die $p \nmid h_K$, wobei K der Kreisteilungskörper $\mathbb{Q}(\zeta)$, ζ eine p-te primitive Einheitswurzel, ist.

Kummer zeigte auch, dass 37, 59, 67, 101, 103, 131, 149, 157 die einzigen irregulären Primzahlen < 164 sind. Noch wenige Jahre vorher hatte Lamé mit größter Mühe den Fall $p = 7$ gelöst.

17 Der Einheitensatz

In diesem Abschnitt wollen wir die Einheitengruppe $\mathcal{O}_K^*$ von $\mathcal{O}_K$ bestimmen. Wir verwenden dazu die multiplikative Minkowski-Theorie und erinnern an das Diagramm 15.17

$$\begin{array}{ccccc} K^* & \xrightarrow{\ j\ } & K_{\mathbb{R}}^* & \xrightarrow{\ l\ } & [\Pi_{\tau\in T}\mathbb{R}]^+ \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \hookrightarrow & \mathbb{R}^* & \xrightarrow{\ l=log|\ |\ } & \mathbb{R} \end{array}$$

Wir spezifizieren Untergruppen der oberen Reihe

$$\begin{array}{rcll} \mathcal{O}_K^* & = & \{\varepsilon \in \mathcal{O}_K;\ N_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}, & \text{die Einheitengruppe} \\ S & = & \{y \in K_{\mathbb{R}}^*;\ N(y) = \pm 1\}, & \text{die } \textit{Norm-Eins-Fläche} \\ H & = & \{x \in [\Pi_\tau \mathbb{R}]^+;\ Tr(x) = 0\}, & \text{die } \textit{Spur-Null-Hyperebene}. \end{array}$$

Wir erhalten eine Homomorphismus

$$\lambda : \mathcal{O}_K^* \xrightarrow{\ j\ } S \xrightarrow{\ l\ } H,$$

dessen Bild wir mit Γ bezeichnen, also $\Gamma = \lambda(\mathcal{O}_K^*) \subset H$.

17.1 Satz: Ist $\mu(K) \subset \mathcal{O}_K^*$ die Gruppe der Einheitswurzeln in K, dann ist die Sequenz

$$1 \longrightarrow \mu(K) \hookrightarrow \mathcal{O}_K^* \xrightarrow{\ \lambda\ } \Gamma \longrightarrow 0$$

exakt.

Beweis: Es ist nur zu zeigen, dass $\mu(K)$ der Kern der Abbildung λ ist. Sei $\zeta \in \mu(K)$ eine Einheitswurzel und sei $\tau : K \to \mathbb{C}$ aus T. Dann ist $\tau(\zeta) \in \mathbb{C}$ eine Einheitswuzel, also $|\tau(\zeta)| = 1$ und damit $\log|\tau(\varepsilon)| = 0$. Also liegt ζ im Kern von λ.

Ist umgekehrt $\varepsilon \in \mathcal{O}_K^*$ im Kern von λ, gilt $l(j(\varepsilon)) = 0$, d.h.$|\tau(\varepsilon)| = 1$ für alle $\tau \in T$. Es folgt $j(\operatorname{Kern}\lambda) \subset K_{\mathbb{R}}^*$ ist beschränkt. Nach 15.10 ist aber $j(\mathcal{O}_K)$ ein vollständiges Gitter in $K_{\mathbb{R}}$. Daher kann $\operatorname{Kern}\lambda$ nur endlich viele Elemente enthalten. Die Behauptung folgt also aus $\square$

17.2 Lemma: Hat $\varepsilon \in \mathcal{O}_K^*$ endliche Ordnung, liegt ε in $\mu(K)$.

Denn ist $\operatorname{ord}\varepsilon = n$, so gilt $\varepsilon^n = 1$, d.h. ε ist n-te Einheitswurzel. $\square$

Wir wollen uns jetzt mit Γ beschäftigen.

17.3 Lemma: Sei $a \in \mathbb{Z}$. Dann gibt es bis auf Assoziierte nur endliche viele $\alpha \in \mathcal{O}_K$ mit $N_{K/\mathbb{Q}}(\alpha) = a$.

Beweis: Sei $a > 0$. Da $a \cdot \mathcal{O}_K \subset \mathcal{O}_K$ ein Ideal ist, ist $|\mathcal{O}_K / a \cdot \mathcal{O}_K|$ endlich. In jeder dieser endlich vielen Nebenklassen gibt es bis auf Assoziierte höchstens ein $\alpha \in \mathcal{O}_K$ mit $|N_{K/\mathbb{Q}}(\alpha)| = |a|$. Denn ist $\beta = \alpha + a \cdot \gamma$ ein weiteres solches Element mit $\gamma \in \mathcal{O}_K$, dann gilt $a = \pm N_{K/\mathbb{Q}}(\beta) = \mathfrak{N}((\beta))$. Nach 16.10.2 ist $a = \mathfrak{N}(\beta) \in (\beta)$, d.h. β teilt a in $\mathcal{O}_K$. Es folgt $a = \beta \cdot b$ und somit

$$\alpha = \beta(1 - b \cdot \gamma) \quad \text{d.h. } \alpha \in (\beta).$$

Analog folgt $\beta \in (\alpha)$, d.h. α und β sind assoziiert.

Es gibt also bis auf Assoziierte höchstens $|\mathcal{O}_K / a \cdot \mathcal{O}_K|$ Elemente mit Norm $\pm a$. $\square$

17.4 Satz: Die Gruppe Γ ist ein vollständiges Gitter im $(r + s - 1)$-dimensionalen $\mathbb{R}$-Vektorraum H. Insbesondere ist $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Beweis: Wir zeigen zunächst, dass Γ eine diskrete Untergruppe von $(H, +)$ und damit nach 14.6 ein Gitter ist. $\lambda : \mathcal{O}_K^* \to H$ ist die Einschränkung der Abbildung

$$K^* \xrightarrow{j} \prod_{\tau \in T} \mathbb{C}^* \xrightarrow{l} \prod_{\tau \in T} \mathbb{R}.$$

Es genügt daher zu zeigen, dass $Y_c = \{(x_\tau) \in \prod_\tau \mathbb{R};\ |x_\tau| \le c\} \subset \prod_\tau \mathbb{R}$ für jedes $c > 0$ nur endlich viele Punkte von $\Gamma = l \circ j(\mathcal{O}_K^*)$ enthält.

$$l^{-1}(Y_c) = \{(z_\tau) \in \prod_{\tau \in T} \mathbb{C}^*;\ e^{-c} \le |z_\tau| \le e^c\}$$

(zur Erinnerung: $l((z_\tau)) = (\log|z_\tau|)$). Da $l^{-1}(Y_c)$ ein beschränkter Bereich und $j(\mathcal{O}_K)$ in $K_\mathbb{R}$ ein Gitter ist, kann $j(\mathcal{O}_K^*) \cap l^{-1}(Y_c)$ für jedes $c > 0$ nur endlich viele Elemente haben.

Der Hauptteil des Beweises beschäftigt sich mit der Vollständigkeit von Γ. Nach 14.7 brauchen wir dafür eine beschränkte Menge $M \subset H$, so dass

$$H = \bigcup_{\gamma\in\Gamma} M + \gamma.$$

Dazu konstruieren wir in der Norm-Eins-Fläche S eine beschränkte Menge Q deren **multiplikative** Verschiebungen S überdecken:

$$S = \bigcup_{\varepsilon\in\mathcal{O}_K^*} Q \cdot j(\varepsilon).$$

Da $l : S \to H$ surjektiv ist, ist $l(Q)$ das gesuchte M.

Wir wählen reelle Zahlen $c_\tau > 0$, $\tau \in T$, so dass $c_\tau = c_{\overline{\tau}}$ und

$$C = \prod_{\tau\in T} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}.$$

Sei nun

$$X = \{(z_\tau) \in K_\mathbb{R}; \quad |z_\tau| < c_\tau \ \forall\tau \in T\}.$$

Für $y = (y_\tau) \in S$ ist dann (komponentenweise Multiplikation)

$$X \cdot y = \{(z_\tau) \in K_\mathbb{R};\ |z_\tau| < c'_\tau \ \forall\tau \in T\}$$

mit $c'_\tau = c_\tau \cdot |y_\tau|$, d.h. y "streckt" die Menge X. Weiter gilt $c'_\tau = c'_{\overline{\tau}}$ und $\prod_\tau c'_\tau = \prod_\tau c_\tau = C$, denn

$$\prod_\tau |y_\tau| = |\prod_\tau y_\tau| = |N(y)| = 1 \quad \text{für } y \in S.$$

Nach 15.12 gibt es ein $a \neq 0$ in $\mathcal{O}_K$, so dass $|\tau(a)| < c'_\tau \ \forall\tau \in T$, d.h.

$$j(a) = (\tau(a))_{\tau\in T} \in X \cdot y.$$

Nach 17.3 haben wir endlich viele Elemente $\alpha_1, \ldots, \alpha_N$ in $\mathcal{O}_K$, $\alpha_i \neq 0$, so dass jedes $a \neq 0$ aus $\mathcal{O}_K$ mit $|N_{K/\mathbb{Q}}(a)| \leq C$ zu einer dieser Zahlen assoziiert ist, denn diese Normen sind in $\mathbb{Z}$, so dass es nur endlich viele Werte vom Betrag $\leq C$ gibt. Wir setzen

$$Q = S \cap \bigcup_{i=1}^{N} X \cdot j(\alpha_i^{-1}).$$

Da X beschränkt ist, ist auch $X \cdot j(\alpha_i^{-1})$ beschränkt und damit auch Q. Weiter gilt

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Q \cdot j(\varepsilon).$$

Denn ist $y \in S$, dann ist auch $y^{-1} \in S$ (komponentenweises Invertieren). Also gibt es ein $a \neq 0$ in $\mathcal{O}_K$ mit $j(a) \in X \cdot y^{-1}$, d.h. $j(a) = x \cdot y^{-1}$ für ein $x \in X$. Da

$$|N_{K/\mathbb{Q}}(a)| = |N(j(a))| = |N(x)| \cdot |N(y^{-1})| = N(x) < \Pi_{\tau \in T} c_\tau = C,$$

ist a zu einem α_i assoziiert, d.h. $\alpha_i = \varepsilon \cdot a$ mit $\varepsilon \in \mathcal{O}_K^*$. Es folgt

$$y = x \cdot j(a)^{-1} = x \cdot j(a^{-1}) = x \cdot j(\alpha_i^{-1} \cdot \varepsilon), \quad x \cdot j(\alpha_i^{-1}) = y \cdot j(\varepsilon^{-1}).$$

Da $\varepsilon^{-1} \in \mathcal{O}_K^*$, ist $j(\varepsilon^{-1}) \in S$. Also ist $x \cdot j(\alpha_i^{-1}) \in S \cap (X \cdot j(\alpha_i^{-1})) \subset Q$ und $y \in Q \cdot j(\varepsilon)$. □

Da Γ eine freie abelsche Gruppe ist, "spaltet" die exakte Sequenz 17.1 und wir erhalten

17.5 Dirichlet'scher Einheitensatz: Für die Einheitengruppe $\mathcal{O}_K^*$ gilt

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}.$$

17.6 Definition: Ein *Fundamentalsystem* von Einheiten ist eine Teilmenge $\{\mu_1, \ldots, \mu_{r+s-1}\} \subset \mathcal{O}_K^*$. so dass $\{\lambda(\mu_1), \ldots, \lambda(\mu_{r+s-1})\}$ eine Basis von Γ ist.

17.7 Beispiel: Ist $K = \mathbb{Q}(\sqrt{m})$ reell-quadratische Erweiterung, dann ist $r = 2$, $s = 0$, $\mu(K) = \{\pm 1\}$. Also haben wir nur eine Fundamentaleinheit die einen Faktor $\mathbb{Z}$ erzeugt. Sei ε eine solche Einheit. Dann erzeugen auch ε^{-1} und $-\varepsilon$, $-\varepsilon^{-1}$ eine unendliche Untergruppe. Unter den Elementen $\pm\varepsilon$, $\pm\varepsilon^{-1}$ gibt es genau eines mit $\varepsilon > 1$. Dieses Element η nennt man die *Fundamentaleinheit* von K. Da seine Norm ± 1 sein muss und

$$\begin{array}{lll} \eta = a + b\sqrt{m} & a, b \in \mathbb{Z} & m \equiv 2, 3 \mod 4 \\ \eta = \dfrac{a + b\sqrt{m}}{2} & a, b \in \mathbb{Z} \text{ von gleicher Parität} & m \equiv 1 \mod 4 \end{array}$$

suchen wir **kleine positive** Werte a, b für die

$$\begin{array}{ll} a^2 = m \cdot b^2 \pm 1 & m \equiv 2, 3 \mod 4 \\ a^2 = m \cdot b^2 \pm 4 & m \equiv 1 \mod 4 \end{array}$$

Beispiel: $m = 3 \quad b = 1,\ a = 2 \quad \eta = 2 + \sqrt{3}$

$$m = 5 \quad b = 1,\ a = 1 \quad \eta = \frac{1 + \sqrt{5}}{2}.$$

Teil IV
Verzweigungstheorie

18 Erweiterungen von Dedekindringen

Die Ergebnisse der vergangenen Paragraphen legen nahe, sich mit den Primidealen in $\mathcal{O}_K$ zu beschäftigen. Ist $\mathfrak{p} \neq 0$ ein Primideal, dann ist $\mathfrak{p} \cap \mathbb{Z} = (p)$ mit $p \in \mathbb{N}$ prim, d.h. $(p) \subset \mathfrak{p}$, also $\mathfrak{p}|(p)$. Wir wollen untersuchen, wie die Primzerlegung von (p), $p \in \mathbb{Z}$ prim, in $\mathcal{O}_K$ aussieht. Wie auch in den vergangenen Paragraphen, machen wir das für beliebige Dedekindringe und nicht nur für Erweiterungen $\mathbb{Z} \subset \mathcal{O}_K$.

18.1 Satz: Sei R ein Dedekindring mit Quotientenkörper K. Sei F/K eine endliche separable Erweiterung und $B \subset F$ der ganze Abschluss von R in F. Dann ist B ein Dedekindring.

Beweis: Nach 7.14 ist F der Quotientenkörper von B, die Nenner können sogar in R gewählt werden. Damit ist B ganz abgeschlossen.

Sei $\mathfrak{p} \neq \{0\}$ ein Primideal in B, dann ist $R \cap \mathfrak{p} \neq \{0\}$ nach 12.7. Die Abbildung

$$R/R \cap \mathfrak{p} \to B/\mathfrak{p}, \quad r + (R \cap \mathfrak{p}) \mapsto r + \mathfrak{p}$$

ist bekanntlich injektiv ($R/R \cap \mathfrak{p} \cong (R + \mathfrak{p})/\mathfrak{p} \subset B/\mathfrak{p}$). Da $\mathfrak{p}$ ein Primideal ist, ist $B/\mathfrak{p}$ ein Integritätsring. Also ist auch $R/R \cap \mathfrak{p}$ ein Integritätsring und damit $R \cap \mathfrak{p}$ ein Primideal in R. Da R ein Dedekindring ist, ist $R \cap \mathfrak{p}$ maximal, also $R/R \cap \mathfrak{p}$ ein Körper. Damit ist aber auch $B/\mathfrak{p}$ ein Körper: Denn sei $\overline{b} \neq \overline{0}$ eine Restklasse in $B/\mathfrak{p}$. Da b ganz über R ist, erfüllt es eine irreduzible Ganzheitsgleichung $f(b) = 0$ mit $f \in R[X]$. Dann ist $\overline{b}$ algebraisch über $R/R \cap \mathfrak{p}$, und $(R/R \cap \mathfrak{p})[\overline{b}]$ ist ein endlich-dimensionaler $(R/R \cap \mathfrak{p})$-Vektorraum. Nach Aufgabe 1.8 ist $\overline{b}$ in $(R/R \cap \mathfrak{p})[\overline{b}] \subset B/\mathfrak{p}$ invertierbar. Damit ist $\mathfrak{p}$ auch maximal.

Es bleibt nur noch nachzuweisen, dass B noethersch ist. Nach 10.3 ist B Untermodul eines freien, endlich erzeugten R-Moduls. Da R kein Hauptidealring zu sein braucht, müssen wir Arbeit investieren. Das Resultat folgt aus folgendem Ergebnis, weil jeder Untermodul eines noetherschen R-Moduls noethersch ist. □

18.2 Satz: Ist R ein noetherscher Ring, dann ist jeder endlich erzeugte R-Modul noethersch.

Beweis: Aus 12.4 folgt: Sind M und N noethersch, dann ist auch $M \oplus N$ noethersch, denn M ist Untermodul von $M \oplus N$ und $M \oplus N/M \cong N$. Damit ist R^n noethersch. Sei e^i der i-te "Einheitsvektor" in R^n. Ist nun M ein endlich erzeugter R-Modul, $M = R \cdot x_1 + \ldots + R \cdot x_n$, dann ist M das Bild von R^n unter der Abbildung, die e_i auf x_i abbildet. Nach 12.4 ist damit M noethersch. □

18.3 Bemerkung: Der Satz 18.1 gilt auch ohne die Voraussetzung "separabel".

18.4 Für Primideale $\mathfrak{p} \subset R$ gilt im Kontext von 18.1, dass $\mathfrak{p} \cdot B \neq B$ ist.

Beweis: Sei $\mathfrak{p} \neq 0$. Da $\mathfrak{p}^2 \neq \mathfrak{p}$, gibt es ein $r \in \mathfrak{p} \backslash \mathfrak{p}^2$. Es folgt $(r) = \mathfrak{p} \cdot J$ mit J coprim zu $\mathfrak{p}$ (denn $r \in \mathfrak{p}$, also $\mathfrak{p}|(r)$, aber $\mathfrak{p}^2 \nmid (r)$). Also gilt $\mathfrak{p} + J = R$. Damit gibt es $b \in \mathfrak{p}$ und $s \in J$, so dass $1 = b + s$. Es gilt $s \notin \mathfrak{p}$, da sonst $\mathfrak{p} = R$, und $s \cdot \mathfrak{p} \subset J \cdot \mathfrak{p} = (r) = R \cdot r$.

Wäre $\mathfrak{p} \cdot B = B$, hätten wir $s \cdot B = s \cdot \mathfrak{p} \cdot B \subset rB$, so dass $s = r \cdot x$ mit $x \in B$. Da $x = \frac{s}{r} \in K$, ist $x \in K \cap B = R$. Also $s \in (r) \subset \mathfrak{p}$, ein Widerspruch. □

Da $\mathfrak{p} \cdot B \neq 0$ für $\mathfrak{p} \neq 0$ und $\mathfrak{p} \cdot B \neq B$, hat das Ideal $\mathfrak{p}B$ eine Pirmzerlegung

18.5 $\mathfrak{p} \cdot B = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$ in B.

Statt $\mathfrak{p} \cdot B$ schreiben wir oft kürzer $\mathfrak{p}$, wenn klar ist, in welchem Ring wir arbeiten.

18.6 Ein Ideal $J \neq B$ von B teilt $\mathfrak{p} \cdot B$ genau dann, wenn $\mathfrak{p} = J \cap R$.

Beweis: „⇒": $J|\mathfrak{p} \cdot B \Rightarrow \mathfrak{p} \subset \mathfrak{p} \cdot B \subset J$. Da $1 \notin J$, ist $J \cap R \neq R$. Also $\mathfrak{p} \subset J \cap R \neq R$. Da $J \cap R$ ein Ideal in R ist, folgt aus der Maximalität von $\mathfrak{p}$, dass $\mathfrak{p} = J \cap R$.

„⇐": Da $\mathfrak{p} = J \cap R$, ist $\mathfrak{p} \cdot B \subset J$. Also ist J Teiler von $\mathfrak{p} \cdot B$ in B. □

18.7 Definition: Sei $\mathfrak{p} \subset R$ ein Primideal, $\mathfrak{p} \neq 0$. Sei

$$\mathfrak{p} \cdot B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$$

die Primzerlegung von $\mathfrak{p}$ in B. Man nennt die $\mathfrak{P}_i$ *Primideale über* $\mathfrak{p}$. Die Zahl e_i heißt *Verzweigungsindex*, bezeichnet mit $e(\mathfrak{P}_i/\mathfrak{p})$. Ist ein $e_i > 1$, heißt $\mathfrak{p}$ *verzweigt* in B. Der Grad der Körpererweiterung $R/\mathfrak{p} \subset B/\mathfrak{P}_i$

$$f_i = f(\mathfrak{P}_i/\mathfrak{p}) = [B/\mathfrak{P}_i, R/\mathfrak{p}]$$

heißt *Trägheitsgrad* von $\mathfrak{P}_i$ über $\mathfrak{p}$.

(Wir erinnern daran, dass wir $R/\mathfrak{p}$ nach dem Beweis von 18.1 als Teilkörper von $B/\mathfrak{P}_i$ auffassen können, weil $\mathfrak{p} = \mathfrak{P}_i \cap R$.)

18.8 Satz: Sei R eine Dedekindring mit Quotientenkörper K. Sei F/K endliche separable Erweiterung und $B \subset F$ der ganze Abschluss von R in F. Sei $\mathfrak{p} \neq 0$ ein Primideal in R und

$$\mathfrak{p} \cdot B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$$

die Primzerlegung von $\mathfrak{p}$ in B mit $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Dann gilt

$$\sum_{i=1}^{r} e_i \cdot f_i = n := [F : K].$$

Gilt $|\operatorname{Gal}(F/K)| = [F : K]$, man nennt dann $K \subset F$ eine *Galoiserweiterung*, dann sind alle e_i gleich und alle f_i gleich, so dass

$$n = r \cdot e \cdot f.$$

Beweis: Da $\mathfrak{P}_i^{e_i}$ und $\mathfrak{P}_j^{e_j}$ für $i \neq j$ coprim sind, folgt aus dem chinesischen Restesatz (beachte $\mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r} = \mathfrak{P}_1^{e_1} \cap \ldots \cap \mathfrak{P}_r^{e_r}$ im coprimen Fall nach Aufgabe 1.3)

$$B/(\mathfrak{p} \cdot B) \cong B/\mathfrak{P}_1^{e_1} \times \ldots \times B/\mathfrak{P}_r^{e_r}.$$

Da $\mathfrak{p} \cdot B \cap R = \mathfrak{p}$, ist $R/\mathfrak{p}$ ein Teilkörper von $B/\mathfrak{p}B$ und die Projektion $B/\mathfrak{p}B \to B/\mathfrak{P}_i^{e_i}$ macht $B/\mathfrak{P}_i^{e_i}$ zu einem $R/\mathfrak{p}$-Vektorraum. Zur Vereinfachung der Schreibweise bezeichnen wir den Körper $R/\mathfrak{p}$ mit $\mathbb{K}$. Der erste Teil des Satzes folgt aus den Behauptungen

$$\dim_{\mathbb{K}}(B/\mathfrak{p}B) = n \quad \dim_{\mathbb{K}}(B/\mathfrak{P}_i^{e_i}) = e_i \cdot f_i$$

und dem chinesischen Restesatz.

Sei $\overline{w}_1, \ldots, \overline{w}_m$ eine $\mathbb{K}$-Basis von $B/\mathfrak{p} \cdot B$ mit Repräsentanten $w_i \in B$. Im Beweis von 18.1 zeigten wir, dass B ein endlich erzeugter R-Modul ist. Also ist $\dim_{\mathbb{K}}(B/\mathfrak{p}B) < \infty$. Wir zeigen jetzt, dass $w_1, \ldots, w_m$ eine K-Basis von F ist. Es folgt $m = n$, womit die erste Gleichung bewiesen wäre.

Angenommen $w_1, \ldots, w_m$ sind linear abhängig über K, dann sind sie auch linear abhängig über R (multipliziere mit dem Produkt der Nenner):

$$r_1 \cdot w_1 + \ldots + r_m \cdot w_m = 0, \qquad r_i \in R, \text{ nicht alle } r_i = 0.$$

Sei J das von $r_1, \ldots, r_m$ erzeugte Ideal in R. Wegen der eindeutigen Primzerlegung gibt es ein $a \in J^{-1}$, so dass $a \notin J^{-1} \cdot \mathfrak{p}$, also $a \cdot J \not\subset \mathfrak{p}$. Da $a \cdot J \subset R$, gilt $a \cdot r_i \in R$ für $i = 1, \ldots, m$, aber nicht alle $a \cdot r_i$ liegen in $\mathfrak{p}$, da sonst $a \cdot J \subset \mathfrak{p}$. Durch Übergang zu den Restklassen $\bmod \mathfrak{p}$ erhalten wir also eine nicht-triviale Darstellung

$$\overline{a \cdot r_1} \cdot \overline{w}_1 + \ldots + \overline{a \cdot r_m} \cdot \overline{w}_m = \overline{0}, \quad \overline{a \cdot r_i} \in \mathbb{K} = R/\mathfrak{p},\ \overline{w}_i \in B/\mathfrak{p}B$$

im Widerspruch zur linearen Unabhängigkeit der $\overline{w}_i$.

Wir wollen nun zeigen, dass $F = Kw_1 + \ldots + Kw_m$.

Sei $M = Rw_1 + \ldots + Rw_m$ und $N = B/M$. Nun gilt $B = M + \mathfrak{p} \cdot B$. Es folgt $\mathfrak{p} \cdot N = N$, da $B = \mathfrak{p}B \mod M$. Nach 18.2 ist B noetherscher R-Modul. Damit sind B und N endlich erzeugte R-Moduln, etwa $N = R\alpha_1 + \ldots + R\alpha_s$. Wegen $\mathfrak{p} \cdot N = N$ erhalten die Gleichungen

$$\alpha_i = \sum_{j=1}^{s} a_{ij} \cdot \alpha_j \quad \text{mit} \quad a_{ij} \in \mathfrak{p}$$

bzw. $0 = \sum_{j=1}^{s} (\delta_{ij} - a_{ij})\alpha_j$

Sei $A = (\delta_{ij} - a_{ij})_{i,j}$ und A^* die adjungierte Matrix. Aus $A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = 0$ folgt

$$0 = A^* \cdot A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = \det A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix}$$

Ist $d = \det A$, folgt somit $d \cdot \alpha_i = 0$, $i = 1, \ldots, s$, also $d \cdot N = 0$. Ist $p : B \to B/M = N$ die Projektion, so folgt $p(d \cdot x) = d \cdot p(x) = 0$, also $d(B) \subset \operatorname{Kern} p = M$, d.h.

$$d \cdot B \subset R \cdot w_1 + \ldots + R \cdot w_m$$

$d \neq 0$, denn rechnen wir $\mod \mathfrak{p}$, erhalten wir $\det A = 1$. Damit erhalten wir

$$F = d \cdot F \subset K \cdot w_1 + \ldots + K \cdot w_m,$$

da F der Quotientenkörper von B ist und die Nenner in R liegen dürfen.

Für die zweite Gleichung betrachten wir folgende Kette von B-Moduln

$$B \supset \mathfrak{P}_i \supset \mathfrak{P}_i^2 \supset \ldots \supset \mathfrak{P}_i^{e_i}.$$

Sei $\mathfrak{P} = \mathfrak{P}_i$. Für jedes r ist $\mathfrak{P}^r/\mathfrak{P}^{r+1}$ ein $B/\mathfrak{P}$-Modul und damit ein $B/\mathfrak{P}$-Vektorraum vermöge der Operation

$$\begin{array}{rcl} B/\mathfrak{P} \times (\mathfrak{P}^r/\mathfrak{P}^{r+1}) & \longrightarrow & \mathfrak{P}^r/\mathfrak{P}^{r+1} \\ ((b + \mathfrak{P}), (a + \mathfrak{P}^{r+1}) & \longmapsto & ab + a \cdot \mathfrak{P} + b \cdot \mathfrak{P}^{r+1} + \mathfrak{P} \cdot \mathfrak{P}^{r+1} \subset a \cdot b + \mathfrak{P}^{r+1} \end{array}$$

Die Dimension von $\mathfrak{P}^r/\mathfrak{P}^{r+1}$ als $B/\mathfrak{P}$-Vektorraum ist 1, denn sonst gäbe es eine surjektive B-lineare Abbildung $\mathfrak{P}^r/\mathfrak{P}^{r+1} \to B/\mathfrak{P}$ mit nicht-trivialen Kern und damit einen B-Modul M mit $\mathfrak{P}^{r+1} \subsetneqq M \subsetneqq \mathfrak{P}^r$. Dieses M wäre somit ein Ideal zwischen $\mathfrak{P}^{r+1}$ und $\mathfrak{P}^r$, aber das ist unmöglich. Es folgt

$$B/\mathfrak{P}_i^{e_i} \text{ ist ein } B/\mathfrak{P}_i\text{-Vektorraum der Dimension } e_i.$$

Nach Definition von f_i ist $B/\mathfrak{P}_i$ ein $\mathbb{K}$-Vektorraum der Dimension f_i. Also ist $B/\mathfrak{P}_i^{e_i}$ ein $\mathbb{K}$-Vektorraum der Dimension $e_i \cdot f_i$.

Sei jetzt F/K Galois-Erweiterung mit Galois-Gruppe G. Ist $b \in B$, so ist b und damit auch $\sigma(b)$, $\sigma \in G$, ganz über R. Es folgt $\sigma(B) = B$ für $\sigma \in G$. Da $\sigma : B \to B$ ein Ringautomorphismus ist, ist $\sigma(\mathfrak{P})$ ein Primideal, falls $\mathfrak{P}$ ein Primideal ist. Weiter gilt: Ist $\mathfrak{P} \subset B$ Teiler von $\mathfrak{p} \cdot B$, so gilt $\mathfrak{p} = \mathfrak{P} \cap R = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P}) \cap \sigma(R) = \sigma(\mathfrak{P}) \cap R$, d.h. auch $\sigma(\mathfrak{P})$ ist Teiler von $\mathfrak{p} \cdot B$ nach 18.6. Da σ ein Automorphismus ist, gilt

$$e(\sigma(\mathfrak{P})/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) \qquad f(\sigma(\mathfrak{P})/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}).$$

Damit folgt der 2. Teil aus dem ersten, wenn wir zeigen können

Behauptung: Sind $\mathfrak{P}$ und $\mathfrak{Q}$ Primideale in B, die $\mathfrak{p}$ teilen, dann gibt es ein $\sigma \in G$ mit $\sigma(\mathfrak{P}) = \mathfrak{Q}$.

Beweis: Wir nehmen an, dass $\sigma(\mathfrak{P}) \neq \mathfrak{Q}$ für alle $\sigma \in G$. Seien $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ die verschiedenen Primideale der Familie $\{\sigma(\mathfrak{P}); \sigma \in G\}$. Dann sind $\mathfrak{Q}, \mathfrak{P}_1, \ldots, \mathfrak{P}_r$ paarweise coprim. Nach dem chinesischen Restsatz haben wir einen Epimorphismus

$$\varphi : B \to B/\mathfrak{Q} \times B/\mathfrak{P}_1 \times \ldots \times B/\mathfrak{P}_r.$$

Sei $\beta \in B$ ein Urbild von $(\overline{0}, \overline{1}, \ldots, \overline{1})$. Dann ist $\beta \in \mathfrak{Q}$ und $\beta \notin \sigma(\mathfrak{P})$ für alle $\sigma \in G$.

$b := N_{F/K}(\beta) = \prod_{\sigma \in G} \sigma(\beta) \in \mathfrak{Q} \cap R = \mathfrak{p}$, denn β ist ganz und $\beta | b$ in B. Da $\beta \in \mathfrak{Q}$, folgt $b \in \mathfrak{Q}$.

Da $\beta \notin \sigma^{-1}(\mathfrak{P})$ für alle $\sigma \in G$, gilt $\sigma(\beta) \notin \mathfrak{P}$ für alle $\sigma \in G$. Da aber $b = \prod \sigma(\beta) \in \mathfrak{p} \subset \mathfrak{P}$ und $\mathfrak{P}$ in B prim ist, muss mindestens ein Faktor $\sigma(\beta)$ in $\mathfrak{P}$ liegen, ein Widerspruch. □

18.9 Bemerkung: Die Gleichung $\sum_{i=1}^r e_i \cdot f_i = n$ in 18.8 nennt man auch die "fundamentale Gleichung". Sie zeigt, dass ein Primideal $\mathfrak{p}$ in R um so "fleißiger" in Primideale aus B zerfällt, je kleiner der Trägheitsgrad ist.

Wir wollen jetzt die Primideale über $\mathfrak{p}$ im Falle einer einfachen Erweiterung bestimmen:

Mit den Bezeichnungen aus 18.8 sei $F = K(\alpha)$, wobei das primitive Element α aus B sei. Das Minimalpolynom f von α liegt nach 7.17 in $R[X]$. Sei $n = \operatorname{grad} f$.

18.10 Definition: $\mathfrak{F} = \{x \in B; x \cdot B \subset R[\alpha]\}$ heißt *Führer* des Ringes $R[\alpha]$.

18.11 $\mathfrak{F}$ ist ein von 0 verschiedenes Ideal in B, und $\mathfrak{F} \subset R[\alpha] \subset B$.

Beweis: Offensichtlich ist $\mathfrak{F}$ ein Ideal. Die Diskriminante $d = D_{F/K}(1, \alpha, \ldots, \alpha^{n-1})$ ist nach 9.9 von 0 verschieden und $d \cdot B \subset R[\alpha]$ nach 10.3. Da $1 \in B$, ist $\mathfrak{F} \subset R[\alpha]$, und $R[\alpha] \subset B$, weil $\alpha \in B$ ist. □

18.12 Satz: Sei $\mathfrak{p}$ ein zum Führer $\mathfrak{F}$ von $R[\alpha]$ teilerfremdes Primideal in R und

$$\overline{f} = \overline{f}_1^{e_1} \cdot \ldots \cdot \overline{f}_r^{e_r}$$

die Zerlegung des Bildes $\overline{f}$ des Minimalpolynoms f von α in $(R/\mathfrak{p})[X]$ in seine Primfaktoren. Dabei sei $f_i \in R[X]$ ein normierter Repräsentant von $\overline{f}_i$. Dann sind

$$\mathfrak{P}_i = \mathfrak{p} \cdot B + f_i(\alpha) \cdot B \qquad i = 1, \ldots r$$

die verschiedenen Primideale in B über $\mathfrak{p}$, und es gilt

(1) $f(\mathfrak{P}_i/\mathfrak{p}) = \operatorname{grad} \overline{f}_i$

(2) $\mathfrak{p} \cdot B = \mathfrak{P}_i^{e_i} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$

Beweis: Sei $C = R[\alpha]$ und $\overline{R} = R/\mathfrak{p}$

Behauptung: $B/(\mathfrak{p} \cdot B) \cong C/(\mathfrak{p} \cdot C) \cong \overline{R}[X]/(\overline{f})$.

Da $\mathfrak{p}$ coprim zu $\mathfrak{F}$ ist, gilt $B = \mathfrak{p} \cdot B + \mathfrak{F}$. Da $\mathfrak{F} \subset C$, folgt $B = \mathfrak{p}B + C$. Damit ist

$$\varphi : C \hookrightarrow B \to B/\mathfrak{p} \cdot B. \qquad (*)$$

surjektiv und $\operatorname{Kern} \varphi = C \cap \mathfrak{p}B$. Also gilt $C/(C \cap \mathfrak{p}B \cong B/(\mathfrak{p} \cdot B)$. Wir zeigen jetzt, dass $C \cap \mathfrak{p}B = \mathfrak{p} \cdot C$, und erhalten so den ersten Isomorphismus der Behauptung.

Da $\mathfrak{p}$ und $\mathfrak{F} \cap R$ coprim sind, gilt

$$\mathfrak{p} + \mathfrak{F} \cap R = R$$

$\mathfrak{p} \cdot B$ und C sind R-Moduln. Es folgt somit

$$\begin{aligned} C \cap \mathfrak{p} \cdot B &= R \cdot (C \cap \mathfrak{p} \cdot B) = (\mathfrak{p} + \mathfrak{F} \cap R) \cdot (C \cap \mathfrak{p} \cdot B) \\ &\subset \mathfrak{p} \cdot C + \mathfrak{p} \cdot \mathfrak{F} \cdot B \subset \mathfrak{p} \cdot C \quad , \text{ da } \mathfrak{F} \cdot B \subset C. \end{aligned}$$

Es folgt $\mathfrak{p} \cdot C = C \cap \mathfrak{p} \cdot B$.

Für den zweiten Isomorphismus betrachten wir die Projektionen

$$\psi : R[X] \to \overline{R}[X] \to \overline{R}[X]/(\overline{f})$$

Kern ψ ist das durch $\mathfrak{p}$ und f erzeugte Ideal $J = (\mathfrak{p}, f) \subset R[X]$. Da nun $C = R[X]/(f)$, folgt $C/(\mathfrak{p} \cdot C) \cong R[X]/J \cong \overline{R}[X]/(\overline{f})$.

Da die $\overline{f}_i$ paarweise teilerfremd sind, liefert der chinesische Restsatz einen Isomorphismus von Ringen

$$\overline{R}[X]/(\overline{f}) \cong \bigoplus_{i=1}^{r} \overline{R}[X]/(\overline{f}_i^{e_i}).$$

Die Primideale der rechten Seite sind Summen, in denen ein Summand von der Form $(\overline{f}_i)$ ist, während die übrigen der ganze Summand ist. Damit sind die Primideale der linken Seite die durch (f_i) mod $\overline{f}$ erzeugten Hauptideale $(\overline{f}_i)$, $i = 1, \ldots, r$. Ist $S = \overline{R}[X]/(\overline{f})$, dann ist der Grad der Körpererweiterung

$$[S/(\overline{f}_i) : \overline{R}] = \operatorname{grad} \overline{f}_i$$

und $0 = (\overline{f}) = \bigcap_{i=1}^{r} (\overline{f}_i)^{e_i}$ in S.

Nach der Behauptung haben wir einen Isomorphismus

$$\overline{R}[X]/(\overline{f}) \xrightarrow{\cong} B/\mathfrak{p} \cdot B, \quad \overline{g} \mapsto \overline{g(\alpha)}.$$

Damit hat $B/\mathfrak{p}B$ dieselben Eigenschaften wie $\overline{R}[X]/(\overline{f})$: Die Primideale $\overline{\mathfrak{P}}_i$ von $\overline{B} := B/\mathfrak{p}B$ entsprechen den Primidealen $(\overline{f}_i)$ und sind die von $f_i(\alpha)$ mod $\mathfrak{p}B$ erzeugten Hauptideale;

$$[\overline{B}/\overline{\mathfrak{P}}_i : \overline{R}] = \operatorname{grad} \overline{f}_i \qquad (0) = \bigcap_{i=1}^{r} \overline{\mathfrak{P}}_i^{e_i} \tag{$**$}$$

$\mathfrak{P}_i = \mathfrak{p} \cdot B + f_i(\alpha) \cdot B$ ist das Urbild von $\overline{\mathfrak{P}}_i$ unter der Projektion $B \to \overline{B} = B/\mathfrak{p}B$. Dann ist $\mathfrak{P}_i$ ein Primideal in B.

Das Urbild von $\overline{\mathfrak{P}}_i^{e_i}$ ist $\mathfrak{p} \cdot B + f_i(\alpha)^{e_i} \cdot B$. Offensichtlich gilt $\mathfrak{P}_i^{e_i} \subset \mathfrak{p} \cdot B + f_i(\alpha)^{e_i} \cdot B$, so dass $\mathfrak{p} \cdot B + f_i(\alpha)^{e_i} \cdot B$ Teiler von $\mathfrak{P}_i^{e_i}$ ist. Aus der Primfaktorisierung folgt, dass $\mathfrak{P}_i^{e_i}$ das Urbild von $\overline{\mathfrak{P}}_i^{e_i}$ ist, da $\mathfrak{p} \cdot B + f_i(\alpha)^{e_i} \cdot B$ und $\mathfrak{P}_i^{e_i}$ dasselbe Bild in $B/\mathfrak{p}B$ haben. Damit folgt aus $(**)$

$$\mathfrak{p}B \supset \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i} \supset \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

so dass $\mathfrak{p} \cdot B$ Teiler von $\prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ ist. Letztlich gilt

$$f(\mathfrak{P}_i/\mathfrak{p}) = [B/\mathfrak{P}_i : R/\mathfrak{p}] = [\overline{B}/\overline{\mathfrak{P}}_i : \overline{R}] = \operatorname{grad} \overline{f}_i.$$

Da aber

$$\sum_{i=1}^{r} e_i \cdot \operatorname{grad} \overline{f}_i = \sum_{i=1}^{r} \operatorname{grad} \overline{f}_i^{e_i} = \operatorname{grad} \overline{f} = \operatorname{grad} f = [F : K]$$

folgt aus 18.8

$$\mathfrak{p} \cdot B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

□

18.13 Satz: In vielen Fällen ist $B = R[\alpha]$. Dann ist $\mathfrak{F} = B$ und jedes Ideal $\mathfrak{p}$ von B ist coprim zu $\mathfrak{F}$.

19 Verzweigungen

Sei wieder R ein Dedekindring, K sein Quotientenkörper, F/K eine separable endliche algebraische Erweiterung und B der ganze Abschluss von R in F. Dann ist B nach18.1 wieder ein Dedekindring.

19.1 Definition: Ein Primideal $\mathfrak{p} \subset R$ heißt *voll zerlegt* (oder *total zerlegt*) in F, wenn in der Primfaktorzerlegung

$$\mathfrak{p} \cdot B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r} \qquad (*)$$

von $\mathfrak{p}$ in B gilt: $r = n = [F : K]$, also $e_i = 1 = f(\mathfrak{P}_i/\mathfrak{p})$ für $i = 1, \ldots, r$. Wir nennen $\mathfrak{p}$ *unzerlegt* in F, wenn $r = 1$, wenn es also in B nur ein Primideal über $\mathfrak{p}$ gibt. Wir nennen $\mathfrak{P}_i$ *unverzweigt* über R (oder über K), wenn $e_i = 1$ und die Körpererweiterung

$$R/\mathfrak{p} \subset B/\mathfrak{P}_i$$

separabel ist. Sonst heißt $\mathfrak{P}_i$ *verzweigt*. Gilt überdies $f(\mathfrak{P}_i/\mathfrak{p}) = 1$, heißt $\mathfrak{P}_i$ *rein verzweigt*. Ist jedes $\mathfrak{P}_i$ der Zerlegung $(*)$ unverzweigt, nennen wir $\mathfrak{p}$ *unverzweigt*, und sonst *verzweigt*.

Sind alle Primideale $\mathfrak{p}$ von R unverzweigt, nennen wir die Körpererweiterung $K \subset F$ unverzweigt.

Ziel dieses Abschnittes ist es zu zeigen, dass ein Primideal nur in endlich vielen Ausnahmefällen verzweigt ist. Das ist Teil der Aussage des folgenden Satzes, der auch in größerer Allgemeinheit als in der vorliegenden Form Gültigkeit hat.

19.2 Satz: Sei K ein Zahlkörper und B ein freier endlich erzeugter R-Modul. Dann ist $\mathfrak{p}$ genau dann in F verzweigt, wenn $\mathfrak{p}$ Teiler von $\mathrm{disc}(B/R)$ ist. Insbesondere sind nur endlich viele Primideale in F verzweigt.

19.3 Erläuterung: Wie wir in 9.3 erläutert haben, ist $\mathrm{disc}(B/R)$ das Ideal in R, das von den Diskriminanten

$$D_{F/K}(\alpha_1, \ldots, \alpha_n)$$

aller K-Basen $\{\alpha_1, \ldots, \alpha_n\} \subset B$ von F erzeugt wird. Insbesondere ist $\mathfrak{p}$ per Definition genau dann Teiler von $\mathrm{disc}(B/R)$, wenn $\mathrm{disc}(B/R) \subset \mathfrak{p}$ ist.

Wir beweisen Satz 19.2 mit einer Reihe von Lemmata.

19.4 Lemma: Sei R ein Ring, $R \subset B$ eine Ringerweiterung, so dass B ein freier R-Modul mit Basis $\{\beta_1, \ldots, \beta_n\}$ ist. Dann sind die Restklassen $\{\overline{\beta}_1, \ldots, \overline{\beta}_n\}$ eine Basis von $B/(J \cdot B)$ als R/J-Modul, wobei $J \subset R$ ein beliebiges Ideal ist. Weiter gilt für die Diskriminanten

$$D(\overline{\beta}_1, \ldots, \overline{\beta}_n) = D(\beta_1, \ldots, \beta_n) \qquad \mathrm{mod}\ J.$$

Beweis: Da jedes $b \in B$ eine R-Linearkombination der β_i ist, ist $\overline{b} \in B/(J \cdot B)$ eine R/J-Linearkombination der $\overline{\beta}_i$ durch Übergang zu dem Restklassen. Gilt nun

$$\overline{r}_1 \cdot \overline{\beta}_1 + \ldots + \overline{r}_n \cdot \overline{\beta}_n = \overline{0}$$

folgt: $r_1 \cdot \beta_1 + \ldots + r_n \cdot \beta_n \in B \cdot J = (R \cdot \beta_1 + \ldots R \cdot \beta_n) \cdot J = J \cdot \beta_1 + \ldots + J \cdot \beta_n$. Aus der Eindeutigkeit der Darstellung folgt $r_i \in J$, also $\overline{r}_i = \overline{0}$.

Die zweite Aussage ist ebenfalls klar, weil sich $D(\overline{\beta}_1, \ldots, \overline{\beta}_n)$ wie $D(\beta_1, \ldots, \beta_n)$ berechnet, nur dass man zur Restklasse übergeht. □

19.5 Lemma: Seien $R \subset B_i$, $i = 1, \ldots, k$ Ringerweiterungen, so dass B_i ein freier R-Modul vom Rang r_i ist. Dann gilt

$$\mathrm{disc}(\prod B_i/R) = \prod \mathrm{disc}(B_i/R).$$

Beweis: Es genügt, den Fall $k = 2$ zu behandeln. Sei $\{\alpha_1, \ldots, \alpha_m\}$ R-Basis von B_1 und $\{\beta_1, \ldots, \beta_n\}$ R-Basis von B_2. Dann ist

$$\{\varepsilon_1, \ldots, \varepsilon_{m+n}\} = \{(\alpha_1, 0), \ldots, (\alpha_m, 0), (0, \beta_1), \ldots, (0, \beta_n)\}$$

R-Basis von $B_1 \times B_2$. Da $(\alpha_i, 0) \cdot (0, \beta_j) = (0, 0)$, ist $(S_{B_1 \times B_2/R}(\varepsilon_i \cdot \varepsilon_j))$ eine Blockmatrix der Form

$$\begin{pmatrix} (S_{B_1/R}(\alpha_i \cdot \alpha_j))_{i,j} & 0 \\ 0 & (S_{B_2/R}(\beta_i \cdot \beta_j))_{i,j} \end{pmatrix}$$

und der Satz folgt. □

19.6 Lemma: (1) Ist K ein Körper und B eine K-Algebra mit $\dim_K B < \infty$ und besitzt B nilpotente Elemente $\beta \neq 0$, dann ist $\operatorname{disc}(B/K) = 0$.

(2) Ist B ein noetherscher Ring, der keine nilpotenten Elemente $x \notin 0$ enthält, dann ist $N = \bigcap\{\mathfrak{p};\ \mathfrak{p} \text{ Primideal in } B\} = 0$.

(3) Seien K und B wie in (1) und K perfekt; sei N durch Durchschnitt aller Primideale $\mathfrak{p}$ in B. Ist $N = 0$, dann ist $\operatorname{disc}(B/K) \neq 0$.

19.7 Definition: Ein Element x eines Ringes heißt *nilpotent*, wenn es ein $k \in \mathbb{N}$ gibt, so dass $x^k = 0$.
Ein Körper heißt *perfekt*, wenn jedes irreduzible Polynom aus $K[X]$ separabel ist.

Beweis: (1) Sei $\beta \neq 0$ aus B nilpotent. Da B ein K-Vektorraum ist, können wir β zu einer Basis $\{\beta_1, \ldots, \beta_n\}$ von B mit $\beta_1 = \beta$ erweitern. Die Abbildung

$$f : B \to B, \quad b \mapsto \beta_1 \cdot \beta_i \cdot b = \beta \cdot \beta_i \cdot b$$

ist nilpotent, d.h. es gibt ein $n \in \mathbb{N}$ mit $f^n = 0$. Also ist das Minimalpolynom $\mu(f; X)$ von f Teiler von X^n und damit selbst von der Form X^k. Da die Primteiler des charakteristischen Polynoms auch Primteiler von $\mu(f; X)$ sind, ist das charakteristische Polynom von f ebenfalls von der Form X^k. Nach 8.3 ist $S_{B/K}(\beta_1 \cdot \beta_i) = 0$. Also ist die erste Zeile der Matrix $(S_{B/K}(\beta_i \cdot \beta_j))$ der Nullvektor und ihre Determinante $\operatorname{disc}(B/K) = 0$.
(2) Sei $b \neq 0$ aus B und $\mathcal{F}$ die Familie aller Ideale $J \subset B$, die keine Potenz von b enthalten. Da $b^k \neq 0\ \forall k \in \mathbb{N}$, ist $(0) \in \mathcal{F}$, also $\mathcal{F}$ nicht leer. Da B ein noetherscher Ring ist, besitzt $\mathcal{F}$ ein maximales Element $\mathfrak{p}$.
Behauptung: $\mathfrak{p}$ ist Primideal.

Aussage (2) folgt aus dieser Behauptung: Nach Definition von $\mathcal{F}$ ist $b \notin \mathfrak{p}$. Also gibt es zu jedem $b \neq 0$ aus B ein Primideal $\mathfrak{p}$, das b nicht enthält.

Angenommen, $\mathfrak{p}$ ist kein Primideal, dann gibt es Elemente $x, y \in B$, so dass $x \notin \mathfrak{p}$, $y \notin \mathfrak{p}$, aber $x \cdot y \in \mathfrak{p}$. Dann gilt

$$\mathfrak{p} \subsetneqq \mathfrak{p} + (x) \text{ und } \mathfrak{p} \subsetneqq \mathfrak{p} + (y).$$

Wegen der Maximalität von $\mathfrak{p}$ in $\mathcal{F}$ gibt es $k, l \in \mathbb{N}$, so dass

$$b^k \in \mathfrak{p} + (x) \quad b^l \in \mathfrak{p} + (y).$$

Also

$$b^{k+l} \in \mathfrak{p}^2 + \mathfrak{p} \cdot (y) + \mathfrak{p} \cdot (x) + (x \cdot y) \subset \mathfrak{p} + \mathfrak{p} + \mathfrak{p} + (x \cdot y) \subset \mathfrak{p},$$

ein Widerspruch.

(3) Ist $\mathfrak{p}$ ein Primideal von B, dann ist $B/\mathfrak{p}$ ein Integritätsring mit Teilkörper K, denn $B/\mathfrak{p}$ ist K-Algebra und $\varphi : K \to B/\mathfrak{p}$, $1 \mapsto \overline{1}$ ist injektiv. Da $\dim_K B/\mathfrak{p} < \infty$, ist $B/\mathfrak{p}$ nach 1.8 ein Körper. Folglich ist $\mathfrak{p}$ nach 1.4 maximal.

Sind nun $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ paarweise verschiedene Primideale, dann sind $\mathfrak{p}_i$ und $\mathfrak{p}_j$ für $i \neq j$ wegen der Maximalität coprim. Der chinesische Restsatz gibt

$$B/\bigcap \mathfrak{p}_i \cong \prod_{i=1}^{k} B/\mathfrak{p}_i \qquad (*)$$

Es folgt

$$\infty > \dim_K B \geq \dim_K (B/\bigcap \mathfrak{p}_i) = \sum_{i=1}^{k} \dim_K (B/\mathfrak{p}_i) \geq k.$$

Also hat B nur endlich viele verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Nach Voraussetzung ist ihr Durchschnitt 0, so dass $(*)$ die Form

$$B \cong \prod_{i=1}^{r} B/\mathfrak{p}_i \qquad (**)$$

annimmt. Jedes $B/\mathfrak{p}_i$ ist ein Körper und endliche Erweiterung von K. Da K perfekt ist, ist die Erweiterung separabel. Nach 9.9 ist $\operatorname{disc}((B/\mathfrak{p}_i)/K) \neq 0$. Aus 19.5 folgt dann $\operatorname{disc}(B/K) \neq 0$ wegen $(**)$. □

Aus dem Beweis von 19.7 halten wir fest

19.8 Ist K ein Körper, B eine K-Algebra mit $\dim_K B < \infty$ und $\mathfrak{p} \subset B$ ein Primideal, dann ist $B/\mathfrak{p}$ ein Körper.

Beweis von Satz 19.2: Sei $\mathfrak{p} \subset R$ ein Primideal. Nach 19.4 gilt

$$\operatorname{disc}(B/R) \equiv \operatorname{disc}((B/\mathfrak{p} \cdot B)/(R/\mathfrak{p})) \qquad \mod \mathfrak{p}.$$

Nach 19.6 gilt, da $R/\mathfrak{p}$ nach 4.14 perfekt ist,

$$\operatorname{disc}((B/\mathfrak{p}B)/(R/\mathfrak{p})) = 0 \iff B/\mathfrak{p}B \text{ hat nilpotente Elemente } \neq 0.$$

Sei nun $\mathfrak{p} \cdot B = \prod \mathfrak{P}_i^{e_i}$, also $B/(\mathfrak{p} \cdot B) \cong \prod B/\mathfrak{P}_i^{e_i}$ nach dem chinesischen Restesatz. Dann gilt
$\mathfrak{p} \nmid \operatorname{disc}(B/R) \iff \operatorname{disc}((B/\mathfrak{p}B)/(R/\mathfrak{p})) \neq 0 \iff \prod B/\mathfrak{P}_i^{e_i}$ hat keine nilpotente Elemente $\neq 0 \iff B/\mathfrak{P}_i^{e_i}$ hat keine nilpotente Elemente $\neq 0$ $\forall i$ $\iff e^i = 1$ $\forall i$. □

Als Folgerung von 19.2 und dem von uns nicht bewiesenen schärferen Ergebnis 16.8 erhält man sofort

19.9 Satz: Es gibt keine unverzweigte Erweiterung von $\mathbb{Q}$.

Beweis: Sei $K/\mathbb{Q}$ endliche Erweiterung von $\mathbb{Q}$. Nach 19.2 genügt es zu zeigen, dass $|\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})| = |\delta_K| > 1$. Nach 16.8 hat jedes Element aus $\mathcal{C}l_K$ ein ganzes Ideal J als Repräsentanten, für das

$$\mathfrak{N}(J) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\delta_K|} \qquad n = [K : \mathbb{Q}].$$

(Wir hatten das schwächere Resultat $\mathfrak{N}(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}$ gezeigt.)
Da $\mathfrak{N}(J) \geq 1$, erhalten wir

$$\sqrt{|\delta_K|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{\frac{n}{2}},$$

letzteres, weil $\left(\frac{\pi}{4}\right) < 1$ und $n = r + 2s$. Ist a_n die rechte Seite, folgt

$$\frac{a_{n+1}}{a_n} = \frac{(n+1)^{n+1} n!}{(n+1)! \cdot n^n} \sqrt{\frac{\pi}{4}} = \frac{(n+1)^n}{n^n} \sqrt{\frac{\pi}{4}} = \left(1 + \frac{1}{n}\right)^n \sqrt{\frac{\pi}{4}} \geq (1+1)\sqrt{\frac{\pi}{4}}$$
$$> 1$$

Da $a_2 > 1$, folgt $a_n > 1$, also $\sqrt{|\delta_K|} > 1$. □

Aus unserem schwächeren Resultat können wir nur folgern: Alle endlichen Erweiterungen $\mathbb{Q} \subset K$, für die es nicht-reelle Einbettungen $K \to \mathbb{C}$ gibt oder für die $\mathcal{O}_K$ kein Hauptidealring ist, sind verzweigt.

20 Hilbert'sche Verzweigungstheorie

Wir behalten die Notation aus §19 bei. Die von David Hilbert (1862-1943) entwickelte Verzweigungstheorie beschäftigt sich mit dem Fall, dass $K \subset F$ eine **Galois-Erweiterung** ist.

Dieser Abschnitt ist daher Hörern gewidmet, die schon einen Kurs über Galois-Theorie besucht haben. Damit die anderen Hörer folgen können, möchte ich die Definitionen und Ergebnisse rekapitulieren, die wir für diesen Abschnitt benötigen.

Vorweggeschickt sei, dass wir uns ausschließlich mit **endlichen** Galois-Erweiterungen beschäftigen.

20.1 Definition: Eine algebraische Erweiterung $K \subset F$ heißt *normal*, wenn jedes irreduzible $f \in K[X]$, das in F eine Nullstelle hat, über F zerfällt. Ist $K \subset F$ normal und separabel, heißt $K \subset F$ *Galois-Erweiterung.*

Bevor wir auf die Äquivalenz dieser Definition mit der in 18.8 eingehen, wollen wir den Grundansatz der Galois-Theorie erläutern. Er verbindet die Körpertheorie mit der Gruppentheorie. Wir schon erwähnt, wollen wir uns auf endliche Erweiterungen beschränken.

Sei also $K \subset F$ eine endlich und folglich auch algebraische Erweiterung. Sei $G = \mathrm{Gal}(F/K)$ die Galois-Gruppe von F/K. Die Menge der Zwischenkörper $K \subset L \subset F$ und die Menge der Untergruppen von G bilden partiell geordnete Mengen. Wir definieren Abbildungen

$$\{\text{Zwischenkörper von } F/K\} \underset{\Omega}{\overset{\Pi}{\rightleftarrows}} \{\text{Untergruppen von } G\}$$

durch $\Pi(L) = \mathrm{Gal}(F/L)$ und $\Omega(U) =$ Fixkörper von U, d.h.

$$\Omega(U) = F^U = \{x \in F;\ \sigma(x) = x\ \forall \sigma \in U\}$$

Man sieht leicht ein

20.2 Ω und Π sind ordnungsumkehrende Abbildungen. D.h.

(1) Ist $K \subset L \subset E \subset F$, dann folgt $\Pi(E) \subset \Pi(L)$, also $\mathrm{Gal}(F/E) \subset \mathrm{Gal}(F/L)$.

(2) Sind $U \subset V \subset G$ Untergruppen, dann folgt $\Omega(V) \subset \Omega(U)$, also $F^V \subset F^U$.

20.3 Hauptsatz der Galoistheorie: Sei $K \subset F$ endliche Erweiterung und $G = \mathrm{Gal}(F/K)$. Dann gilt

(1) Ist U Untergruppe von G, dann gilt $\Pi\Omega(U) = U$.

(2) Ist L Zwischenkörper von F/K, dann gilt

$$\Pi\Omega(L) = L \iff [F : L] = |\,\mathrm{Gal}(F/L)|$$

(3) Äquivalent sind

(i) $K \subset F$ ist Galois

(ii) $K = \Omega\Pi(K) = F^G$

(iii) $[F : K] = |G|$

(iv) Π und Ω sind zueinander inverse ordnungsumkehrende Abbildungen.

Aus 20.3.3 folgt die Äquivalenz der Definition 20.1 mit unserer Definition aus 18.8.

Als Folgerung aus 20.3 erhalten wir

20.4 Ist $K \subset F$ endliche Galois-Erweiterung und ist $K \subset L \subset F$ ein Zwischenkörper, dann ist $L \subset F$ endliche Galois-Erweiterung.

Beweis: Die Endlichkeit folgt aus der Gradschachtelungsformel. Aus 20.3.3 folgt, dass $\Omega\Pi(L) = L$, also $[F : L] = |\,\mathrm{Gal}(F/L)|$ nach 20.3.2. Also ist $L \subset F$ Galois nach 20.3.3. □

Wir wollen nun wissen, wann $K \subset L$ Galois ist. Die Antwort gibt

20.5 Satz: Sei $K \subset F$ beliebige Galois-Erweiterung und $K \subset L \subset F$ ein Zwischenkörper. Dann gilt

$$K \subset L \text{ ist Galois} \iff \mathrm{Gal}(F/L) \text{ ist Normalteiler von } \mathrm{Gal}(F/K).$$

In diesem Fall ist die Abbildung

$$\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K), \quad \sigma \mapsto \sigma|L$$

ein Epimorphismus mit Kern $\mathrm{Gal}(F/L)$, so dass

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(F/K)/\,\mathrm{Gal}(F/L).$$

Mehr brauchen Sie für diesen Abschnitt nicht über Galois-Theorie zu wissen. Vielleicht ist Ihr Interesse für die Beweise dieser Aussagen und für Anwendungen der Galois-Theorie geweckt.

Sei jetzt R wieder ein Dedekindring, K sein Quotientenkörper, $K \subset F$ eine endliche Galoie-Erweiterung mit Galois-Gruppe G und B der ganze Abschluss von R in F. Dann gilt $\sigma(b) \in B$ für alle $b \in B$ und alle $\sigma \in G$, so dass wir eine Operation

$$G \times B \to B, \quad (\sigma, b) \mapsto \sigma(b)$$

von G auf B erhalten. Im Beweis von 18.8 haben wir bereits gezeigt:

20.6 (1) Ist $\mathfrak{P} \subset B$ ein Primideal über dem Primideal $\mathfrak{p} \subset R$, dann ist auch $\sigma(\mathfrak{P})$ ein Primideal über $\mathfrak{p}$, und es gilt

$$e(\sigma(\mathfrak{P})/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) \quad \text{und} \quad f(\sigma(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}).$$

(2) G operiert *transitiv* auf der Menge der Primideale über $\mathfrak{p}$. D.h. sind $\mathfrak{P}$ und $\mathfrak{Q}$ Primideale in B über $\mathfrak{p}$, dann gibt es ein $\sigma \in G$ mit $\mathfrak{Q} = \sigma(\mathfrak{P})$.

20.7 Definition: Sei $\mathfrak{P}$ ein Primideal in B. Die Standuntergruppe von $\mathfrak{P}$

$$G_{\mathfrak{P}} = \{\sigma \in G;\ \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

heißt *Zerlegungsgruppe* von $\mathfrak{P}$ über K. Der Fixkörper

$$L_{\mathfrak{P}} = \{x \in F;\ \sigma(x) = x\ \ \forall \sigma \in G_{\mathfrak{P}}\} = F^{G_{\mathfrak{P}}}$$

heißt *Zerlegungskörper* von $\mathfrak{P}$ über K.

Die Zerlegungsgruppe "misst", in wie viele verschieden Primideale ein Primideal $\mathfrak{p} \subset R$ in B zerfällt: Sei $\mathfrak{P}$ ein Primideal über $\mathfrak{p}$, dann besteht der Orbit von $\mathfrak{P}$ nach 20.6 genau aus den Primidealen über $\mathfrak{p}$. Da nun $|G \cdot \mathfrak{P}| = |G : G_{\mathfrak{P}}|$ (s. Einführung, Lemma 13.6) erhalten wir

20.8 (1) Ist $\mathfrak{P} \subset B$ ein Primideal über $\mathfrak{p} \subset R$, dann gibt es genau $[G : G_{\mathfrak{P}}]$ verschiedene Primideale in $\mathfrak{p}$.

(2) $G_{\mathfrak{P}} = \{\mathrm{id}\} \iff L_{\mathfrak{P}} = F \iff \mathfrak{p}$ ist voll zerlegt.
$G_{\mathfrak{P}} = G \iff L_{\mathfrak{P}} = K \iff \mathfrak{p}$ ist unzerlegt.

(3) Sind $\mathfrak{P}$ und $\mathfrak{Q} = \sigma(\mathfrak{P})$ Primideale über $\mathfrak{p}$, dann gilt

$$G_{\mathfrak{Q}} = \sigma \cdot G_{\mathfrak{P}} \cdot \sigma^{-1}.$$

Weiter erhalten wir aus 18.8.

20.9 Ist $\mathfrak{P} \subset B$ ein Primideal über $\mathfrak{p}$ und $\sigma_1, \ldots, \sigma_r$ ein volles Repräsentantensystem der Nebenklassen von $G_\mathfrak{P}$ in G, dann gilt

$$\mathfrak{p} \cdot B = \left(\prod_{i=1}^{r} \sigma_i(\mathfrak{P}) \right)^e \qquad \text{mit } [F:K] = r \cdot e \cdot [(B/\mathfrak{P}) : (R/\mathfrak{p})]$$

und $r = \frac{|G|}{|G_\mathfrak{P}|}$, $|G_\mathfrak{P}| = e \cdot f$. Weiter gilt $[(B/\mathfrak{P}) : (R/\mathfrak{p})] = f(\mathfrak{P}/\mathfrak{p})$.

20.10 Satz: Sei $\mathfrak{P}_L := \mathfrak{P} \cap L_\mathfrak{P}$ das "unter $\mathfrak{P}$ liegende" Primideal von $L_\mathfrak{P} \cap B$. Dann gilt:

(1) $\mathfrak{P}_L$ ist unzerlegt in F, d.h. $\mathfrak{P}$ ist das einzige über $\mathfrak{P}_L$ liegende Primideal in B.

(2) $\mathfrak{P}$ hat über $L_\mathfrak{P}$ den Verzweigungsindex $e = e(\mathfrak{P}/\mathfrak{p})$ und den Trägheitsgrad $f = f(\mathfrak{P}/\mathfrak{p})$.

(3) Der Verzweigungsindex und Trägheitsgrad von $\mathfrak{P}_L$ über K sind beide 1.

Beweis: (1) Da F/K Galois-Erweiterungen ist, gilt $\mathrm{Gal}(F/L_\mathfrak{P}) = G_\mathfrak{P}$. Also ist $\mathfrak{P}$ nach 20.8.1 das einzige über $\mathfrak{P}_L$ liegende Primideal in B.
(2), (3) Sei $\mathfrak{p} \cdot B = \mathfrak{P}^e \cdot \ldots$, $\mathfrak{p} \cdot (B \cap L_\mathfrak{P}) = \mathfrak{P}_L^{e''} \cdot \ldots$ und $\mathfrak{P}_L \cdot B = \mathfrak{P}^e$. Dann folgt $e = e' \cdot e''$.
Ist $C = B \cap L_\mathfrak{P}$, dann haben wir Körpererweiterungen

$$R/\mathfrak{p} \subset C/\mathfrak{P}_L \subset B/\mathfrak{P} \subset B/\mathfrak{P}, \text{ also } \underbrace{f(\mathfrak{P}/\mathfrak{p})}_{=:f} = \underbrace{f(\mathfrak{P}/\mathfrak{P}_L)}_{=:f'} \cdot \underbrace{f(\mathfrak{P}_L/\mathfrak{p})}_{=:f''}$$

nach der Gradschachtelungsformel. Da nun

$$|G_\mathfrak{P}| = [F : L_\mathfrak{P}] = e' \cdot f' \quad \text{ und } \quad |G| = [F:K] = r \cdot e \cdot f \text{ mit } r = \frac{|G|}{|G_\mathfrak{P}|},$$

folgt $e' \cdot f' = e \cdot f$ und damit $e = e'$, $f = f'$. Es folgt $e'' = 1$ und $f'' = 1$. $\square$
Da $\sigma(B) = B$ und $\sigma(\mathfrak{P}) = \mathfrak{P}$ für jedes $\sigma \in G_\mathfrak{P}$, erhalten wir einen Automorphismus

$$\overline{\sigma} : B/\mathfrak{P} \to B/\mathfrak{P}, \quad b + \mathfrak{P} \mapsto \sigma(b) + \sigma(\mathfrak{P}) = \sigma(b) + \mathfrak{P}$$

der Restklassenkörper, d.h. $\overline{\sigma} \in \mathrm{Gal}(B/\mathfrak{P}/R/\mathfrak{p})$.

20.11 Satz: Die Erweiterung $R/\mathfrak{p} \subset B/\mathfrak{P}$ ist normal und $\sigma \mapsto \overline{\sigma}$ definiert einen Epimorphismus

$$G_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(R/\mathfrak{p})).$$

Beweis: Sei $L_{\mathfrak{P}}$ der Fixkörper von $G_{\mathfrak{P}}$. Da $f(\mathfrak{P}_{L_{\mathfrak{P}}}/\mathfrak{p}) = 1$, genügt es, den Fall $K = L_{\mathfrak{P}}$ und $G_{\mathfrak{P}} = G$ zu behandeln.
Sei $\overline{b} \in B/\mathfrak{P}$, sei $f \in K[X]$ das Minimalpolynom von b und $\overline{g} \in (R/\mathfrak{p})[X]$ das Minimalpolynom von $\overline{b}$. Da $\overline{f}(\overline{b}) = \overline{0}$, ist $\overline{g}$ Teiler von $\overline{f}$. Nach 7.17 ist $f \in R[X]$. Da F/K als Galois-Erweiterung normal ist, zerfällt f über F und damit über B in Linearfaktoren; letzteres, weil die Nullstellen von $f \in R[X]$ in B liegen. Folglich zerfällt $\overline{f}$ und damit auch $\overline{g}$ über $B/\mathfrak{P}$ in Linearfaktoren, d.h. $R/\mathfrak{p} \subset B/\mathfrak{P}$ ist normal.
Für den zweiten Teil des Beweises benötigen wir einen neuen Begriff.

20.12 Definition: Sei $K \subset F$ algebraische Körpererweiterung. Dann heißt

$$K^s = \{x \in F;\ x \text{ separabel über } K\}$$

separabler Abschluss von K in F.

Wir machen jetzt eine weitere Anleihe aus der Körper- und Galoistheorie.

20.13 Satz: K^s ist ein Zwischenkörper der Erweiterung $K \subset F$ und

$$\mathrm{Gal}(F/K) \to \mathrm{Gal}(K^s/K), \quad \sigma \mapsto \sigma|K^s$$

ist ein Isomorphismus.

Sei nun $\overline{b}$ ein primitives Element im separablen Abschluss $R/\mathfrak{p}$ in $B/\mathfrak{P}$ und $\overline{\sigma} \in \mathrm{Gal}((B/\mathfrak{P})/(R/\mathfrak{p})) = \mathrm{Gal}((R/\mathfrak{p})(\overline{b})/R(\mathfrak{p}))$.
Dann ist $\overline{\sigma}(\overline{b})$ eine Nullstelle von $\overline{g}$, also auch von $\overline{f}$. Da f über F zerfällt, gibt es eine Nullstelle $b_1 \in F$ von f, so dass $\overline{b}_1 = \overline{\sigma}(\overline{b})$ in $B/\mathfrak{P}$. Da b_1 und b Nullstellen von f sind, gibt es ein $\tau \in \mathrm{Gal}(F/K)$ mit $\tau(b) = b_1$. Es folgt

$$\overline{\tau}(\overline{b}) = \overline{b}_1 = \overline{\sigma}(\overline{b}),$$

also $\overline{\tau} = \overline{\sigma}$, da $\overline{b}$ primitives Element ist. Insbesondere ist $\sigma \mapsto \overline{\sigma}$ surjektiv.

□

20.14 Definition: $I_{\mathfrak{P}} = \mathrm{Kern}(G_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(R/\mathfrak{p}))$ heißt *Trägheitsgruppe* von $\mathfrak{P}$ über K. Der Fixkörper von $I_{\mathfrak{P}}$

$$T_{\mathfrak{P}} := F^{I_{\mathfrak{P}}} = \{x \in F;\ \sigma(x) = x \ \ \forall \sigma \in I_{\mathfrak{P}}\}$$

heißt *Trägheitskörper* von $\mathfrak{P}$ über K.

20.15 Die Inklusionen ($U \triangleleft V$ bedeutet: U ist Normalteiler von V.)

$$\{\mathrm{id}\} \triangleleft I_{\mathfrak{P}} \triangleleft G_{\mathfrak{P}} \subset \mathrm{Gal}(F/K)$$

definieren nach 20.3 einen Turm von Körpern

$$K \subset L_{\mathfrak{P}} \subset T_{\mathfrak{P}} \subset F$$

und wir haben eine exakte Sequenz

$$\{\mathrm{id}\} \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(R/\mathfrak{p})) \to 1.$$

20.16 Satz: $L_{\mathfrak{P}} \subset T_{\mathfrak{P}}$ ist normal, und es gilt

$$\begin{array}{rcl} \mathrm{Gal}(T_{\mathfrak{P}}/L_{\mathfrak{P}}) & \cong & \mathrm{Gal}((B/\mathfrak{P}))/(R/\mathfrak{p})) \\ \mathrm{Gal}(F/T_{\mathfrak{P}}) & \cong & I_{\mathfrak{P}} \end{array}$$

Ist $(R/\mathfrak{p}) \subset B/\mathfrak{P}$ separable Erweiterung, dann gilt

$$I_{\mathfrak{P}} = [F : T_{\mathfrak{P}}] = e, \quad [G_{\mathfrak{P}} : I_{\mathfrak{P}}] = [T_{\mathfrak{P}} : L_{\mathfrak{P}}] = f.$$

In diesem Fall gilt für das untere $\mathfrak{P}$ liegende Primideal $\mathfrak{P}_T$ von $T_{\mathfrak{P}}$:

(1) $e(\mathfrak{P}/\mathfrak{P}_T) = e$, $f(\mathfrak{P}/\mathfrak{P}_T) = 1$

(2) $e(\mathfrak{P}_T/\mathfrak{P}_L) = 1$, $f(\mathfrak{P}_T/\mathfrak{P}_L) = f$

Beweis: Da $T_{\mathfrak{P}} \triangleleft G_{\mathfrak{P}}$, ist $L_{\mathfrak{P}} \subset T_{\mathfrak{P}}$ Galois-Erweiterung nach 20.5, also auch normal, und

$$\mathrm{Gal}(T_{\mathfrak{P}}/L_{\mathfrak{P}}) \cong G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}((B/\mathfrak{P}), (R/\mathfrak{p})).$$

Die zweite Isomorphie folgt aus 20.3.
Wie wir im Beweis von 20.10 gesehen haben, ist $|G_{\mathfrak{P}}| = e \cdot f$. Da $f = [(B/\mathfrak{P})/(R/\mathfrak{p})]$ und $R/\mathfrak{p} \subset B/\mathfrak{P}$ nach Voraussetzung Galois-Erweiterung ist, folgt

$$f = |\,\mathrm{Gal}(B/\mathfrak{P})/(R/\mathfrak{p}))| = \frac{|G_{\mathfrak{P}}|}{|I_{\mathfrak{P}}|}.$$

Es folgt $|I_{\mathfrak{P}}| = e$ und $[G_{\mathfrak{P}} : I_{\mathfrak{P}}] = f$.
Nach Definition gilt:

$$\sigma \in I_{\mathfrak{P}} \iff \sigma \text{ lässt } \mathfrak{P} \text{ fest und } \overline{\sigma} \text{ lässt } R/\mathfrak{p} \text{ fest.}$$

Nach Definition von $T_{\mathfrak{P}}$ gilt:

$$\sigma \in I_{\mathfrak{P}} \iff \sigma(x) = x \quad \forall x \in T_{\mathfrak{P}}.$$

Damit ist $I_{\mathfrak{P}}$ auch die Trägheitsgruppe von $\mathfrak{P}$ über $T_{\mathfrak{P}}$. Wir wenden nun 20.11 auf die Galois-Erweiterung $T_{\mathfrak{P}} \subset F$ an. Die zugehörige Galoisgruppe $\mathrm{Gal}(F/T_{\mathfrak{P}})$ ist $I_{\mathfrak{P}}$, so dass aus 20.15 folgt

$$\mathrm{Gal}((B/\mathfrak{P})/(T_{\mathfrak{P}} \cap B/\mathfrak{P}_T)) = 1.$$

Also $B/\mathfrak{P} \cong T_{\mathfrak{P}} \cap B/\mathfrak{P}_T$. Damit erhalten wir $f(\mathfrak{P}/\mathfrak{P}_T) = 1$. Da $[F : T_{\mathfrak{P}}] = e$, folgt aus der fundamentalen Gleichung $e(\mathfrak{P}/\mathfrak{P}_T) = e$.
Da $e(\mathfrak{P}/\mathfrak{P}_L) = e$, muss nun folgen, dass $e(\mathfrak{P}_T/\mathfrak{P}_L) = 1$. Da $L_{\mathfrak{P}} \subset T_{\mathfrak{P}}$ Galois-Erweiterung vom Grad f ist, folgt $f(\mathfrak{P}_T/\mathfrak{P}_L) = f$. □

20.17 Wir haben folgendes Bild (falls $R/\mathfrak{p} \subset B/\mathfrak{P}$ separabel ist)

Verzweigungsindex		1		1	e	
Erweiterung	K	$\subset$	$L_{\mathfrak{P}}$	$\subset$	$T_{\mathfrak{P}}$	$\subset$ F
Trägheitsgrad		1		f	1	

Weiter gilt: $I_{\mathfrak{P}} = 1 \iff F = T_{\mathfrak{P}} \iff \mathfrak{p}$ ist unverzweigt in F.

21 Zyklotomische Erweiterungen

21.1 Definition: Eine1 *primitive* n-te *Einheitswurzel* in einem Körper K ist ein Element der Ordnung n in $(K^*, \cdot)$. Eine n-te *Einheitswurzel* ist ein Element $a \in K$ mit $a^n = 1$. Man nennt $K \subset \mathrm{Zer}(X^n - 1)$ *zyklotomische Erweiterung* von K.

21.2 Die Menge $\mu_n(K)$ der n-ten Einheitswurzel von K ist eine endliche zyklische Untergruppe von $(K^*, \cdot)$ und $|\mu_n(K)|$ teilt n.

Beweis: $\mu_n(K)$ ist die Menge der Nullstellen von $X^n - 1$ in K und daher endlich. $1 \in \mu_n(K)$ und mit x, y ist auch x^{-1} und xy in $\mu_n(K)$. Also ist $\mu_n(K)$ eine Untergruppe von $(K^*, \cdot)$. Nach 4.21 ist $\mu_n(K)$ zyklisch. Ist a ein Erzeuger, gilt $a^n = 1$, so dass $|\mu_n(K)| = \mathrm{ord}(a)$ Teiler von n ist. □

21.3 Satz: Sei K ein Körper der Charakteristik 0 oder p, wobei $p \nmid n$. Sei $F = \mathrm{Zer}(X^n - 1)$. Dann gilt

(1) F enthält eine primitive n-te Einheitswurzel und $\mu_n(F) = \mathbb{Z}/n$.

(2) Ist ζ n-te primitive Einheitswurzel, so gilt $F = K[\zeta]$.

(3) F/K ist Galois und die Abbildung

$$\begin{array}{rcl} \psi : \mathrm{Gal}(F/K) & \longrightarrow & ((\mathbb{Z}/n)^*, \cdot) \\ \sigma & \longmapsto & \bar{i}, \text{ falls } \sigma(\zeta) = \zeta^i \end{array}$$

ist ein Monomorphismus.

Beweis: (1) $f = X^n - 1$ hat nur einfache Nullstellen, weil $f' = nX^{n-1}$ und n wegen $p \nmid n$ invertierbar ist. Also enthält F genau n verschiedene Einheitswurzeln. Nach 21.2 ist $\mu_n(F) \cong \mathbb{Z}/n$ und jeder Erzeuger von $\mathbb{Z}/n$ entspricht einer primitiven n-te Einheitswurzel.

(2) $K[\zeta]$ enthält ganz $\mu_n(F)$. Es folgt $K[\zeta] = F$.

(3) Sei ζ primitive n-te Einheitswurzel. Alle anderen primitiven n-ten Einheitswuzeln sind dann von der Form ζ^i mit $\mathrm{ggT}(i, n) = 1$, d.h. $\bar{i} \in (\mathbb{Z}/n)^*$.

Ein Automorphismus $\sigma \in \mathrm{Gal}(F/K)$ muss primitive n-te Einheitswurzeln auf primitive n-te Einheitswurzeln abbilden. Also ist $\sigma(\zeta) = \zeta^i$ mit $\bar{i} \in (\mathbb{Z}/n)^*$ und $\tau \circ \sigma(\zeta) = \tau(\zeta^i) = (\tau(\zeta))^i = \zeta^{j \cdot i}$, falls $\tau(\zeta) = \zeta^j$. Also ist ψ ein Homomorphismus.

$$\psi(\sigma) = 1 \iff \sigma(\zeta) = \zeta \iff \sigma = \mathrm{id},$$

da auch $\sigma | K = \mathrm{id}$ und F von K und ζ erzeugt wird. □

21.4 Beispiel: (1) $K = \mathbb{C}$. Dann ist $F = K$, also $\mathrm{Gal}(F/K) = \{id\}$.

(2) $K = \mathbb{R}$ und $n > 2$. Dann ist $F = \mathbb{C}$, $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}] = 2$, also $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2$ erzeugt von $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(x + iy) = x - iy$.

In beiden Fällen ist ψ nicht surjektiv.

21.5 $d | n \Rightarrow X^d - 1 | X^n - 1$.

Denn aus $n = k \cdot d$ folgt

$$X^n - 1 = (X^d)^k - 1 = (X^d - 1) \cdot (X^{d(k-1)} + X^{d(k-2)} + \ldots + X^d + 1).$$

Wir suchen nun nach dem Minimalpolynom einer primitiven Einheitswurzel. 21.5 legt nahe, folgende Polynome zu betrachten.

21.6 Definition: Die Polynome $\Phi_n = \prod (X - \zeta)$, das Produkt läuft über die n-ten primitiven Einheitswurzeln ζ, heißen n-te *Kreisteilungspolynome*.

21.7 (1) $\mathrm{grad}\, \Phi_n = \varphi(n) = |(\mathbb{Z}/n)^*|$

(2) $X^n - 1 = \prod_{d|n} \Phi_d$

(3) Der Leitkoeffizient von Φ_n ist 1.

21.8 Beispiel:
$$\begin{aligned} \Phi_1 &= X - 1 \\ \Phi_2 &= (X^2-1)/(X-1) = X+1 \\ \Phi_3 &= (X^3-1)/\Phi_1 = X^2+X+1 \\ \Phi_4 &= (X^4-1)/\Phi_1 \cdot \Phi_2 = (X^4-1)/(X^2-1) = X^2+1 \end{aligned}$$

Sei F der Zerfällungskörper von $X^n - 1$. Nach Definition ist $\Phi_n \in F[X]$. Die Beispiele lassen aber vermuten, dass $\Phi_n \in \mathbb{Z}[X]$, falls $\operatorname{char} F = 0$, bzw. in $\mathbb{F}_p[X]$, falls $\operatorname{char} F = p$.

21.9 Lemma: $\Phi_n \in \begin{cases} \mathbb{Z}[X] & \text{in Charakteristik } 0 \\ \mathbb{F}_p[X] & \text{in Charakteristik } p > 0 \end{cases}$

Beweis: Es genügt, Charakteristik 0 zu behandeln. Reduzieren wir mod p, erhalten wir den zweiten Teil. Den ersten Teil zeigen wir durch Induktion nach n : $\Phi_1 \in \mathbb{Z}[X]$ und hat Leitkoeffizient 1.

Induktionsschritt: Sei $g = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$. Dann gilt $X^n - 1 = g \cdot \Phi_n$ nach 21.7.

Nach Induktion ist $g \in \mathbb{Z}[X]$ und hat Leitkoeffzient $1 \in \mathbb{Z}^*$. Daher können wir den Divisionalalgorithmus in $\mathbb{Z}[X]$ anwenden und erhalten $\Phi_n \in \mathbb{Z}[X]$ mit Leitkoeffzient 1. □

21.10 Lemma: Sei K ein Körper der Charakteristik 0 oder p mit $p \nmid n$. Sei ζ primitive n-te Einheitswurzel in einer Erweiterung L von K. Dann sind äquivalent

(1) Φ_n ist irreduzibel in $K[X]$.

(2) $[K[\zeta] : K] = \varphi(n)$

(3) $\psi : \operatorname{Gal}(K[\zeta]/K) \to (\mathbb{Z}/n)^*$ aus 21.3 ist ein Isomorphismus.

Beweis: ζ ist Nullstelle von Φ_n. Sei f der normierte irreduzible Faktor von Φ_n, der ζ als Nullstelle hat. Dann ist f das Minimalpolynom von ζ. Es gilt

$$\begin{aligned} [K[\zeta] : K] = \varphi(n) &\iff \operatorname{grad} f = \varphi(n) \iff f = \Phi_n \\ &\iff |\operatorname{Gal}(K[\zeta]/K)| = \varphi(n) \iff \psi \text{ ist bijektiv.} \end{aligned}$$

□

21.11 Satz: Φ_n ist irreduzibel in $\mathbb{Q}[X]$.

Beweis: Sei f ein irreduzibler Faktor von Φ_n. Wir zeigen

(1) ζ Nullstelle von $f \Rightarrow \zeta^i$ Nullstelle von f $\forall i$ mit $\mathrm{ggT}(i,n) = 1$.

Das genügt, denn jede primitive n-te Einheitswurzel ist von der Form ζ^i mit $\mathrm{ggT}(i,n) = 1$. Wir erhalten also $f = \Phi_n$.

Um (1) zu zeigen, genügt der Nachweis von

(2) ζ Nullstelle von $f \Rightarrow \zeta^p$ Nullstelle von f, falls p prim, $p \nmid n$. Denn i aus (1) ist ein Produkt $i = p_1, \ldots, p_k$ solcher Primzahlen. Durch iteriertes Anwenden von (2) (ersetze ζ durch $\zeta^{p_1 \cdots p_k}$) erhält man (1).

Sei also $\Phi_n = f \cdot g$ mit $f, g \in \mathbb{Z}[X]$ und ζ Nullstelle von f. Angenommen ζ^p ist nicht Nullstelle von f, dann ist es Nullstelle von g, so dass $g(\zeta^p) = 0$. Insbesondere ist ζ Nullstelle von $g(X^p)$. Da f das Minimalpolynom von ζ ist, folgt $f | g(X^p)$, d.h.

$$g(X^p) = f \cdot h$$

in $\mathbb{Z}[X]$ (Der Leitkoeffizient von f ist 1, so dass wir in $\mathbb{Z}[X]$ durch f dividieren können). Die Gleichungen

$$\Phi_n = f \cdot g \qquad g(X^p) = f \cdot h$$

gelten auch über $\mathbb{F}_p$ nach Reduktion mod p. Sei $g = \sum_{i=0}^{p} a_i X^i$. Dann gilt mod p

$$g(X)^p = (\sum_{i=0}^{p} a_i X^i)^p = \sum_{i=0}^{r} a_i^p X^{ip} = \sum_{i=0}^{r} a_i (X^p)^i = g(X^p)$$

Es folgt

$$(g(X))^p = f \cdot h \qquad \text{in } \mathbb{F}_p[X].$$

Da $\mathbb{F}_p[X]$ euklidisch ist, können wir beide Seiten eindeutig in Primfaktoren zerlegen. Ist $u \in \mathbb{F}_p[X]$ ein Primfaktor von f, so ist u auch Teiler von g. Es folgt $u^2 | \Phi_n$ in $\mathbb{F}_p[X]$. Insbesondere hat Φ_n in seinem Zerfällungskörper über $\mathbb{F}_p[X]$ mehrfache Nullstellen. Wie wir aber im Beweis von 21.3 gesehen haben, hat $X^n - 1$ und damit auch Φ_n nur einfache Nullstellen. □

21.12 Satz: Der Fall Charakteristik $\mathbf{p \nmid n}$:

21.13 Beispiel: Φ_4 ist reduzibel in $\mathbb{F}_5[X]$, denn in $\mathbb{F}_E[X]$ gilt

$$X^2 + 1 = (X + 3) \cdot (X + 2).$$

Das Beispiel zeigt, dass Φ_n über $\mathbb{F}_p$ reduzibel sein kann.

Sei ζ primitive n-te Einheitswurzel und $f \in \mathbb{F}_p[X]$ das Minimalpolynom von ζ. Da $\Phi_n(\zeta) = 0$, folgt $f | \Phi_n$.

21.14 Satz: Sei p prim, $p \nmid n$ und sei $e = \operatorname{ord}(\overline{p})$ in $(\mathbb{Z}/n)^*$. Dann hat jeder irreduzible Faktor f von Φ_n in $\mathbb{F}_p[X]$ den Grad e. Also hat Φ_n genau $\frac{\varphi(n)}{e}$ irreduzibel Faktoren und

$$[\mathbb{F}_p[\zeta] : \mathbb{F}_p] = e.$$

Beweis: Sei ζ primitive n-Einheitswurzel, $F = \mathbb{F}_p[\zeta]$ ist der Zerfällungskörper von Φ_n nach 21.3. Sei f das Minimalpolynom von ζ, $\operatorname{grad} f = m$. Dann gilt $\dim_{\mathbb{F}_p}(F) = \operatorname{grad} f = m$, also

$$|F| = p^m.$$

Damit ist ζ Nullstelle von $X^{p^m} - X$ (s. Einführung in die Algebra), so dass $\zeta^{p^m-1} = 1$. Da $\operatorname{ord}(\zeta) = n$ in F^*, folgt $n | p^m - 1$, also

$$p^m \equiv 1 \mod n.$$

Da $p \nmid n$, ist $p \in (\mathbb{Z}/n)^*$. Sei $e = \operatorname{ord}(p)$ in $(\mathbb{Z}/n)^*$. Dann folgt

$$e|m, \quad p^e \equiv 1 \mod n, \quad \zeta^{p^e} = \zeta \qquad (*)$$

letzteres, weil $p^e \equiv 1 \mod n$ und $\zeta^n = 1$.
Nach 4.3 ist $\{1, \zeta, \zeta^2, \ldots \zeta^{m-1}\}$ eine Basis von F. Sei $y \in F^* \cong \mathbb{Z}/p^m - 1$ ein Erzeuger und

$$y = \sum_{i=0}^{m-1} c_i \zeta^i \quad c_i \in \mathbb{F}_p.$$

seine Darstellung als Linearkombination der Basiselemente. Dann gilt

$$y^{p^e} = \left(\sum_{i=0}^{m-1} c_i \cdot \zeta^i \right)^{p^e} = \sum_{i=0}^{m-1} c_i^{p^e} \cdot \zeta^{ip^e} = \sum_{i=0}^{m-1} c_i \cdot \zeta^i = y$$

weil $c^p = c$ in $\mathbb{F}_p$ nach dem kleinen Fermat'schen Satz und $\zeta^{p^e} = \zeta$. Es folgt

$$\operatorname{ord} y = p^m - 1 | p^e - 1, \quad \text{also } e = m \text{ wegen } (*)$$

Also hat f den Grad e. □

21.15 Beispiel: $\operatorname{ord} \overline{5}$ in $(\mathbb{Z}/4)^*$ ist 1 und $\varphi(4) = 2$. Also zerfällt Φ_4 in zwei irreduzible Faktoren über $\mathbb{F}_5$.

22 Der Ring der ganzen Zahlen in $\mathbb{Q}(\zeta)$

Wie wir schon früher erwähnten, spielen Kreisteilungskörper in der algebraischen Zahlentheorie eine wichtige Rolle. Wir wollen jetzt ihre Ringe der ganz Zahlen untersuchen.

Im Folgenden sei l eine Primzahl, $n = l^r$ eine Potenz von l, ζ primitive n-te Einheitswurzel und $K = \mathbb{Q}(\zeta)$. Für die Bestimmung von $\mathcal{O}_K$ benötigen wir

22.1 Satz: Sei $\lambda = 1 - \zeta$. Dann ist $(\lambda) = \mathcal{O}_K \cdot \lambda$ ein Primideal in $\mathcal{O}_K$ vom Trägheitsgrad 1, und es gilt

(1) $l \cdot \mathcal{O}_K = (\lambda)^d$ mit $d := \varphi(l^r) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, insbesondere ist $l \cdot \mathcal{O}_K$ voll zerlegt.

(2) $D_{K/\mathbb{Q}}(1, \zeta, \zeta^2, \ldots, \zeta^{d-1}) = \pm l^s$ mit $s = l^{r-1}(rl - r - 1)$.

Wir suchen zunächst das l^r-te Kreisteilungspolynom Φ_{l^r}.

22.2 Lemma: Für $n = l^r$ gilt

$$\Phi_n = (X^{l^{r-1}})^{l-1} + (X^{l^{r-1}})^{l-2} + \ldots + (X^{l^{r-1}}) + 1$$

Beweis: $X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \cdot \prod_{\substack{d|n \\ d \neq n}} \Phi_d = \Phi_n \cdot \left(X^{l^{r-1}-1}\right)$. Also

$$\Phi_n = \frac{X^{l^r} - 1}{X^{l^{r-1}} - 1} = \frac{(X^q)^l - 1}{X^q - 1} = (X^q)^{l-1} + (X^q)^{l-2} + \ldots + X^q + 1 \text{ mit } q = l^{r-1}$$

□

Beweis 22.1: Da $\Phi_n = \prod_{\eta}(X - \eta)$, wobei η alle primitiven n-ten Einheitswurzeln durchläuft, gilt

$$\Phi_n = \prod_{k \in (\mathbb{Z}/n)^*} (X - \zeta^k).$$

Setzen wir $X = 1$, erhalten wir mit 21.10

$$l = \prod_{k \in (\mathbb{Z}/n)^*} (1 - \zeta^k) \qquad (*)$$

Behauptung: Für $k \in (\mathbb{Z}/n)^*$ ist $\frac{1-\zeta^k}{1-\zeta} =: \varepsilon_k \in \mathcal{O}_K^*$.

Beweis: $\frac{1-\zeta^k}{1-\zeta} = 1+\zeta+\zeta^2+\ldots\zeta^{k-1} \in \mathcal{O}_K$. Sei nun $m \in \mathbb{N}$ eine Zahl, so dass $m \cdot k \equiv 1 \mod n$ (m existiert, da $k \in (\mathbb{Z}/n)^*$), dann gilt

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-\zeta^{m\cdot k}}{1-\zeta^k} = 1+\zeta^k+\zeta^{2k}+\ldots+\zeta^{k(m-1)} \in \mathcal{O}_K.$$

Also ist ε_k in $\mathcal{O}_K$ invertierbar.
Es folgt $1-\zeta^k = \varepsilon_k \cdot (1-\zeta)$ und $l = \varepsilon \cdot (1-\zeta)^{\varphi(n)}$ mit $\varepsilon = \prod_k \varepsilon_k \in \mathcal{O}_K^*$. Wir erhalten

$$l \cdot \mathcal{O}_K = (1-\zeta)^{\varphi(n)} \cdot \mathcal{O}_K = (\lambda)^{\varphi(n)}.$$

Mit der fundamentalen Gleichung 18.8 folgt (1), da (λ) nicht weiter zerlegt werden kann.
Seien nun $\zeta = \zeta_1,\ \zeta_2, \ldots,\ \zeta_d$ alle primitiven n-ten Einheitswurzeln, wobei $d = (l-1)\cdot l$, dann gilt nach 9.8

$$D_{K/\mathbb{Q}}(1,\zeta,\ldots,\zeta^{d-1}) = (-1)^t \cdot N_{K/\mathbb{Q}}(\Phi_n'(\zeta)) \qquad t = d \cdot \frac{d-1}{2}.$$

Differenzieren wir $(X^{l^{r-1}}-1)\cdot\Phi_n(X) = \left(X^{l^r}-1\right)$, erhalten wir

$$l^{r-1}\cdot X^{l^{r-1}-1}\cdot\Phi_n + \left(X^{l^{r-1}}-1\right)\Phi_n' = l^r \cdot X^{l^r-1}.$$

Setzen wir ζ ein und nehmen $\eta = \zeta^{l^{r-1}}$, ergibt dies

$$(\eta-1)\cdot\Phi_n'(\zeta) = l^r\cdot\zeta^{-1},$$

da $\Phi_n(\zeta) = 0$ ist. Da η eine primitive l-te Einheitswurzel ist, erhalten wir aus $(*)$ für den Fall $r = 1$

$$N_{\mathbb{Q}(\eta)/\mathbb{Q}}(\eta-1) = \prod_{k\in(\mathbb{Z}/l)^*}(\eta^k-1) = \pm l$$

(die Einbettungen $\mathbb{Q}(\eta)\to\mathbb{C}$ sind durch $\eta\mapsto\eta^k$, $k\in(\mathbb{Z}/l)^*$, gegeben). Da $\zeta^{-1} = \zeta^{d-1} \in \mathcal{O}_K$ eine Einheit ist, ist $N_{K/\mathbb{Q}}(\zeta) = \pm 1$. Nach 8.6 gilt

$$N_{K/\mathbb{Q}}(\eta-1) = (N_{\mathbb{Q}(\eta)/\mathbb{Q}}(\eta-1))^m \quad \text{mit} \quad m = [\mathbb{Q}(\zeta):\mathbb{Q}(\eta)] = l^{r-1}$$

Es folgt

$$D_{K/\mathbb{Q}}(1,\zeta,\ldots,\zeta^{d-1}) = \pm N_{K/\mathbb{Q}}(\Phi_n'(\zeta)) = \pm\frac{l^{r_d}\cdot(\pm 1)}{(\pm l)^{l^{r-1}}} = \pm l^{rd-l^{r-1}} = \pm l^s$$

mit $s = rd - l^{r-1} = r\cdot(l-1)l^{r-1} - l^{r-1} = l^{r-1}(rl-r-1)$. □

Bevor wir fortfahren, eine kurze Bemerkung zur *Euler'schen φ-Funktion*

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad \varphi(n) = |(\mathbb{Z}/n)^*|.$$

Ist p prim, dann sind

$$p, 2p, \ldots, p^{r-1} \cdot p$$

genau die Elemente $x \leq p^r$ aus $\mathbb{N}$ mit $\mathrm{ggT}(x, p^r) \neq 1$. Es folgt

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1).$$

Ist $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ die Primfaktorzerlegung von n, dann folgt aus dem chinesischen Restesatz

$$(\mathbb{Z}/n)^* \cong (\mathbb{Z}/p_1^{r_1})^* \times \ldots \times (\mathbb{Z}/p_k^{r_k})^*,$$

und damit $\varphi(n) = \varphi(p_1^{r_1}) \cdot \ldots \cdot \varphi(p_k^{r_k})$.

22.3 $\varphi(n) = \prod_{i=1}^k (p_i^{r_i-1} \cdot (p_i - 1)) = n \cdot \prod_{i=1}^k (1 - \frac{1}{p_i})$

Ist $n \equiv 2 \mod 4$, dann ist $n = 2m$ mit ungeradem m. Ist ζ eine primitive m-te Einheitswurzel, dann ist $-\zeta$ eine n-te Einheitswurzel, aber $\mathbb{Q}(-\zeta) = \mathbb{Q}(\zeta)$. Deshalb setzen wir ab jetzt stets voraus, dass $n \not\equiv 2 \mod 4$.

22.4 Satz: Sei $n = l_1^{r_1} \cdot \ldots \cdot l_k^{r_k}$ die Primfaktorzerlegung von $n \in \mathbb{N}$ und $n \not\equiv 2 \mod 4$. Sei ζ primitive n-te Einheitswurzel. Sei $\zeta_i = \zeta^{n_i}$ mit $n_i = n/l_i^{r_i}$. Sei $K = \mathbb{Q}(\zeta)$, $K_i = \mathbb{Q}(\zeta_i)$ und $\delta_i = \delta_{K_i} = \mathrm{disc}(\mathcal{O}_{K_i}/\mathbb{Z})$. Dann gilt

(1) $\delta_K = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \delta_1^{\varphi(n_1)} \cdot \ldots \cdot \delta_k^{\varphi(n_k)}$

(2) $\{1, \zeta, \zeta^2, \ldots, \zeta^{d-1}\}$ mit $d = \varphi(n)$ ist Ganzheitsbasis von $\mathcal{O}_K$, also $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Beweis: Induktion nach k.
Fall $k = 1$: Dann ist $n = l^r$ mit l prim. Nach 10.3 und 21.10 gilt

$$\delta \cdot \mathcal{O}_K \subset \mathbb{Z}[\zeta] \subset \mathcal{O}_K \quad \text{mit} \quad \delta = D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s.$$

Es folgt $l^s \cdot \mathcal{O}_K \subset \mathbb{Z}[\zeta]$. Sei wieder $\lambda = 1 - \zeta$. Da (λ) den Trägheitsgrad 1 hat, gilt $\mathcal{O}_K/(\lambda) \cong \mathbb{Z}/l$, also

$$\mathcal{O}_K = \mathbb{Z} + \lambda \cdot \mathcal{O}_K \quad \text{und damit} \quad \mathcal{O}_K = \lambda \cdot \mathcal{O}_K + \mathbb{Z}[\zeta],$$

also auch

$$\mathcal{O}_K = \lambda(\lambda \cdot \mathcal{O}_K + \mathbb{Z}[\zeta]) + \mathbb{Z}[\zeta] = \lambda^2 \mathcal{O}_K + \mathbb{Z}[\zeta]$$

und damit

$$\mathcal{O}_K = \lambda^t \cdot \mathcal{O}_K + \mathbb{Z}[\zeta] \quad \forall t \geq 1.$$

Für $t = s \cdot d$, $d = \varphi(l^r)$, erhalten wir

$$\mathcal{O}_K = (\lambda \cdot \mathcal{O}_K)^{d \cdot s} + \mathbb{Z}[\zeta] = l^s \cdot \mathcal{O}_K + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$$

Induktionsschritt: Sei n wie im Satz und $m = l_1^{r_1} \cdot \ldots \cdot l_1^{r_{k-1}} = n_k$. Da $\text{ord}(\zeta_1 \cdot \ldots \cdot \zeta_{k-1}) = m$, ist $\eta = \zeta_1 \cdot \ldots \cdot \zeta_{k-1}$ eine primitive m-te Einheitswurzel. Es gilt

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1, \ldots, \zeta_k) = \mathbb{Q}(\eta)(\zeta_k)$$

und wir erhalten ein Diagramm von Körpern

$$\begin{array}{ccc} \mathbb{Q} & \subset & Q(\eta) \\ \cap & & \cap \\ \mathbb{Q}(\zeta_k) & \subset & Q(\zeta) \end{array}$$

und $\mathbb{Q}(\zeta_k)$ ist der kleinste Teilkörper von $\mathbb{C}$, der $Q(\eta)$ und $\mathbb{Q}(\zeta_k)$ enthält. Sei $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_k)) = \{\sigma_1, \ldots, \sigma_p\}$ und $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\eta)) = \{\tau_1, \ldots, \tau_q\}$, $p = \varphi(m)$ und $q = \varphi(l_k^{r_k})$. Dann ist

$$\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) = \{\sigma_i \circ \tau_j;\ 1 \leq i \leq p, 1 \leq j \leq q\}$$

Nach Induktion und dem Fall $k = 1$ ist $\{\alpha_1, \ldots, \alpha_p\}$ mit $\alpha_i = \eta^{i-1}$ ganze Basis von $\mathbb{Q}(\eta)$ und $\{\beta_1, \ldots, \beta_q\}$ mit $\beta_i = \zeta_k^{i-1}$ ganze Basis von $\mathbb{Q}(\zeta_k)$. Also ist $\mathcal{B} = \{\alpha_i \cdot \beta_j;\ 1 \leq i \leq p, 1 \leq j \leq q\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta)$ und damit eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\eta, \zeta_k]$. Da $\eta \cdot \zeta_k$ eine primitiver n-te Einheitswurzel ist, gilt $\mathbb{Z}[\eta, \zeta_k] = \mathbb{Z}[\zeta]$.
Sei jetzt $a \in \mathbb{Q}(\zeta)$ ganz über $\mathbb{Q}$ und

$$a = \sum_{i,j} r_{ij} \alpha_i \beta_j \quad \text{mit } r_{ij} \in \mathbb{Q}.$$

Wir müssen zeigen, dass die $r_{ij} \in \mathbb{Z}$ sind. Dann folgt, dass $\mathbb{Q}_K = \mathbb{Z}[\zeta]$. Da $\{1, \zeta, \ldots, \zeta^{d-1}\}$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\zeta]$ ist, wäre Teil (2) gezeigt.
Wir setzen

$$\begin{array}{rcl} y_j = \sum\limits_i r_{ij} \alpha_i & \text{und} & y = (y_1, \ldots, y_q)^t \\ x_i = \tau_i(a) = \sum\limits_{s,j} r_{sj} \tau_i(\alpha_s \beta_j) = \sum\limits_{s,j} r_{sj} \alpha_s \tau_i(\beta_j) = \sum\limits_j \tau_i(\beta_j) y_j & & \\ x = (x_1, \ldots, x_q)^t & \text{und} & T = (\tau_s \beta_j)_{s,j} \end{array}$$

Es folgt nach 9.5

$$(\det T)^2 = \delta_k \quad \text{und} \quad x = T \cdot y.$$

Ist T^* die adjungiert Matrix, gilt nach dem Laplace'schen Entwicklungssatz

$$T^* \cdot T = \det(T) \cdot E_q \quad \text{also} \quad \det(T) \cdot y = T^* \cdot T \cdot y = T^* \cdot x.$$

Mit β_j sind auch die $\tau_s(\beta_j)$ ganz über $\mathbb{Z}$. Also sind die Einträge von T^* und T ganz. Da a ganz ist, gilt dasselbe für die Koordinaten von x und damit von $\det(T) \cdot y$. Da auch $\det(T)$ ganz und $\delta_k \in \mathbb{Z}$, ist

$$\delta_k \cdot y_j = \sum_i \delta_k r_{ij} \alpha_i \in \mathbb{Q}(\eta) =: L$$

ganz. Da die α_i eine ganze Basis von $\mathbb{Q}(\eta)$ bilden, folgt

$$\delta_k \cdot r_{ij} \in \mathbb{Z} \quad \text{für alle } i, j.$$

Jetzt vertauschen wir die Rollen von $\mathbb{Q}(\eta)$ und $\mathbb{Q}(\zeta_k)$ und erhalten unter Ausnutzung der Induktionsannahme mit $\delta' = \operatorname{disc}(\mathcal{O}_L/\mathbb{Z})$

$$\delta' \cdot r_{ij} \in \mathbb{Z} \quad \text{für alle } i, j.$$

Nach 22.1 sind δ_k und δ' teilerfremd, so dass es $u, v \in \mathbb{Z}$ gibt mit

$$r_{ij} = (u \cdot \delta_k + v \cdot \delta') \cdot r_{ij} = u \cdot \delta_k \cdot r_{ij} + v \cdot \delta' \cdot r_{ij} \in \mathbb{Z}$$

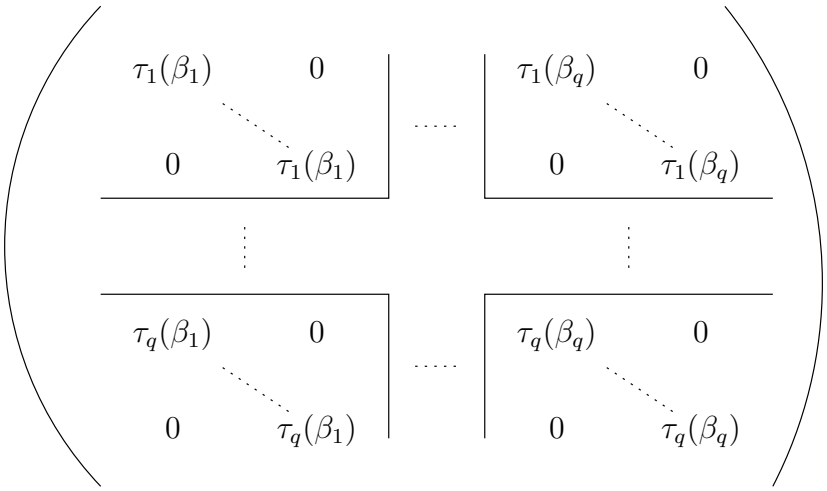
Zum Beweis von Teil (1) genügt es, die Diskriminate von $\mathcal{B}$ zu berechnen. Sie ist das Quadrat der Determinante der $(p \cdot q \times p \cdot q)$-Matrix $M = (\sigma_i \circ \tau_j(\alpha_s \cdot \beta_t))$. Wir fassen M als $(q \times q)$-Matrix von $(p \times p)$-Matrizen auf: Ihr (j,t)-ter Eintrag ist die Matrix $Q \cdot \tau_j(\beta_t)$ mit $Q = (\sigma_i(\alpha_s))_{i,s}$. Es folgt $M = A \cdot B$ mit

$$A = \begin{pmatrix} Q & & 0 \\ & Q & \\ & \ddots & \\ 0 & & Q \end{pmatrix} \quad B = \begin{pmatrix} E_p \cdot \tau_1(\beta_1), \ldots, E_p \cdot \tau_1(\beta_q) \\ \vdots \qquad\qquad \vdots \\ E_p \cdot \tau_q(\beta_1), \ldots, E_p \cdot \tau_q(\beta_q) \end{pmatrix}$$

und jeder Eintrag in A und B ist eine $(k \times k)$-Matrix. Es folgt

$$\det(M)^2 = \det(A)^2 \cdot \det(B)^2 = (\det(Q)^q)^2 \cdot \det(B)^2 = \delta'^q \cdot \det(B)^2.$$

B ist eine $(p \cdot q \times p \cdot q)$-Matrix der Form



Durch Zeilen- und Spaltenvertauschungen, können wir sie in die Form

$$B' = \begin{pmatrix} C & & \\ & \ddots & 0 \\ 0 & & C \end{pmatrix} \quad \text{mit } C = (\tau_j(\beta_t))_{j,t}$$

überführen. Es folgt

$$\det(B)^2 = (\pm \det(B')^2 = (\det(C)^p)^2 = \delta_k^p.$$

Es folgt $\delta := \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = (\delta')^{\varphi(l_k^{r_k})} \cdot \delta_k^{\varphi(m)}$.
Wir erinnern daran, dass $m = n_k$ und nach Induktion mit $m_i = m/l_i^{r_i}$ gilt

$$\delta' = \delta_1^{\varphi(m_1)} \cdot \ldots \cdot \delta_{k-1}^{\varphi(m_{k-1})}.$$

Da $\varphi(m_i) \cdot \varphi(l_k^{r_k}) = \varphi(n_i)$, erhalten wir die Aussage (1). □
Als nächstes studieren wir die Zerlegungen eines Primideals $(p) \subset \mathbb{Z}$ in $\mathcal{O}_K$.

22.5 Satz: Sei $n = \prod_p p^{r_p}$ die Primfaktorzerlegung von $n \in \mathbb{N}$, $n \not\equiv 2 \bmod 4$. Sei k_p die Ordnung der Restklasse von p in $(\mathbb{Z}/m)^*$ mit $m = n/p^{r_p}$. Sei ζ primitive n-te Einheitswurzel und $K = \mathbb{Q}(\zeta)$. Dann gilt in $\mathcal{O}_K$

$$p \cdot \mathcal{O}_K = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s)^{\varphi(p^{r_p})} \quad \text{mit } s = \varphi(m)/k_p,$$

wobei $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s$ verschiedene Primideale vom Trägheitsgrad k_p sind.

Beweis: Da $\mathcal{O}_K = \mathbb{Z}[\zeta]$, ist der Führer von $\mathbb{Z}[\zeta]$ der Ring $\mathcal{O}_K$. Wir können daher 18.12 auf jedes Primideal (p), $p \neq 0$, anwenden. Danach zerfällt $p \cdot \mathcal{O}_K$ auf gleiche Weise in Primfaktoren wie das Kreisteilungspolynom Φ_n in $\mathbb{F}_p[X]$. Sei $m = n/p^{r_p}$, so dass $\mathrm{ggT}(m,p) = 1$. Durchläuft ξ_i die primitiven m-ten und η_j die primitiven p^{r_p}-ten Einheitswurzeln, dann durchlaufen $\xi_i \cdot \eta_j$ alle primitiven n-ten Einheitswurzeln, so dass

$$\Phi_n = \prod_{ij}(X - \xi_i\eta_j)$$

$f = X^{p^{r_p}} - 1$ zerfällt über $\mathcal{O}_K$ in Linearfaktoren $f = \prod(X - \rho_t)$, wobei ρ_t **alle** p^{r_p}-ten Einheitswurzeln durchläuft. Sei jetzt $\mathfrak{p} \subset \mathcal{O}_K$ ein Ideal über (p). Dann zerfällt $\overline{f}$ über $\mathcal{O}_K/\mathfrak{p}$ in Linearfaktoren. Da $f \in \mathbb{Z}[X]$ ist, ist $\overline{f} \in \mathbb{Z}[X]/\mathfrak{p} \cap \mathbb{Z}[X] = \mathbb{Z}/p[X]$. Aber

$$\overline{f} = (X-1)^{p^{r_p}} \text{ in } \mathbb{Z}/p[X].$$

Da $\mathcal{O}_K/\mathfrak{p}$ ein Körper ist, sind die Nullstellen von $\overline{f}$ in $\mathcal{O}_K/\mathfrak{p}$ alle 1, liegen also bereits in $\mathbb{Z}/p \subset \mathcal{O}_K/\mathfrak{p}$. Insbesondere gilt

$$\eta_j \equiv 1 \mod \mathfrak{p}$$

und damit

$$\Phi_n = \prod_i (X - \xi_i)^{\varphi(p^{r_p})} = \Phi_m^{\varphi(p^{r_p})} \quad \text{in } (\mathcal{O}_K)/\mathfrak{p}[X].$$

Da die Koeffizienten dieser Polynome in $\mathbb{Z}/p$ liegen, gilt die Gleichung auch über $\mathbb{Z}/p$. Da nun $p \nmid m$, zerfällt Φ_m nach 21.14 in $\varphi(m)/k_p$ irreduzibel Faktoren vom Grad k_p über $\mathbb{Z}/p$. Da Φ_m keine Mehrfachnullstellen hat (der Beweis ist dem Leser überlassen), sind die irreduziblen Faktoren verschieden. Wir erhalten

$$\Phi_n = (f_1 \cdot \ldots \cdot f_s)^t \text{ über } \mathbb{Z}/p \text{ mit } s = \frac{\varphi(m)}{k_p},\ t = \varphi(p^{r_p}),\ p^{r_p} \cdot m = n.$$

□

22.6 Bemerkung: Aus 18.12 erhalten wir mit den Bezeichnungen des Satzes 22.5 und seines Beweises

$$\mathfrak{p}_i = p \cdot \mathcal{O}_K + f_i(\zeta) \cdot \mathcal{O}_K.$$

22.7 Folgerung: Sei $n > 0$ beliebig, $n \not\equiv 2 \mod 4$, und ζ eine primitive n-te Einheitswurzel. Dann gilt

(1) Ist $p \neq 2$, dann ist p genau dann in $\mathbb{Q}(\zeta)$ verzweigt, wenn

$$n \equiv 0 \mod p.$$

(2) 2 ist genau dann in $\mathbb{Q}(\zeta)$ verzweigt, wenn $4 \mid n$.

(3) $p \neq 2$ ist genau dann voll zerlegt in $\mathbb{Q}(\zeta)$, wenn

$$p \equiv 1 \mod n.$$

Beweis: Für jede Primzahl p gilt $\varphi(p^r) = (p-1)p^{r-1}$. Daraus folgen (1) und (2).
p ist genau dann voll zerlegt, wenn $\varphi(p^{r_p}) = 1 = k_p$ ist. Nun ist $\varphi(p^{r_p}) = 1$ genau dann 1, wenn $p \nmid n$ und damit $m = n/pr_p = n$ ist. Weiter ist $k_p = 1$ genau dann, wenn $p \equiv 1 \mod m$, also $p \equiv 1 \mod n$ ist. □

23 Das Gauß'sche Reziprozitätsgesetz

Das Gauß'sche Reziprozitätsgesetz ist eng mit den Zerlegungen von Primzahlen in Kreisteilungskörpern und quadratischen Erweiterungen verbunden. Entdeckt wurde es bei Untersuchungen der Lösbarkeit der diophantischen Gleichung.

$$x^2 + by = a \quad a, b \in \mathbb{Z}$$

in $\mathbb{Z} \times \mathbb{Z}$. Diese Frage lässt sich auf das Problem der Lösbarkeit von Kongruenzen des Typs

23.1 $x^2 \equiv a \mod p$,

$p \nmid a$, reduzieren. Gibt es ein solches x, nennt man a *quadratischen Rest* mod p. Der Fall $p = 2$ wird gesondert behandelt. Wir beschäftigen uns hier mit dem Fall $p \neq 2$.

23.2 Definition: Sei $p \neq 2$ prim, $a \in \mathbb{Z}$, $p \nmid a$. Das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ ist wie folgt definiert

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{23.1 hat eine Lösung } x \in \mathbb{Z} \\ -1 & \text{sonst} \end{cases}$$

23.3 Das Legendre-Symbol definiert einen Epimorphismus

$$\mathbb{F}_p^* = (\mathbb{Z}/p)^* \to \{\pm 1, \cdot\} \cong \mathbb{Z}/2, \quad \overline{a} \mapsto \left(\frac{a}{p}\right)$$

mit Kern $\mathbb{F}_p^{*2} = \{x^2;\ x \in \mathbb{F}_p^*\}$.

Beweis: $p \nmid a \iff \overline{a} \in \mathbb{F}_p^*$. Wie wir bereits gesehen haben, enthält $\mathbb{F}_p^*$ genau $\frac{p-1}{2}$ Quadrate. Damit ist $\mathbb{F}_p^{*2} \subset \mathbb{F}_p^*$ eine Untergruppe vom Index 2, und die beiden Nebenklassen sind die Quadrate und die Nicht-Quadrate. Das Legendre-Symbol kann daher als die Projektionsabbildung $\mathbb{F}_p^* \mapsto \mathbb{F}_p^*/\mathbb{F}_p^{*2}$ interpretiert werden. □

23.4 $p \neq 2$ prim, $p \nmid a$. Dann gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Beweis: $\mathbb{F}_p^*$ ist zyklisch von der Ordnung $p-1$. Also ist $a^{p-1} \equiv 1 \mod p$ und somit $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Die Zuordnung $\overline{a} \mapsto \overline{a}^{\frac{p-1}{2}}$ definiert einen Epimorphismus $\mathbb{F}_p^* \to \{\pm 1, \cdot\}$, dessen Kern die Quadrate enthält. Also ist der Kern genau die Menge der Quadrate. □

23.5 Satz: Sei $m \in \mathbb{Z}$ quadratfrei und p prim, so dass $p \nmid 2m$. Dann gilt:

$$\left(\frac{m}{p}\right) = 1 \iff p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{m}).$$

Beweis: Sei $K = \mathbb{Q}(\sqrt{m})$ und sei $\mathfrak{F}$ der Führer von $\mathbb{Z}[\sqrt{m}]$. Ist $m \not\equiv 1 \mod 4$, so ist $\{1, \sqrt{m}\}$ ganze Basis von $\mathcal{O}_K$ (vergl. 10.12) und $\mathfrak{F} = \mathcal{O}_K$. Ist $m \equiv 1 \mod 4$, so ist $\{1, \frac{1+\sqrt{m}}{2}\}\}$ ganze Basis von $\mathcal{O}_K$, also $(2) \subset \mathfrak{F}$, denn das Ideal $\mathcal{O}_K \cdot 2$ liegt in $\mathbb{Z}[\sqrt{m}]$. Es folgt $\mathfrak{F}|(2)$ in $\mathcal{O}_K$.
Ist $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, so dass $\mathfrak{p}|\mathfrak{F}$, so folgt $\mathfrak{p}|(2)$, also $\mathfrak{p} \cap \mathbb{Z} = (2)$.
Nach Voraussetzung ist $p \neq 2$. Also können wir Satz 18.12 anwenden:
$f = X^2 - m$ ist das Minimalpolynom von $\sqrt{m}$. Es gilt

$$\begin{aligned}
\left(\frac{m}{p}\right) = 1 \quad &\iff \quad x^2 \equiv m \mod p \text{ hat Lösungen } \pm\alpha \\
&\iff \quad \overline{f} = (X-\alpha)(X+\alpha) \text{ in } \mathbb{Z}/p[X] \\
&\iff \quad p \cdot \mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \text{ mit } \mathfrak{p}_1 \neq \mathfrak{p}_2 \text{ prim } 18.12 \\
&\iff \quad p \text{ voll zerlegt.}
\end{aligned}$$

Da $[K : \mathbb{Q}] = 2$, sind die Trägheitsgrade der $\mathfrak{p}_i$ gleich 1. □

23.6 Gauß'sches Reziprozitätsgesetz: Sind $p \neq l$ ungerade Primzahlen, dann gilt

$$\left(\frac{l}{p}\right) \cdot \left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2} \cdot \frac{p-1}{2}}.$$

Weiter gelten die Ergänzungen

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

Die erste Ergänzung folgt aus 23.4. Für die zweite Ergänzung rechnen wir in $\mathbb{Z}[i] \subset \mathbb{Q}(\sqrt{-1})$. Dort gilt

$$\begin{aligned}(1+i)^2 &= 1+2i-1 = 2i \\ (1+i)^p &= (1+i)((1+i)^2)^{\frac{p-1}{2}} \\ &= (1+i)\cdot i^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \\ &\equiv (1+i)\cdot\left(\tfrac{2}{p}\right)\cdot i^{\frac{p-1}{2}} \mod p\end{aligned}$$

Da aber $(1+i)^p \equiv 1+i^p \mod p$, folgt

$$1+i\cdot(-1)^{\frac{p-1}{2}} = 1+i^p \equiv (1+i)^p \equiv (1+i)\cdot i^{\frac{p-1}{2}}\cdot\left(\frac{2}{p}\right) \mod p.$$

1. Fall: $p = 4k+1$. Wir erhalten

$$1+i\cdot(-1)^{2k} = 1+i \equiv (1+i)\cdot(-1)^k\cdot\left(\frac{2}{p}\right).$$

Für den Realteil folgt $1 \equiv (-1)^k\cdot\left(\frac{2}{p}\right)$. Da $(-1)^k\cdot\left(\frac{2}{p}\right) = \pm 1$, folgt $\left(\frac{2}{p}\right) = (-1)^k = (-1)^{\frac{p^2-1}{8}}$, denn $\frac{p^2-1}{8} = \frac{16k^2-8k}{8} \equiv k \mod 2$.

2. Fall: $p = 4k+3$, also $\frac{p-1}{2} = 2k+1$. Wir erhalten

$$1-i \equiv (1+i)\cdot i\cdot(-1)^k\cdot\left(\frac{2}{p}\right) = (i-1)\cdot(-1)^k\left(\frac{2}{p}\right).$$

Wie im ersten Fall folgt $\left(\frac{2}{p}\right) = (-1)^{k+1} = (-1)^{\frac{p^2-1}{8}}$, denn $\frac{p^2-1}{8} = \frac{16k^2-24k+8}{8} = 2k^2+3k+1 \equiv k+1 \mod 2$.

Für den Beweis des Hauptteils zeigen wir zunächst

23.7 Definition und Satz: Sei $l \neq 2$ prim und ζ eine primitive l-te Einheitswurzel.

$$\tau = \sum_{a\in(\mathbb{Z}/l)^*}\left(\frac{a}{l}\right)\cdot\zeta^a$$

heißt *Gauß'sche Summe*. Es gilt: $\tau^2 = \left(\frac{-1}{l}\right)\cdot l = (-1)^{\frac{l-1}{2}}\cdot l$.

Beweis:

$$\left(\frac{-1}{l}\right)\cdot\tau^2 = \sum_{a,b\in(\mathbb{Z}/l)^*}\left(\frac{a}{l}\right)\left(\frac{b}{l}\right)\left(\frac{-1}{l}\right)\zeta^{a+b} \overset{(1)}{=} \sum_{a,b}\left(\frac{ab^{-1}}{l}\right)\zeta^{a-b}$$
$$\overset{(2)}{=} \sum_{c,b}\left(\frac{c}{l}\right)\zeta^{bc-b} = \sum_{c\neq 1}\left(\frac{c}{l}\right)\sum_{b}\zeta^{b(c-1)} + \sum_{b}\left(\frac{1}{l}\right)$$

Bei (1) nutzten wir aus, dass $\left(\frac{b^{-1}}{l}\right) = \left(\frac{b}{l}\right)^{-1} = \left(\frac{b}{l}\right)$ ist und machten den Übergang $b \rightsquigarrow -b$. Bei (2) machten wir den Übergang $c = ab^{-1}$.
(3) Sei $x \in (\mathbb{Z}/l)^*$, so dass $\left(\frac{x}{l}\right) = -1$. Dann gilt (setze $d = xc$)

$$-\sum_{c}\left(\frac{c}{l}\right) = \sum_{c}\left(\frac{x}{l}\right)\left(\frac{c}{l}\right) = \sum_{c}\left(\frac{xc}{l}\right) = \sum_{d}\left(\frac{d}{l}\right). \text{ Also } \sum_{c}\left(\frac{c}{l}\right) = 0.$$

(4) Mit $\eta = \zeta^{c-1}$ gilt $\sum_{b}\zeta^{b(c-1)} = \sum_{b}\eta^b = \eta + \eta^2 + \ldots + \eta^{l-1} = -1$, denn für $c \neq 1$ ist η ebenfalls primitive l-te Einheitswurzel, also $1+\eta+\eta^2+\ldots+\eta^{l-1} = 0$.
Somit erhalten wir, da $\sum_{c}\left(\frac{c}{l}\right) = \left(\frac{1}{l}\right) + \sum_{c\neq 1}\left(\frac{c}{l}\right) = 1 + \sum_{c\neq 1}\left(\frac{c}{l}\right)$ ist,

$$\left(\frac{-1}{l}\right)\tau^2 = (-1)\cdot(-1) + l - 1 = l.$$

□

Restbeweis von 23.6: Sei τ die Gauß'sche Summe

(1) $\tau^p = \tau\cdot(\tau^2)^{\frac{p-1}{2}} \equiv \tau\cdot(-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}\cdot\left(\frac{l}{p}\right) \mod p$ nach 23.4, 23.7.

(2) $\tau^p \equiv \sum_{a}\left(\frac{a}{l}\right)^p\cdot\zeta^{ap} = \sum_{a}\left(\frac{a}{l}\right)\zeta^{ap} = \left(\frac{p}{l}\right)\sum_{a}\left(\frac{p}{l}\right)\cdot\left(\frac{a}{l}\right)\zeta^{ap} \mod p$
$= \left(\frac{p}{l}\right)\cdot\sum_{a}\left(\frac{ap}{l}\right)\cdot\zeta^{ap} = \left(\frac{p}{l}\right)\sum_{b}\left(\frac{b}{l}\right)\zeta^{b} = \left(\frac{p}{l}\right)\cdot\tau$

Nach 23.7 ist $\tau \neq 0$. Also folgt $\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}\cdot\left(\frac{l}{p}\right)$. □

Die eigentliche Erklärung des Reziprozitätsgesetzes ist die Aussage des folgenden Satzes, der zu einem alternativen Beweis des Reziprozitätsgesetzes führt.

23.8 Satz: Seien l und p verschiedene ungerade Primzahlen, $l^* = (-1)^{\frac{l-1}{2}} \cdot l$ und ζ eine primitive l-te Einheitswurzel. Dann gilt

p ist voll zerlegt in $\mathbb{Q}(\sqrt{l^*}) \iff$ die Zahl der über p liegenden Primideale "in" $\mathbb{Q}(\zeta)$ ist gerade.

Beweis: Sei $K = \mathbb{Q}(\sqrt{l^*})$ und $F = \mathbb{Q}(\zeta)$. Nach 23.7 ist $l^* = \tau^2$, also $\sqrt{l^*} = \tau \in \mathbb{Q}(\zeta)$. Es folgt $\mathbb{Q}(\sqrt{l^*}) \subset \mathbb{Q}(\zeta)$. Da $[\mathbb{Q}(\sqrt{l^*}) : \mathbb{Q}] = 2$ gilt:

$$p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{l^*}) \iff (p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \text{ mit } \mathfrak{p}_1 \neq \mathfrak{p}_2 \text{ prim in } \mathcal{O}_K$$

Ein $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ mit $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$ bildet die Menge der über $\mathfrak{p}_1$ liegenden Ideale bijektiv auf die Menge der über $\mathfrak{p}_2$ liegenden Ideale ab. Damit liegt über p eine gerade Anzahl von Idealen in $\mathcal{O}_F$.

Umgekehrt sei die Zahl der über p liegenden Primideale in $\mathcal{O}_F$ gerade. Sei $\mathfrak{p} \subset \mathcal{O}_F$ ein Ideal über p. Ist $G_\mathfrak{p}$ die Zerlegungsgruppe von $\mathfrak{p}$, dann gilt mit $G = \mathrm{Gal}(F/\mathbb{Q})$ nach 20.8

$$[G : G_\mathfrak{p}] \text{ ist gerade.}$$

Ist $L_\mathfrak{p}$ der Zerlegungskörper, $L_\mathfrak{p} = F^{G_\mathfrak{p}}$, dann folgt, dass $[L_\mathfrak{p} : \mathbb{Q}] = [G : G_\mathfrak{p}]$ gerade ist.

Da $G \cong (\mathbb{Z}/l)^*$ zyklisch ist, besitzt G genau eine Untergruppe U vom Index 2 und $G_\mathfrak{p} \subset U$. Es folgt $K = F^U \subset F^{G_\mathfrak{p}} = L_\mathfrak{p}$. Sei $\mathcal{O}_L = \mathcal{O}_F \cap L_\mathfrak{p}$.

Nach 20.10 hat $\mathfrak{p} \cap L_\mathfrak{p}$ über $\mathbb{Q}$ den Trägheitsgrad 1, d.h.

$$\mathcal{O}_L/\mathfrak{p} \cap L_\mathfrak{p} \cong \mathbb{Z}/p.$$

Da $K \subset L_\mathfrak{p} \subset F$, folgt, dass der Trägheitsgrad von $\mathfrak{p} \cap K$ gleich 1 ist. Da auch der Verzweigungsindex von $\mathfrak{p} \cap L_\mathfrak{p}$ über $\mathbb{Q}$ gleich 1 ist, gilt dasselbe für $\mathfrak{p} \cap K$. Damit ist p voll zerlegt in K. □

23.9 Alternativer Beweis des Reziprozitätsgesetzes: Da nach 23.3 und 23.4

$$\left(\frac{l^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{l-1}{2}} \cdot \left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}} \cdot \left(\frac{l}{p}\right),$$

besagt das Reziprozitätsgesetz:

$$\left(\frac{l^*}{p}\right) = \left(\frac{p}{l}\right)$$

$$\left(\frac{l^*}{p}\right) = 1 \quad \overset{23.5}{\iff} \quad p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{l^*})$$
$$\overset{23.8}{\iff} \quad \text{in } \mathbb{Q}(\zeta) \text{ liegt über } p \text{ eine gerade Zahl } s \text{ von verschiedenen Primidealen.}$$

Nach 22.5 ist $s = \frac{\varphi(l)}{k_p}$, wobei k_p die Ordnung von $\overline{p}$ in $(\mathbb{Z}/l)^*$ ist. Da $\varphi(l) = l-1$, ist s genau dann gerade, wenn $k_p | \frac{l-1}{2}$. Da k_p die Ordnung von $\overline{p}$ ist, ist das gleichbedeutend mit

$$p^{\frac{l-1}{2}} \equiv 1 \mod l, \quad \text{d.h.} \quad \left(\frac{p}{l}\right) = 1.$$

□

Das Reziprozitätsgesetz stand am Ausgangspunkt der Entwicklung der algebraischen Zahlentheorie. Sein Studium führte zur Untersuchung von Kreisteilungskörpern.

24 Quadratische Körper

Sei $m \in \mathbb{Z}$ quadratfrei. Zunächst wollen wir die Zerlegung von Primzahlen $p \in \mathbb{Z}$ über $K = \mathbb{Q}(\sqrt{m})$ studieren.

24.1 Nach der fundamentalen Gleichung gibt es folgende Möglichkeiten

(1) $(p) = \mathfrak{p}^2$, d.h. p ist verzweigt, $e = 2, f = 1, r = 1$

(2) (p) bleibt prim, $e = 1, f = 2, r = 1$

(3) $(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, d.h. p ist voll zerlegt, $e = 1, f = 1, r = 2$.

24.2 Wir erinnern daran, dass $\delta_K = \begin{cases} 4m & m \equiv 2, 3 \mod 4 \\ m & m \equiv 1 \mod 4. \end{cases}$

24.3 Satz: Sei $p \neq 2$ eine Primzahl. Dann gilt in $K = \mathbb{Q}(\sqrt{m})$

(1) p ist verzweigt $\iff p \mid m$ 19.2

(2) p ist voll zerlegt $\iff p \nmid m$ und $\left(\frac{m}{p}\right) = 1$ 23.5

(3) $p =$ bleibt prim (ist *träge*) $\iff p \nmid m$ und $\left(\frac{m}{p}\right) = -1$ 23.5.

24.4 Satz: (1) 2 ist verzweigt in $\mathcal{O}_K$, falls $m \not\equiv 1 \mod 4$

(2) Ist $m \equiv 1 \mod 4$, so ist 2 unverzweigt in $\mathcal{O}_K$, und es gilt

(i) 2 ist voll zerlegt $\iff m \equiv 1 \mod 8$

(ii) 2 bleibt prim $\iff m \equiv 5 \mod 8$

Beweis: (1) ist 19.2. Im Fall (2) ist $\{1, \alpha\}$ mit $\alpha = \frac{1+\sqrt{m}}{2}$ eine ganze Basis. Also ist $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Damit sind die Voraussetzungen von 18.12 erfüllt. Das Minimalpolynom von α ist

$$f = X^2 - X + \frac{1-m}{4} \in \mathbb{Z}[X] \qquad (\text{ beachte } m \equiv 1 \mod 4).$$

Ist $m = 8k+1$, folgt

$$f = X^2 - X - 2k = X \cdot (X+1) \quad \text{über } \mathbb{Z}/2.$$

Nach 18.12 ist 2 damit voll zerlegt in $\mathcal{O}_K$.
Ist $m = 8k+5$, folgt

$$f = X^2 - X - (2k+1) = X^2 + X + 1 \quad \text{über } \mathbb{Z}/2.$$

f ist über $\mathbb{Z}/2$ irreduzibel. Aus 18.12 folgt, dass 2 träge ist. □

24.5 Ergänzung:

(1) Ist $m \equiv 2 \mod 4$, gilt $2 \cdot \mathcal{O}_K = \mathfrak{p}^2$ mit $\mathfrak{p} = (2, \sqrt{m})$

(2) Ist $m \equiv 3 \mod 4$, gilt $2 \cdot \mathcal{O}_K = \mathfrak{p}^2$ mit $\mathfrak{p} = (2, 1+\sqrt{m})$

(3) Ist $m \equiv 1 \mod 8$, gilt $2 \cdot \mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ mit $\mathfrak{p}_1 = (2, \alpha)$, $\mathfrak{p}_2 = (2, 1+\alpha)$
Ist $m \equiv 5 \mod 8$, gilt $2 \cdot \mathcal{O}_K = (2, 1+\alpha+\alpha^2) = (2)$, $\alpha = \frac{1+\sqrt{m}}{2}$

Dies folgt aus 18.12. Im Falle (1) und (2) ist $\{1, \sqrt{m}\}$ ein Ganzheitsbasis, also $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ und $f = X^2 - m$ das Minimalpolynom von $\sqrt{m}$. Über $\mathbb{Z}/2$ gilt

$$f = \begin{cases} X^2 & \text{im Fall (1)} \\ X^2 + 1 = (X+1)^2 & \text{im Fall (2)} \end{cases}$$

Damit erhält man die $\mathfrak{p}_i$. Im Fall (3) s. Beweis 24.4. Im Fall $m = 8k+5$ wissen wir, dass 2 träge ist, dass also $(2, 1+\alpha+\alpha^2) = (2)$ sein muss. Das sieht man aber auch direkt ein: Aus $f(\alpha) = 0$ folgt $\alpha^2 - \alpha - 1 = 2k$, so dass $\alpha^2 + \alpha + 1 = 2k + 2\alpha + 2 = (k + \alpha + 1) \cdot 2 \in (2)$. □

Als nächstes wollen wir uns der Bestimmung der Hauptidealringe $\mathcal{O}_K$ für imaginär-quadratische Körper $K = \mathbb{Q}(\sqrt{m})$, $m < 0$ quadratfrei, zuwenden.

24.6 Satz: Für $m \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\} =: S$ ist $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{m})$, ein Hauptidealring.

Beweis: Aus einer Übungsaufgabe wissen wir, dass $\mathcal{O}_K$ mit der Norm ein euklidischer Ring und damit ein Hauptidealring ist, falls $m \in \{-1,-2, -3,-7,-11\}$. Es bleiben die anderen Fälle. Wir nutzen 16.7: Jedes $x \in \mathcal{C}l_K$ wird durch ein Ideal $J \subset \mathcal{O}_K$ mit

$$\mathfrak{N}(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|} \qquad (*)$$

repräsentiert. Da K imaginär-quadratisch ist, ist $s = 1$.

m = −19: $\mathfrak{N}(J) \leq \frac{2}{\pi}\sqrt{19} = \frac{\sqrt{76}}{\pi} < \frac{9}{\pi} < 3$, so dass $\mathfrak{N}(J) \in \{1,2\}$.

Wir wollen zeigen, dass jedes solche J ein Hauptideal ist. Ist $\mathfrak{N}(J) = 1$, folgt $J = \mathcal{O}_K = (1)$. Ist $\mathfrak{N}(J) = 2$, folgt aus 16.10, dass $J|(2)$ in $\mathcal{O}_K$.

Da $-19 \equiv 5 \mod 8$, ist (2) träge, also $J = (2)$.

Bevor wir die anderen Fälle behandeln, zeigen wir

24.7 Lemma: Sei K ein Zahlkörper, r die Anzahl der reellen Einbettung $K \to \mathbb{R}$ und $2s$ die Anzahl der nicht-reellen Einbettungenen $K \to \mathbb{C}$, $r+2s = [K:\mathbb{Q}]$. Für alle Primzahlen $p \in \mathbb{N}$ mit

$$p \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|} \qquad (*)$$

gelte: Ist $\mathfrak{p} \in \mathcal{O}_K$ ein Primideal, das $p \cdot \mathcal{O}_K$ teilt, dann ist $\mathfrak{p}$ ein Hauptideal.
Dann gilt: $h_K = |\mathcal{C}l_K| = 1$, d.h. $\mathcal{O}_K$ ist Hauptidealring.

Beweis: Sei $J \subset \mathcal{O}_K$ ein Ideal mit $\mathfrak{N}(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\delta_K|}$ und $\mathfrak{N}(J) = p_1 \cdot \ldots \cdot p_k$ die Primfaktorzerlegung von $\mathfrak{N}(J)$. Sei

$$J = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s$$

die Primfaktorzerlegung in $\mathcal{O}_k$. Sei $\mathfrak{p} = \mathfrak{p}_i$. Da $J \mid \mathfrak{N}(J)$, gilt $\mathfrak{p} \mid (p_1 \cdot \ldots \cdot p_k)$. Also gibt es ein p_j mit $\mathfrak{p} \mid p_j$. Da $p_j \leq \mathfrak{N}(J)$, erfüllt p_j die Voraussetzung $(*)$. Also ist $\mathfrak{p}$ ein Hauptideal, $\mathfrak{p} = \mathfrak{p}_i = (\alpha_i)$ in $\mathcal{O}_K$. Es folgt

$$J = (\alpha_1 \cdot \ldots \cdot \alpha_s) \text{ ist Hauptideal in } \mathcal{O}_K.$$

Damit wird jedes $x \in \mathcal{C}l_K$ durch ein Hauptideal repräsentiert. Es folgt: $h_K = 1$. □

24.8 Bemerkung: Mit dem Beweis von Bemerkung 16.8 kann man den Faktor $\left(\frac{2}{\pi}\right)^s$ in $(*)$ durch die Minkowski'sche Zahl $\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s$, $n = [K : \mathbb{Q}]$ ersetzen. Für imaginär quadratische Zahlkörper stimmen die beiden Zahlen überein.

Fortsetzung von 24.6:

m = −43: $\mathfrak{N}(J) \leq \frac{2}{\pi}\sqrt{43} = \frac{\sqrt{172}}{\pi} < \frac{15}{\pi} < 5$. Nach 24.7 müssen wir (2) und (3) untersuchen.

Da $-43 \equiv 5 \mod 8$, ist (2) träge, also selbst prim in $\mathcal{O}_K$

$3 \nmid -43$ und $\left(\frac{-43}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$, also ist auch (3) prim in $\mathcal{O}_K$.

m = −67: $\frac{2}{\pi}\sqrt{67} = \frac{\sqrt{268}}{\pi} < \frac{17}{\pi} < 6$. Nach 24.7 müssen wir (2), (3), (5) untersuchen. Da $-67 \equiv 5 \mod 8$, ist (2) träge. Da $3 \nmid -67$, $5 \nmid -67$ und

$$\left(\frac{-67}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

und

$$\left(\frac{-67}{5}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}} \left(\frac{5}{3}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

sind auch (3) und (5) träge.

m = −163: $\frac{2}{\pi}\sqrt{163} = \frac{\sqrt{652}}{\pi} < \frac{26}{\pi} < 9$. Wir müssen die Ideale (2), (3), (5), (7) untersuchen.

$-163 \equiv 5 \mod 8$, also ist (2) träge.

$3 \nmid -163$ und $\left(\frac{-163}{3}\right) = \left(\frac{-1}{3}\right) = -1$, also ist (3) träge.

$5 \nmid -163$ und $\left(\frac{-163}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{25-1}{8}} = -1$, also ist (5) träge.

$7 \nmid -163$ und $\left(\frac{-163}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right) \cdot \left(\frac{2}{7}\right) = (-1)^{\frac{6}{2}}(-1)^{\frac{49-1}{8}} = (-1)^3 \cdot (-1)^6 = -1$. Also ist auch (7) träge.

□

Über die Umkehrung des Satzes 24.6, nämlich: Ist $K = \mathbb{Q}(\sqrt{m})$ imaginär-quadratischer Körper und $\mathcal{O}_K$ ein Hauptidealring, dann ist $m \in S$, gab es einen langen Disput. Hegner veröffentlichte einen Beweis, bei dem er einen in Teilen fehlerhaften Satz zitierte. 1967 bewies Starck die Umkehrung mit völlig anderen Methoden. Kurz darauf zeigten Deuring und Siegel, dass Hegner's Beweis schlüssig war. In der angelsächsischen Literatur wird er aber noch immer Starck zugerechnet.

24.9 Satz: Für $m \in \{-1,-2,-3,-7,-11\}$ ist $\mathcal{O}_K$ mit $K = \mathbb{Q}(\sqrt{m})$ euklidisch mit der Norm als Strukturabbildung. Für $m \in \{-19,-43,-67,-163\}$ ist $\mathcal{O}_K$ zwar Hauptidealring, aber nicht euklidisch.

Beweis: Wir müssen nur zeigen, dass $\mathcal{O}_K$ für $m \in \{-19,-43,-67,-163\}$ nicht euklidisch ist. Wir nehmen das Gegenteil an. Dann gibt es eine Abbildung

$$\delta : \mathcal{O}_K \backslash \{0\} \to \mathbb{N},$$

so dass

(1) $\delta(x) \leq \delta(x \cdot y)\ \forall x.y \in \mathcal{O}_K \backslash \{0\}$

(2) zu $x \in \mathcal{O}_K$ und $y \in \mathcal{O}_K \backslash \{0\}$ gibt es $q, r \in \mathcal{O}_K$ mit

$$x = q \cdot y + r, \quad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(y).$$

Wir wählen aus $\{x \in \mathcal{O}_K; x \neq 0, x \notin \mathcal{O}^*\}$ ein b mit minimalem $\delta(b)$. Für jedes $a \in \mathcal{O}_K$ haben wir dann eine Gleichung

$$a = q \cdot b + r \text{ mit } r = 0 \text{ oder } \delta(r) < \delta(b).$$

Ist $r \neq 0$, folgt $r \in \mathcal{O}^* = \{\pm 1\}$ wegen der Minimalität von $\delta(b)$.
Es folgt:

(A) Ist $a \in \mathcal{O}_K$ beliebig, dann teilt b mindestens eines der Elemente $a, a+1, a-1$ (Fälle: $r = 0, r = -1, r = 1$)

Sei $N : \mathcal{O}_K \to \mathbb{N}$ die Normalabbildung. Da $b \notin \mathcal{O}_K^*$, gilt $N(b) > 1$.

Aus (A) erhalten wir mit $a = 2$

$$b \text{ teilt } 1, 2, \text{ oder } 3, \text{ also } N(b) \text{ teilt } 1, 4 \text{ oder } 9$$

(B) Da $N(b) > 1$, sind 2 und 3 die einzig möglichen Primteiler von $N(b)$.

In unseren Fällen ist $m \equiv 1 \mod 4$, Also ist $a = \frac{1}{2} + \frac{1}{2}\sqrt{m} \in \mathcal{O}_K$. Wir erhalten

$$\begin{aligned} N(a) &= N(a-1) = \tfrac{1}{4} + |m|\tfrac{1}{4} = \tfrac{|m|+1}{4} \\ N(a+1) &= N(\tfrac{3}{2} + \tfrac{1}{2}\sqrt{m}) = \tfrac{9}{4} + |m|\tfrac{1}{4} = \tfrac{|m|+1}{4} + 2 \end{aligned}$$

Es folgt

(C) $N(b)$ teilt $\frac{|m|+1}{4}$ oder $\frac{|m|+1}{4} + 2$, d.h.

$m = -19$	$N(b)$ teilt 5 oder 7
$m = -43$	$N(b)$ teilt 11 oder 13
$m = -67$	$N(b)$ teilt 17 oder 19
$m = -163$	$N(b)$ teilt 41 oder 43

Jeder dieser Fälle widerspricht aber (B). □