Algebraische Zahlentheorie

Prof. Dr. Nils Scheithauer

TU Darmstadt
Sommersemester 2012

Mitschrift von Fabian Völz

Inhaltsverzeichnis

1 Ganze Ringerweiterungen

Sei K eine Körpererweiterung von $\mathbb{Q}$. Der Körper K heißt **algebraischer Zahlkörper**, wenn der Index $[K : \mathbb{Q}]$ endlich ist, und ein Element $b \in K$ heißt **ganz**, wenn b Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[x]$, $f \neq 0$, ist. Der Fokus dieser Vorlesung liegt auf der Charakterisierung ganzer Elemente algebraischer Zahlkörper.

Im Folgenden betrachten wir aber zunächst den allgemeineren Fall ganzer Ringerweiterungen. Dabei nehmen wir immer an, dass Ringe kommutativ sind und ein Einselement besitzen. Sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt **ganz über** A, wenn es Nullstelle eines normierten Polynoms $f \in A[x]$, $f \neq 0$, ist. Weiter heißt der Ring B **ganz über** A, wenn alle $b \in B$ ganz über A sind.

Satz 1.1. *Sei $A \subseteq B$ eine Ringerweiterung und $b_1, \ldots, b_n \in B$. Dann sind äquivalent:*

(1) Der Ring $A[b_1, \ldots, b_n]$ ist ganz über A.

(2) Die Elemente $b_1, \ldots, b_n$ sind ganz über A.

(3) Der Ring $A[b_1, \ldots, b_n]$ ist ein endlich erzeugter A-Modul.

Um dies zu beweisen, benötigen wir das folgende Resultat aus der linearen Algebra, welches sich zum Beispiel als Proposition 4.16 in Kapitel 8 in [Lan02] finden lässt.

Theorem 1.2. *Sei $M = (m_{ij})$ eine $m \times m$ Matrix mit Einträgen in einem Ring R, und sei $N = (n_{ij})$ die zu M komplementäre Matrix, das heißt die Matrix mit den Einträgen $n_{ij} = (-1)^{i+j} \det(M_{ji})$, wobei M_{ji} die $(m-1) \times (m-1)$ Matrix bezeichnet, welche durch entfernen der j-ten Zeile und der i-ten Spalte aus M entsteht. Dann gilt*

$$MN = NM = \det(M) E_m.$$

Hier bezeichnet E_m die Einheitsmatrix vom Rang m.

Beweis von Satz 1.1. Es ist klar, dass (2) aus (1) folgt. Wir zeigen nun per Induktion über n, dass Aussage (2) Aussage (3) impliziert. Sei dazu $b_1 \in B$ ganz über A und $f \in A[x]$ normiert vom Grad m mit $f(b_1) = 0$. Für beliebiges $g \in A[x]$ ist dann $g = fq + r$ mit $q, r \in A[x]$ und $\operatorname{grad}(r) < m$. Man beachte, dass hierbei eingeht, dass f normiert ist. Es folgt

$$g(b_1) = r(b_1) = a_0 + a_1 b + \ldots + a_{m-1} b^{m-1}$$

für geeignete $a_i \in A$, und somit

$$A[b_1] = A + Ab_1 + \ldots + Ab_1^{m-1}.$$

Der Ring $A[b_1]$ wird als A-Modul daher von den Elementen $1, b_1, \ldots, b_1^{m-1}$ erzeugt. Dies zeigt den Induktionsanfang.

Seien nun $b_1, \ldots, b_n \in B$ ganz über A. Dann ist b_n auch ganz über $R = A[b_1, \ldots, b_{n-1}]$ und wie zuvor lässt sich zeigen, dass $R[b_n]$ ein endlich erzeugter R-Modul ist. Nehmen wir nun an, dass R bereits ein endlich erzeugter A-Modul ist, dann ist auch

$$A[b_1, \ldots, b_n] = R[b_n]$$

ein endlich erzeugter A-Modul, was den Induktionsschritt beweist.

Es bleibt zu zeigen, dass aus (3) auch (1) folgt. Sei $A[b_1, \ldots, b_n] \subseteq B$ ein endlich erzeugter A-Modul, das heißt es gilt

$$A[b_1, \ldots, b_n] = A\omega_1 + \ldots + A\omega_m$$

für geeignete $\omega_i \in B$. Wir finden also für jedes $b \in A[b_1, \ldots, b_n]$ Koeffizienten $a_{ij} \in A$, sodass

$$b\omega_i = \sum_{j=1}^{m} a_{ij}\omega_j.$$

Sei M die $m \times m$ Matrix mit den Einträgen $b\delta_{ij} - a_{ij}$. Dann gilt

$$M\omega = \left(\sum\nolimits_{j=1}^{m} \left(b\delta_{ij} - a_{ij}\right)\omega_j\right)_{i=1,\ldots,m} = 0.$$

Man beachte weiter, dass

$$\det(M) = c_0 + c_1 b + \ldots + c_{m-1}b^{m-1} + b^m$$

für geeignete $c_i \in A$, also $\det(M) = f(b)$ für ein normiertes, nicht-triviales Polynom $f \in A[x]$. Wir werden im Folgenden zeigen, dass $\det(M) = 0$ ist. Dies impliziert dann, dass b ganz über A ist.

Sei N die zu M komplementäre Matrix. Dann gilt $NM = \det(M)E_m$ nach obigem Theorem 1.2. Somit ist $\det(M)\omega = NM\omega = 0$ und daher $\det(M)\omega_i = 0$ für alle i. Schließlich gibt es $d_1, \ldots, d_n \in A$, sodass $1 = \sum_{i=1}^{n} d_i\omega_i$, also ist

$$\det(M) = \det(M) \cdot 1 = \sum_{i=1}^{n} d_i \det(M)\omega_i = 0.$$

Damit ist gezeigt, dass jedes $b \in A[b_1, \ldots, b_n]$ ganz über A ist. □

Sei $A \subseteq B$ eine Ringerweiterung. Wir definieren den **ganzen Abschluss von A in B** als

$$\overline{A} = \{b \in B \colon b \text{ ist ganz über } A\}.$$

Weiterhin sagen wir, dass A **ganz abgeschlossen in** B ist, wenn $A = \overline{A}$ gilt.

Bemerkung. Ist K ein Körper und L ein algebraischer Abschluss von K, dann stimmt der ganze Abschluss von K in L mit L überein. Dies ist klar, da das Minimalpolynom eines Elementes $l \in L$ ein normiertes, nicht-triviales Polynom in $K[x]$ ist.

Korollar 1.3. *Sei $A \subseteq B$ eine Ringerweiterung. Dann ist $\overline{A}$ ein Unterring von B.*

Beweis. Seien $b_1, b_2 \in B$ ganz über A. Nach Satz 1.1 ist dann auch jedes $b \in A[b_1, b_2]$ ganz über A. Insbesondere sind also $b_1 b_2$ und $b_1 - b_2$ ganz über A. □

Korollar 1.4. *Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Ist C ganz über B und B ganz über A, so ist auch C ganz über A.*

Beweis. Sei $c \in C$. Dann ist c ganz über B, und daher

$$b_0 + b_1 c + \ldots b_{n-1} c^{n-1} + c^n = 0$$

für geeignete $b_i \in B$. Sei $R = A[b_0, \ldots, b_{n-1}]$. Da c ganz über $R \subseteq B$ ist, ist $R[c]$ ein endlich erzeugter R-Modul, und da $b_0, \ldots, b_{n-1} \in B$ ganz über A sind, ist R ein endlich erzeugter A-Modul. Somit ist auch $R[c] = A[b_0, \ldots, b_{n-1}, c]$ ein endlich erzeugter A-Modul, und damit ist c ganz über A. □

Korollar 1.5. *Sei $A \subseteq B$ eine Ringerweiterung. Dann ist $\overline{A}$ ganz abgeschlossen in B.*

Beweis. Offensichtlich liegt $\overline{A}$ im ganzen Abschluss von $\overline{A}$. Sei b ein Element des ganzen Abschlusses von $\overline{A}$. Dann ist b ganz über $\overline{A}$. Nach Satz 1.4 und da $\overline{A}$ per Konstruktion ganz über A ist, ist damit b auch ganz über A, also $b \in \overline{A}$. Dies zeigt, dass $\overline{A}$ ganz abgeschlossen in B ist. □

Sei A ein Integritätsbereich. Wir bezeichnen A als **ganz abgeschlossen**, falls A ganz abgeschlossen in seinem Quotientenkörper K ist. Allgemeiner nennen wir den ganzen Abschluss $\overline{A}$ von A in K **Normalisierung von** A.

Satz 1.6. *Sei A ein faktorieller Integritätsbereich. Dann ist A ganz abgeschlossen.*

Beweis. Sei K der Quotientenkörper von A und $a/b \in K$ ganz über A mit $a, b \in A$, $\mathrm{ggT}(a, b) = 1$. Dann ist

$$(a/b)^n + a_1 (a/b)^{n-1} + \ldots + a_n = 0$$

für geeignete $a_i \in A$, also

$$a^n + a_1 a^{n-1} b + \ldots a_{n-1} a b^{n-1} + a_n b^n = 0.$$

Somit wird a^n von b geteilt. Da andererseits a und b nach Annahme teilerfremd sind, muss b eine Einheit sein, was $a/b \in A$ impliziert. Dies zeigt die Behauptung. □

Beispiel. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein faktorieller Integritätsbereich und damit ganz abgeschlossen in seinem Quotientenkörper $\mathbb{Q}$.

Satz 1.7. *Sei A ein Integritätsbereich mit Quotientenkörper K, L/K eine algebraische Körpererweiterung und B der ganze Abschluss von A in L. Sei $\alpha \in L$. Dann gibt es $a \in A$, $a \neq 0$, und $b \in B$, sodass $\alpha = b/a$ gilt.*

Beweis. Sei $m_{\alpha,K}$ das Minimalpolynom von α über K, das heißt

$$m_{\alpha,K} = x^n + a_1 x^{n-1} + \ldots + a_n$$

für geeignete $a_i \in K$. Dann gibt es $b_i, c_i \in A$, $c_i \neq 0$, sodass $a_i = b_i/c_i$. Somit ergibt sich

$$\begin{aligned} 0 = m_{\alpha,K}(\alpha) &= \alpha^n + b_1/c_1 \cdot \alpha^{n-1} + \ldots + b_n/c_n \\ &= \left(\prod\nolimits_i c_i\right) \alpha^n + b_1 \left(\prod\nolimits_{i\neq 1} c_i\right) \alpha^{n-1} + \ldots + b_n \left(\prod\nolimits_{i\neq n} c_i\right). \end{aligned}$$

Setze $d_0 = \prod_i c_i$. Dann ist $d_0 \in A$ und $d_0 \neq 0$, da alle $c_i \neq 0$ sind und A ein Integritätsbereich ist. Es folgt

$$0 = d_0^n \alpha^n + b_1 d_0^{n-1} \left(\prod\nolimits_{i\neq 1} c_i\right) \alpha^{n-1} + \ldots + b_n d_0^{n-1} \left(\prod\nolimits_{i\neq n} c_i\right).$$

Setze $d_k = b_k d_0^{k-1} \prod_{i\neq k} c_i$ für $k = 1, \ldots, n$. Offensichtlich ist $d_i \in A$. Definiere

$$f(x) = x^n + d_1 x^{n-1} + \ldots + d_n.$$

Dann ist $f \in A[x]$ ein normiertes, nicht-triviales Polynom und es gilt $f(d_0\alpha) = 0$ nach Konstruktion. Also ist $d_0\alpha$ ganz über A, und somit gibt es ein $b \in B$, sodass $b = d_0\alpha$, bzw. $\alpha = b/d_0$. □

Satz 1.8. *Sei A ein Integritätsbereich mit Quotientenkörper K, A ganz abgeschlossen in K und L/K eine algebraische Körpererweiterung. Dann sind für $\alpha \in L$ äquivalent:*

(1) Das Element α ist ganz über A.

(2) Das Minimalpolynom $m_{\alpha,K}$ von α über K liegt in $A[x]$.

Beweis. Wir zeigen zunächst, das Aussage (1) Aussage (2) impliziert. Sei $\alpha \in L$ ganz über A, das heißt es gilt $f(\alpha) = 0$ für ein normiertes, nicht-triviales Polynom $f \in A[x]$. Sei $m_{\alpha,K}$ das Minimalpolynom von α über K. Dann teilt $m_{\alpha,K} \in K[x]$ das Polynom f, das heißt es gibt $q \in K[x]$, sodass $m_{\alpha,K} \cdot q = f$. Über einem algebraischen Abschluss $\overline{L}$ von L zerfällt

$$m_{\alpha,K} = \prod_{i=1}^{n} (x - \alpha_i)$$

mit geeigneten $\alpha_i \in \overline{L}$. Aus der Teilbarkeit folgt $f(\alpha_i) = 0$ für alle i. Damit sind alle α_i ganz über A, und somit sind auch die Koeffizienten von $m_{\alpha,K}$ ganz über A, da der ganze Abschluss von A ein Unterring von K ist. Nach Annahme ist A aber bereits selbst ganz abgeschlossen in K, was $m_{\alpha,K} \in A[x]$ impliziert.

Die Rückrichtung ist klar, da das Minimalpolynom $m_{\alpha,K}$ von α über K normiert und nicht-trivial ist. □

Sei L/K eine endliche Körpererweiterung. Dann ist L ein endlich-dimensionaler Vektorraum über K. Die Abbildung

$$T_x\colon L \to L,\ \alpha \mapsto x\alpha$$

ist K-linear. Wir definieren

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x) \quad \text{und} \quad \mathrm{N}_{L/K}(x) = \det(T_x).$$

Dabei nennen wir $\mathrm{Tr}_{L/K}$ **Spurabbildung** und $\mathrm{N}_{L/K}$ **Normabbildung**. Ist $[L:K] = n$ und

$$f_x(t) = \det(t \cdot \mathrm{id} - T_x) = t^n + c_1 t^{n-1} + \ldots + c_n \in K[t]$$

das charakteristische Polynom von T_x, so gilt

$$c_1 = \mathrm{Tr}_{L/K}(x) \quad \text{und} \quad c_n = (-1)^n \mathrm{N}_{L/K}(x).$$

Die Spurabbildung $\mathrm{Tr}_{L/K}\colon L \to K$ ist K-linear und die Normabbildung $\mathrm{N}_{L/K}\colon L \to K$ ist multiplikativ, das heißt es gilt $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\,\mathrm{N}_{L/K}(y)$ für alle $x, y \in L$.

Satz 1.9. *Sei $K(a)$ eine algebraische Körpererweiterung von K und*

$$m_{a,K} = x^n + c_1 x^{n-1} + \ldots + c_n$$

das Minimalpolynom von a über K. Dann gilt

$$\mathrm{Tr}_{K(a)/K}(a) = -c_1 \quad \textit{und} \quad \mathrm{N}_{K(a)/K}(a) = (-1)^n c_n.$$

Beweis. Die Menge $\{1, a, \ldots, a^{n-1}\}$ ist eine Basis von $L = K(a)$ über K. Die Matrix von $T_a\colon L \to L, x \mapsto ax$ bezüglich dieser Basis ist gegeben durch

$$C = \begin{pmatrix} 0 & & & -c_n \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -c_2 \\ 0 & & 1 & -c_1 \end{pmatrix}.$$

Es folgt, dass $\mathrm{Tr}_{K(a)/K}(a) = \mathrm{Tr}(C) = -c_1$ und $\mathrm{N}_{K(a)/K}(a) = \det(C) = (-1)^n c_n$. □

Satz 1.10. *Sei L/K eine endliche Körpererweiterung, $a \in L$ und $n = [L : K(a)]$. Dann gilt*

$$\mathrm{Tr}_{L/K}(a) = n \cdot \mathrm{Tr}_{K(a)/K}(a) \quad \textit{und} \quad \mathrm{N}_{L/K}(a) = \left(\mathrm{N}_{K(a)/K}(a)\right)^n.$$

Beweis. Sei $X = \{x_1, \ldots, x_m\}$ eine Basis von $K(a)/K$ und sei $Y = \{y_1, \ldots, y_n\}$ eine Basis von $L/K(a)$. Dann ist durch $Z := \{xy\colon x \in X, y \in Y\}$ eine Basis von L/K gegeben. Weiter sei $A \in K^{m\times m}$ die Matrix der Abbildung

$$K(a) \to K(a),\ x \mapsto ax$$

bezüglich der Basis X. Dann ist die Matrix der Abbildung

$$L \to L,\ x \mapsto ax$$

bezüglich der Basis Z von der Form

$$C = \begin{pmatrix} A & & \\ & \ddots & \\ & & A \end{pmatrix}.$$

Es folgt

$$\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(C) = n \cdot \mathrm{Tr}(A) = n \cdot \mathrm{Tr}_{K(a)/K}(a)$$

und

$$\mathrm{N}_{L/K}(a) = \det(C) = \det(A)^n = \left(\mathrm{N}_{K(a)/K}(a)\right)^n.$$

□

Satz 1.11. *Sei A ein Integritätsbereich mit Quotientenkörper K, A ganz abgeschlossen in K und L/K eine endliche Körpererweiterung. Ist $a \in L$ ganz über A, so gilt*

$$\mathrm{Tr}_{L/K}(a) \in A \quad \textit{und} \quad \mathrm{N}_{L/K}(a) \in A.$$

Beweis. Da A ganz abgeschlossen in K ist, gilt

$$m_{a,K} = x^n + c_1 x^{n-1} + \ldots + c_n \in A[x]$$

nach Satz 1.8. Daher ist $\mathrm{Tr}_{K(a)/K}(a) = -c_1 \in A$ und somit

$$\mathrm{Tr}_{L/K}(a) = [L : K(a)] \cdot \mathrm{Tr}_{K(a)/K}(a) \in A.$$

Ein analoges Argument zeigt, dass auch $\mathrm{N}_{L/K}(a) \in A$ gilt. □

Beispiel. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist als Hauptidealring ganz abgeschlossen in seinem Quotientenkörper $\mathbb{Q}$. Sei $d \in \mathbb{Z}$ quadratfrei und $d \neq 0, 1$. Setze

$$K = \mathbb{Q}(\sqrt{d}\,) = \mathbb{Q}[\sqrt{d}\,] = \{x + y\sqrt{d} \colon x, y \in \mathbb{Q}\}.$$

Dann ist $K/\mathbb{Q}$ eine Körpererweiterung vom Grad 2. Für $z = x + y\sqrt{d}$ definieren wir $\overline{z} = x - y\sqrt{d}$. Das Minimalpolynom von $z = x + y\sqrt{d} \in K$ über $\mathbb{Q}$ ist gegeben durch

$$m_{z,\mathbb{Q}}(t) = t^2 - (z + \overline{z})t + z \cdot \overline{z} = t^2 - 2xt + \left(x^2 - dy^2\right).$$

Nach Satz 1.9 gilt somit $\mathrm{Tr}_{K/\mathbb{Q}}(z) = 2x$ und $\mathrm{N}_{K/\mathbb{Q}}(z) = x^2 - dy^2$. Sei

$$\omega = \begin{cases} \sqrt{d}, & \text{falls } d = 2, 3 \bmod 4 \\ (1 + \sqrt{d}\,)/2, & \text{falls } d = 1 \bmod 4. \end{cases}$$

Dann ist ω als Nullstelle des Polynoms $t^2 - d$ bzw. $t^2 - t + (1-d)/4$ ganz über $\mathbb{Z}$ und

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega = \{m + n\omega \colon m, n \in \mathbb{Z}\}$$

ein Ring. Wir behaupten, dass $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K ist.

Um dies einzusehen, sei $z = x + y\sqrt{d}$ ganz über $\mathbb{Z}$. Dann ist nach Satz 1.9

$$\mathrm{Tr}_{K/\mathbb{Q}}(z) = 2x \in \mathbb{Z} \quad \text{und} \quad \mathrm{N}_{K/\mathbb{Q}}(z) = x^2 - dy^2 \in \mathbb{Z}.$$

Also gilt $x \in \mathbb{Z}/2$. Ist $x \in \mathbb{Z}$, so folgt $y^2 d \in \mathbb{Z}$ und damit $y \in \mathbb{Z}$, da d quadratfrei ist. In diesem Fall gilt also $z \in \mathcal{O}_K$. Ist andererseits $x \in \mathbb{Z} + 1/2$, so ergibt sich $y^2 d \in \mathbb{Z} + 1/4$. Dies impliziert $y \in \mathbb{Z} + 1/2$, da d quadratfrei ist. Seien schließlich $N, M \in \mathbb{Z}$, sodass $y^2 d = N + 1/4$ und $y = M + 1/2$. Dann folgt

$$4N + 1 = 4y^2 d = 4M^2 d + 4Md + d.$$

Also gilt in diesem Fall $d = 1 \bmod 4$, das heißt $\omega = (1 + \sqrt{d}\,)/2$, und daher

$$z = x + y\sqrt{d} \in \left(\mathbb{Z} + \frac{1}{2}\right) + \left(\mathbb{Z} + \frac{1}{2}\right)\sqrt{d} = \frac{1}{2}(2\mathbb{Z}) + \omega + \frac{\sqrt{d}}{2}(2\mathbb{Z}) = (2\mathbb{Z} + 1)\omega.$$

Somit gilt jeweils $z \in \mathcal{O}_K$, das heißt der ganze Abschluss von $\mathbb{Z}$ ist in $\mathcal{O}_K$ enthalten. Umgekehrt lässt sich zeigen, dass es zu jedem Element $z \in \mathcal{O}_K$ ein normiertes Polynom $f \in \mathbb{Z}[x]$ vom Grad 2 mit $f(z) = 0$ gibt.

Satz 1.12. *Sei L/K eine endliche separable Körpererweiterung vom Grad n, und seien $\sigma_1, \ldots, \sigma_n$ die n verschiedenen K-Homomorphismen $L \to \overline{K}$. Dann gilt*

$$\mathrm{Tr}_{L/K}(a) = \sum_{i=1}^{n} \sigma_i(a) \quad \textit{und} \quad \mathrm{N}_{L/K}(a) = \prod_{i=1}^{n} \sigma_i(a)$$

für alle $a \in L$.

Beweis. Sei $a \in L$ und $m_{a,K} = x^m + c_1 x^{m-1} + \ldots + c_m$ das Minimalpolynom von a über K. Da L/K separabel ist, ist auch $K(a)/K$ separabel. Wir bezeichnen die m verschiedenen K-Homomorphismen $K(a) \to \overline{K}$ mit $\tau_1, \ldots, \tau_m$. Dann ist

$$m_{a,K} = \prod_{i=1}^{m} (x - \tau_i(a))\,.$$

Es folgt

$$\mathrm{Tr}_{K(a)/K}(a) = -c_1 = \sum_{i=1}^{m} \tau_i(a)$$

und

$$\mathrm{N}_{K(a)/K}(a) = (-1)^m c_m = \prod_{i=1}^{m} \tau_i(a).$$

Da die Einschränkung von einem σ_j auf $K(a)$ weiterhin ein K-Homomorphismus ist, gibt es zu jedem $j \in \{1, \dots, n\}$ ein $i \in \{1, \dots, m\}$, sodass $\sigma_j|_{K(a)} = \tau_i$ gilt. Umgekehrt lässt sich jedes τ_i zu einem K-Homomorphismus auf L fortsetzen. Die Anzahl dieser Fortsetzungen ist gegeben durch $[L : K(a)]$.

(Zur Erinnerung: Es gibt ein $b \in L$, sodass $L = K(a)(b)$. Die Anzahl der Fortsetzungen von τ_i auf L entspricht der Anzahl der verschiedenen Nullstellen des Minimalpolynoms $m_{b,K(a)}$ in $\overline{K}$. Diese Anzahl ist unabhängig von der Wahl von b und wird mit $[L : K(a)]_s$ bezeichnet. Weiterhin ist jede Nullstelle von $m_{b,K(a)}$ einfach, da $m_{b,K(a)}$ das Minimalpolynom $m_{b,K}$ von b über K teilt und L/K separabel ist. Also gilt $[L : K(a)]_s = [L : K(a)]$.)

Schließlich folgt somit

$$\mathrm{Tr}_{L/K}(a) = [L : K(a)] \cdot \mathrm{Tr}_{K(a)/K}(a) = [L : K(a)] \cdot \sum_{i=1}^{m} \tau_i(a) = \sum_{j=1}^{n} \sigma_j(a).$$

Analog ergibt sich für die Norm, dass

$$\mathrm{N}_{L/K}(a) = \big(\mathrm{N}_{K(a)/K}(a)\big)^{[L:K(a)]} = \prod_{i=1}^{m} (\tau_i(a))^{[L:K(a)]} = \prod_{j=1}^{n} \sigma_j(a).$$

□

Bemerkung. Ist L/K sogar eine endliche Galoiserweiterung, so zeigt der vorhergehende Satz, dass $\mathrm{Tr}_{L/K}$ und $\mathrm{N}_{L/K}$ invariant unter der Galoisgruppe $\mathrm{Gal}(L/K)$ sind.

Sei K ein Körper und G eine Gruppe. Ein Homomorphismus $\chi\colon G \to K^*$ wird als **K-wertiger Charakter von** G bezeichnet. Sind χ_1, χ_2 zwei K-wertige Charaktere, so ist auch

$$\chi_1\chi_2\colon G \to K^*,\ g \mapsto \chi_1(g)\chi_2(g)$$

ein K-wertiger Charakter. Die Menge aller K-wertigen Charaktere einer Gruppe G bildet unter dieser Operation selbst wieder eine Gruppe. Wir wiederholen das folgende wichtige Resultat, welches bereits in der Veranstaltung „Algebra“ bewiesen wurde, und zenral für den Beweis des darauf folgenden Satzes ist.

Theorem 1.13. *Sei G eine Gruppe, K ein Körper und seien $\chi_1, \dots, \chi_n$ paarweise verschiedene K-wertige Charaktere von G. Dann sind $\chi_1, \dots, \chi_n$ linear unabhängige Elemente des Vektorraums* $\mathrm{Abb}(G, K)$.

Satz 1.14. *Sei L/K eine endliche separable Körpererweiterung. Dann gilt:*

(1) Es gibt ein $a \in L$ mit $\mathrm{Tr}_{L/K}(a) \neq 0$. Die K-lineare Abbildung $\mathrm{Tr}_{L/K}\colon L \to K$ ist somit surjektiv.

(2) Durch

$$(\ ,\ )\colon L \times L \to K,\ (a, b) \mapsto \mathrm{Tr}_{L/K}(ab)$$

wird eine nicht ausgeartete, symmetrische Bilinearform auf L definiert.

Beweis. Sei $n = [L : K]$ und seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Homomorphismen $L \to \overline{K}$. Die entsprechenden K-wertigen Charaktere $L^* \to \overline{K}$ sind nach dem vorhergehenden Theorem linear unabhängig in $\mathrm{Abb}(L^*, \overline{K})$. Insbesondere ist somit $\sum_{i=1}^n \sigma_i$ nicht die Nullabbildung in $\mathrm{Abb}(L^*, \overline{K})$. Also gibt es ein $a \in L^*$, sodass $\sum_{i=1}^n \sigma_i(a) \neq 0$. Dies zeigt Aussage (1), da $\mathrm{Tr}_{L/K}(a) = \sum_{i=1}^n \sigma_i(a)$ nach Satz 1.12. (Die Surjektivität von $\mathrm{Tr}_{L/K}$ folgt dann aus der K-Linearität.)

Es bleibt (2) zu zeigen. Die angegebene Abbildung ist offensichtlich bilinear und symmetrisch. Sei $a \in L$ mit $\mathrm{Tr}_{L/K}(a) \neq 0$. (Ein solches Element existiert nach Teil (1) des Satzes.) Dann gilt für ein beliebiges $b \in L^*$, dass

$$(b, ab^{-1}) = \mathrm{Tr}_{L/K}(bab^{-1}) = \mathrm{Tr}_{L/K}(a) \neq 0.$$

Also ist Abbildung auch nicht ausgeartet. □

Der folgende Satz zeigt, dass die Spur- und die Normabbildung sich transitiv bezüglich Körpererweiterungen verhalten:

Satz 1.15. *Sei $K \subseteq L \subseteq M$ eine Kette endlicher separabler Körpererweiterungen. Dann gilt*

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} \quad \textit{und} \quad \mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}\,.$$

Beweis. Sei $\overline{K}$ ein algebraischer Abschluss von K, sodass $K \subseteq L \subseteq M \subseteq \overline{K}$ gilt. Sei weiter $m = [L : K]$, $n = [M : L]$ und

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_m\}, \quad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_1, \ldots, \tau_n\}.$$

Wir wählen Fortsetzungen $\sigma_i' \colon \overline{K} \to \overline{K}$ der σ_i. Dann ist

$$\mathrm{Hom}_K(M, \overline{K}) = \{\sigma_i' \circ \tau_j \colon 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Sei $a \in M$. Es gilt

$$\mathrm{Tr}_{M/K}(a) = \sum_{i=1}^m \sum_{j=1}^n (\sigma_i' \circ \tau_j)(a) = \sum_{i=1}^m \sigma_i' \left(\sum_{j=1}^n \tau_j(a) \right).$$

Nach Satz 1.12 ist $\sum_{j=1}^n \tau_j(a) = \mathrm{Tr}_{M/L}(a)$, und da $\mathrm{Tr}_{M/L}(a) \in L$ sehen wir

$$\mathrm{Tr}_{M/K}(a) = \sum_{i=1}^m \sigma_i' \left(\mathrm{Tr}_{M/L}(a) \right) = \sum_{i=1}^m \sigma_i \left(\mathrm{Tr}_{M/L}(a) \right) = \mathrm{Tr}_{L/K} \left(\mathrm{Tr}_{M/L}(a) \right).$$

Analog erhält man

$$\mathrm{N}_{M/K}(a) = \prod_{i=1}^m \prod_{j=1}^n (\sigma_i' \circ \tau_j)(a) = \prod_{i=1}^m \sigma_i' \left(\prod_{j=1}^n \tau_j(a) \right) = \mathrm{N}_{L/K} \left(\mathrm{N}_{M/L}(a) \right).$$

□

Bemerkung. Der vorangegangene Satz gilt auch wenn die Kette endlicher Körpererweiterungen nicht mehr separabel ist.

Sei L/K eine endliche separable Körpererweiterung und $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von L über K. Wir definieren die **Diskriminante** dieser Basis als

$$d(\alpha_1, \ldots, \alpha_n) = \det\left((\alpha_i, \alpha_j)_{ij}\right),$$

wobei $(\alpha_i, \alpha_j) = \mathrm{Tr}_{L/K}(\alpha_i\alpha_j)$ wie in Satz 1.14. Da $\mathrm{Tr}_{L/K}$ nach K abbildet, ist die Diskriminante $d(\alpha_1, \ldots, \alpha_n)$ ebenfalls ein Element in K. Aus der linearen Algebra ist außerdem bekannt, dass die zu einer nicht ausgearteten, symmetrischen Bilinearform assoziierte Matrix nicht singulär ist, das heißt es ist

$$d(\alpha_1, \ldots, \alpha_n) = \det\left((\alpha_i, \alpha_j)_{ij}\right) \neq 0.$$

Zusammengefasst gilt also $d(\alpha_1, \ldots, \alpha_n) \in K^*$.

Seien nun $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Homomorphismen $L \to \overline{K}$. Dann gilt

$$(\alpha_i, \alpha_j) = \mathrm{Tr}_{L/K}(\alpha_i\alpha_j) = \sum_{l=1}^{n} \sigma_l(\alpha_i\alpha_j) = \sum_{l=1}^{n} \sigma_l(\alpha_i)\sigma_l(\alpha_j).$$

Des Weiteren lässt sich leicht nachrechnen, dass

$$(\sigma_i(\alpha_j))_{ij}^T \cdot (\sigma_i(\alpha_j))_{ij} = \left(\sum\nolimits_{l=1}^{n} \sigma_l(\alpha_i)\sigma_l(\alpha_j)\right)_{ij}.$$

Damit ergibt sich

$$d(\alpha_1, \ldots, \alpha_n) = \det\left((\sigma_i(\alpha_j))_{ij}^T\right) \cdot \det\left((\sigma_i(\alpha_j))_{ij}\right) = \left[\det\left((\sigma_i(\alpha_j))_{ij}\right)\right]^2$$

als alternative Form der Diskriminante.

Satz 1.16. *Sei A ein Integritätsbereich mit Quotientenkörper K und sei A ganz abgeschlossen in K. Sei weiterhin L/K eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L. Schließelich sei $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von L/K, welche in B enthalten ist. Dann gilt*

$$d(\alpha_1, \ldots, \alpha_n)B \ \subseteq \ A\alpha_1 + \ldots + A\alpha_n.$$

Insbesondere ist $d(\alpha_1, \ldots, \alpha_n) \in A$.

Bemerkung. In der Situation des Satzes finden wir immer eine Basis von L/K, welche in B enthalten ist. Um dies einzusehen sei $\{\alpha_1, \ldots, \alpha_n\}$ eine beliebige Basis von L/K. Nach Satz 1.7 gibt es zu jedem $\alpha_i \in L$ ein $a_i \in A$, $a_i \neq 0$, und ein $\beta_i \in B$, sodass $a_i\alpha_i = \beta_i$ ist. Wir behaupten, dass $\{\beta_1, \ldots, \beta_n\} \subseteq B$ eine Basis von L/K ist. Offensichtlich gilt

$$L = K\alpha_1 + \ldots + K\alpha_n = K\beta_1 + \ldots + K\beta_n.$$

Es bleibt daher zu zeigen, dass die Elemente $\beta_1, \ldots, \beta_n$ linear unabhängig über K sind. Sei

$$0 = \sum_{i=1}^{n} \lambda_i \beta_i = \sum_{i=1}^{n} (\lambda_i a_i) \alpha_i$$

mit $\lambda_i \in K$. Dann folgt $\lambda_i a_i = 0$, da die Elemente $\alpha_1, \ldots, \alpha_n$ linear unabhängig über K sind, und $\lambda_i a_i \in K$ gilt. Wegen $a_i \neq 0$ und da K ein Körper ist, folgt damit $\lambda_i = 0$ für alle i. Also sind die Elemente $\beta_1, \ldots, \beta_n$ wie gewünscht linear unabhängig über K.

Beweis von Satz 1.16. Sei $\alpha \in B \subseteq L$. Dann ist $\alpha = \sum_{j=1}^{n} a_j \alpha_j$ für geeignete $a_j \in K$ und

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha) = \sum_{j=1}^{n} a_j \, \mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$$

auf Grund der Linearität der Spurabbildung. Dies lässt sich umformulieren zu

$$\begin{pmatrix} \mathrm{Tr}_{L/K}(\alpha_1 \alpha) \\ \vdots \\ \mathrm{Tr}_{L/K}(\alpha_n \alpha) \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_{L/K}(\alpha_1 \alpha_1) & \cdots & \mathrm{Tr}_{L/K}(\alpha_1 \alpha_n) \\ \vdots & & \vdots \\ \mathrm{Tr}_{L/K}(\alpha_n \alpha_1) & \cdots & \mathrm{Tr}_{L/K}(\alpha_n \alpha_n) \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Da $\alpha_i \alpha$ und $\alpha_i \alpha_j$ Elemente von B sind, liegen die Elemente $\mathrm{Tr}_{L/K}(\alpha_i \alpha)$ und $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$ nach Satz 1.11 in A. Die Cramersche Regel (vergleiche Theorem 4.4, [Lan02, Kapitel 8]) liefert nun

$$a_i = \frac{c_i}{d(\alpha_1, \ldots, \alpha_n)}$$

für geeignete $c_i \in A$, denn die Determinante der Matrix $(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))_{ij}$ ist gerade die Diskriminante der gegebenen Basis. Also ist $d(\alpha_1, \ldots, \alpha_n) a_i \in A$, und somit

$$d(\alpha_1, \ldots, \alpha_n) \alpha = \sum_{i=1}^{n} (d(\alpha_1, \ldots, \alpha_n) a_i) \alpha_i \in A\alpha_1 + \ldots + A\alpha_n.$$

Außerdem gilt $d(\alpha_1, \ldots, \alpha_n) \in A$, da alle Einträge der entsprechenden Matrix in A enthalten sind, wie weiter oben bemerkt. □

Sei A wie eben ein Integritätsbereich mit Quotientenkörper K, A ganz abgeschlossen in K, L/K eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L. Eine Menge $\{\omega_1, \ldots, \omega_n\} \subseteq B$ heißt **A-Basis von B**, wenn sich jedes $b \in B$ eindeutig als Linearkombination $b = a_1\omega_1 + \ldots + a_n\omega_n$ für geeignete $a_i \in A$ schreiben lässt. Es gilt also

$$B = A\omega_1 \oplus \ldots \oplus A\omega_n,$$

das heißt B ist ein freier A-Modul vom Rang n.

Bemerkung. In diesem Fall ist $\{\omega_1, \ldots, \omega_n\}$ auch eine K-Basis von L: Nach Satz 1.7 ist jedes $\beta \in L$ von der Form $\beta = b/a$ mit $b \in B$ und $a \in A$. Somit gilt

$$\beta \in 1/a \cdot B \subseteq 1/a \cdot A\omega_1 + \ldots + 1/a \cdot A\omega_n \subseteq K\omega_1 + \ldots + K\omega_n$$

und daher $L = K\omega_1 + \ldots + L\omega_n$. Es bleibt zu zeigen, dass $\omega_1, \ldots, \omega_n$ auch linear unabhängig über K sind. Sei $0 = \lambda_1\omega_1 + \ldots + \lambda_n\omega_n$ mit $\lambda_i \in K$. Wir können ohne Beschränkung der Allgemeinheit annehmen, dass $\lambda_i \in A$, da K der Quotientenkörper von A ist. Aus der Eindeutigkeit der Darstellung eines Elementes in B folgt damit bereits $\lambda_i = 0$ für alle i. Also ist $\{\omega_1, \ldots, \omega_n\}$ tatsächlich eine K-Basis von L. Insbesondere gilt somit $n = [L : K]$.

Das folgende Theorem ist ein bekanntes Resultat aus der Algebra und wird im Weiteren von großem Nutzen sein. Insbesondere liefert es eine hinreichende Bedingung für die Existenz einer A-Basis in der obigen Situation.

Theorem 1.17. *Sei R ein Hauptidealring und M ein freier R-Modul vom Rang n. Dann ist jeder Untermodul von M frei vom Rang $m \leq n$.*

Für einen Beweis verweisen wir auf Theorem 7.1 in Kapitel 3 in [Lan02].

Satz 1.18. *Sei A ein Integritätsbereich und Hauptidealring mit Quotientenkörper K. Sei weiterhin L/K eine endliche separable Körpererweiterung mit $n = [L : K]$ und B der ganze Abschluss von A in L. Schließlich sei $M \subseteq L$ ein nicht-trivialer endlich erzeugter B-Modul. Dann ist M ein freier A-Modul vom Rang n. Insbesondere besitzt B eine A-Basis.*

Beweis. Wir bemerken zunächst, dass A als Hauptidealring ein faktorieller Ring ist, und damit ganz abgeschlossen in seinem Quotientenkörper K ist. Sei nun $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von L/K. Wie weiter oben bemerkt können wir ohne Beschränkung der Allgemeinheit annehmen, dass die Basis in B enthalten ist. Sei weiter $d = d(\alpha_1, \ldots, \alpha_n)$ die Diskriminante dieser Basis. Dann gilt nach Satz 1.16, dass

$$dB \subseteq A\alpha_1 + \ldots + A\alpha_n =: \Lambda.$$

Da $\{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L ist, sind die Elemente $\alpha_1, \ldots, \alpha_n$ linear unabhängig über K, also auch über A. Nach Konstruktion ist $\{\alpha_1, \ldots, \alpha_n\}$ somit auch eine A-Basis des A-Moduls Λ, welcher daher frei vom Rang n ist.

Nach Theorem 1.17 ist somit der A-Untermodul dB frei vom Rang $m \leq n$ und besitzt also eine A-Basis. Sei diese $\{d\nu_1, \ldots, d\nu_m\}$. Dann ist $\{\nu_1, \ldots, \nu_m\}$ eine A-Basis von B und B somit ebenfalls ein freier A-Modul vom Rang m. Weiterhin haben wir in der vorhergehenden Bemerkung gezeigt, dass damit durch $\{\nu_1, \ldots, \nu_m\}$ auch eine K-Basis von L gegeben ist. Also gilt $m = n$.

Sei nun $\{\mu_1, \ldots, \mu_l\} \subseteq L$ ein Erzeugendensystem von M über B. Nach Satz 1.7 gibt es zu jedem μ_i ein $a_i \in A$, $a_i \neq 0$, sodass $a_i\mu_i \in B$ ist. Setze $a := \prod_{i=1}^{l} a_i$. Dann gilt

$$aM \subseteq B.$$

Damit können wir erneut Theorem 1.17 anwenden, welches besagt, dass der A-Untermodul aM des freien A-Moduls B selbst frei ist mit

$$\operatorname{rank}(aM) \leq \operatorname{rank}(B) = n.$$

Wie zuvor für dB folgt, dass somit auch M ein freier A-Modul ist, welcher den gleichen Rang wie aM besitzt. Ferner ist M nach Voraussetzung ein endlich erzeugter B-Modul. Also gilt auch $\operatorname{rank}(B) \leq \operatorname{rank}(M)$ als A-Moduln. Dies zeigt $\operatorname{rank}(M) = n$. □

Den folgenden Satz werden wir erst in Kapitel 9 benötigen. Wir verzichten hier auf einen Beweis und verweisen stattdessen auf Proposition 2.11 auf Seite 13 in [Neu99].

Satz 1.19. *Sei A ein Integritätsbereich mit Quotientenkörper K und A ganz abgeschlossen in K. Seien L/K und L'/K zwei Galoiserweiterungen vom Grad n und n', sodass L und L' in einem gemeinsamen Erweiterungskörper enthalten sind und $L \cap L' = K$ gilt. Weiterhin sei B bzw. B' der ganze Abschluss von A in L bzw. L' und sei $\{\omega_1, \ldots, \omega_n\}$ bzw. $\{\omega'_1, \ldots, \omega'_{n'}\}$ eine A-Basis von B bzw. B' mit Diskriminante d bzw. d'. Schließlich gelte $xd + x'd' = 1$ für geeignete $x, x' \in A$. Dann ist*

$$\{\omega_i \omega'_j \colon 1 \leq i \leq n, 1 \leq j \leq n'\}$$

eine A-Basis des ganzen Abschlusses von A in LL' mit Diskriminante $d^{(n')} \cdot (d')^n$.

Der Ring der ganzen Zahlen $\mathbb{Z}$ ist als Hauptidealring ganz abgeschlossen in seinem Quotientenkörper $\mathbb{Q}$. Sei $K/\mathbb{Q}$ eine endliche Erweiterung, das heißt K ist ein algebraischer Zahlkörper. Dann bezeichnen wir mit $\mathcal{O}_K$ den **ganzen Abschluss von $\mathbb{Z}$ in K**. Sei $a \subseteq K$ ein endlich erzeugter $\mathcal{O}_K$-Modul. Dann ist a nach Satz 1.18 ein freier $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$. Das heißt es gibt $\alpha_1, \ldots, \alpha_n \in a$, sodass

$$a = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n.$$

Wir werden im Folgenden zeigen, dass die Diskriminante $d(\alpha_1, \ldots, \alpha_n)$ unabhängig von der Wahl der Basis ist:

Sei $\{\alpha'_1, \ldots, \alpha'_n\}$ eine weitere $\mathbb{Z}$-Basis von a. Dann ist

$$\alpha'_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

für geeignete $a_{ij} \in \mathbb{Z}$. Die Matrix $T := (a_{ij})_{ij}$ hat dementsprechend ganzzählige Einträge und ist invertierbar über $\mathbb{Z}$, da $\{\alpha_1, \ldots, \alpha_n\}$ und $\{\alpha'_1, \ldots, \alpha'_n\}$ Basen über $\mathbb{Z}$ sind. Somit gilt $\det(T)\det(T^{-1}) = 1$ und deshalb $\det(T) = \pm 1$. Außerdem lässt sich leicht nachrechnen, dass

$$\begin{aligned}(\alpha'_i, \alpha'_j)_{ij} &= \Big(\sum\nolimits_{l=1}^{n} a_{il}\alpha_l, \sum\nolimits_{m=1}^{n} a_{jm}\alpha_m\Big)_{ij} \\ &= \Big(\sum\nolimits_{l=1}^{n} a_{il} \sum\nolimits_{m=1}^{n} a_{jm}(\alpha_l, \alpha_m)\Big)_{ij} \\ &= \big(a_{il}\big)_{il} \cdot \big(\alpha_l, \alpha_m\big)_{lm} \cdot \big(a_{jm}\big)_{mj}.\end{aligned}$$

Offensichtlich ist

$$\det\big[(a_{il})_{il}\big] \cdot \det\big[(a_{mj})_{mj}\big] = \det(T)\det\big(T^T\big) = \big[\det(T)\big]^2 = 1.$$

Es folgt

$$d(\alpha'_1, \ldots, \alpha'_n) = \det\left[(\alpha'_i, \alpha'_j)_{ij}\right] = \det\left[(\alpha_l, \alpha_m)_{lm}\right] = d(\alpha_1, \ldots, \alpha_n).$$

Also ist die Diskriminante einer ganzzahligen Basis von a unabhängig von der Wahl dieser Basis. Wir definieren

$$d(a) := d(\alpha_1, \ldots, \alpha_n)$$

als die Diskriminante des endlich erzeugten $\mathcal{O}_K$-Moduls a.

Insbesondere können wir nun auch d_K, die **Diskriminante des algebraischen Zahlkörpers** K, definieren. Sei dazu $\{\omega_1, \ldots, \omega_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$. Dann ist die Diskriminante d_K von K gegeben durch

$$d_K := d(\mathcal{O}_K) = d(\omega_1, \ldots, \omega_n) = \det((\omega_i, \omega_j)_{ij}).$$

Wir haben bereits bemerkt, dass die Diskriminante im Allgemeinen ein Element des Quotientenkörpers und nicht Null ist. Da aber nach Satz 1.11 die Spur eines ganzen Elementes wieder in A bzw. in unserem Fall in $\mathbb{Z}$ liegt, gilt hier

$$d_K \in \mathbb{Z} \setminus \{0\}.$$

Beispiel. Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$, und $K = \mathbb{Q}(\sqrt{d}\,)$. Wir haben in einem vorhergehenden Beispiel gezeigt, dass der ganze Abschluss von $\mathbb{Z}$ in K durch

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$$

gegeben ist, wobei $\omega = \sqrt{d}$ für $d = 2, 3 \bmod 4$ und $\omega = (1 + \sqrt{d}\,)/2$ für $d = 1 \bmod 4$. Eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ ist daher durch $\{1, \omega\}$ gegeben. Sei $d = 2, 3 \bmod 4$. Dann gilt

$$d_K = d(1, \omega) = \det\left[\begin{pmatrix} (1,1) & (1,\omega) \\ (\omega,1) & (\omega,\omega) \end{pmatrix}\right] = \det\left[\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}\right] = 4d.$$

Analog lässt sich d_K für $d = 1 \bmod 4$ bestimmen, und man erhält

$$d_K = \begin{cases} d, & \text{falls } d = 1 \bmod 4, \\ 4d, & \text{falls } d = 2, 3 \bmod 4. \end{cases}$$

Wir schließen dieses Kapitel mit einem ersten Resultat für algebraische Zahlkörper, welches uns im Folgenden noch von Nutzen sein wird.

Satz 1.20. *Sei K ein algebraischer Zahlkörper und seien a, a' zwei endlich erzeugte $\mathcal{O}_K$-Untermoduln von K mit $\{0\} \subsetneq a \subseteq a'$. Dann hat a endlichen Index in a' und es gilt*

$$d(a) = |a'/a|^2 \cdot d(a').$$

Dies besagt insbesondere, dass der Index $|\mathcal{O}_K/a|$ für alle Ideale $a \neq \{0\}$ in $\mathcal{O}_K$ endlich ist, und dass deren Diskriminante gegeben ist durch

$$d(a) = |\mathcal{O}_K/a|^2 \, d_K.$$

Für den Beweis des Satzes nutzen wir das folgende bekannte Theorem, welches zum Beispiel als Theorem 7.8 in Kapitel 3 in [Lan02] zu finden ist.

Theorem 1.21 (Elementarteilersatz)**.** *Sei R ein Integritätsbereich und Hauptidealring, M ein freier R-Modul vom Rang $m < \infty$ und N ein Untermodul von M. Dann gibt es eine R-Basis $\{\alpha_1, \ldots, \alpha_m\}$ von M und Koeffizienten $c_1, \ldots, c_m \in R \setminus \{0\}$, sodass die Menge $\{c_1\alpha_1, \ldots c_m\alpha_m\}$ eine R-Basis von N ist und jedes c_i seinen Nachfolger c_{i+1} teilt.*

Beweis von Satz 1.20. Nach Satz 1.18 sind a und a' freie $\mathbb{Z}$-Moduln vom selben Rang $n = [K : \mathbb{Q}]$. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Z}$-Basis von a'. Nach dem Elementarteilersatz gibt es Elemente $c_1, \ldots, c_n \in \mathbb{Z} \setminus \{0\}$, sodass $\{c_1\alpha_1, \ldots, c_n\alpha_n\}$ eine $\mathbb{Z}$-Basis von a ist. Somit gilt

$$\begin{aligned} |a'/a| &= |(\mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n)/(\mathbb{Z}c_1\alpha_1 + \ldots + \mathbb{Z}c_n\alpha_n)| \\ &= |(\mathbb{Z}\alpha_1)/(\mathbb{Z}c_1\alpha_1)| \cdot \ldots \cdot |(\mathbb{Z}\alpha_n)/(\mathbb{Z}c_n\alpha_n)| \\ &= |c_1 \cdot \ldots \cdot c_n| , \end{aligned}$$

und daher

$$\begin{aligned} d(a) = \det\left[(c_i\alpha_i, c_j\alpha_j)_{ij}\right] &= \det\left[(c_ic_j(\alpha_i, \alpha_j))_{ij}\right] \\ &= c_1^2 \cdot \ldots \cdot c_n^2 \cdot \det\left[(\alpha_i, \alpha_j)_{ij}\right] = [a' : a]^2 \cdot d(a'). \end{aligned}$$

Dies zeigt die Behauptung. □

2 Ideale

Der Ring der ganzen Zahlen $\mathbb{Z}$ ist als Hauptidealring insbesondere eine faktorieller Ring, das heißt jedes $\alpha \in \mathbb{Z}$, welches keine Einheit ist, lässt sich eindeutig in irreduzible Elemente zerlegen.

Sei nun K ein algebraischer Zahlkörper und $\mathcal{O}_K$ der algebraische Abschluss von $\mathbb{Z}$ in K. Auch hier zerfällt jedes $\alpha \in \mathcal{O}_K$, das keine Einheit ist, in irreduzible Faktoren. Diese sind im Allgemeinen aber nicht eindeutig, das heißt $\mathcal{O}_K$ ist im Allgemeinen nicht mehr faktoriell. Im Folgenden zeigen wir zunächst, wie sich Elemente in $\mathcal{O}_K$ in ihre irreduziblen Faktoren zerlegen lassen, und betrachten anschließend ein Beispiel, in welchem eine solche Zerlegung nicht eindeutig ist. Dazu beginnen wir mit einem kleinen Satz, welcher die Einheiten in $\mathcal{O}_K$ charakterisiert.

Satz 2.1. *Sei A ein Integritätsbereich mit Quotientenkörper K und sei A ganz abgeschlossen in K. Sei L/K eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L. Dann ist $\mathrm{N}_{L/K}(b) \in A$ für jedes $b \in B$ und es gilt*

$$b \in B^* \quad \Longleftrightarrow \quad N_{L/K}(b) \in A^*.$$

Beweis. Der erste Teil wurde bereits in Satz 1.11 bewiesen. Sei $b \in B^*$. Dann gibt es $c \in B$, sodass $bc = 1$ ist, und es gilt

$$1 = \mathrm{N}_{L/K}(1) = \mathrm{N}_{L/K}(bc) = \mathrm{N}_{L/K}(b)\,\mathrm{N}_{L/K}(c).$$

Dies zeigt die Hinrichtung, da $\mathrm{N}_{L/K}(b)$ und $\mathrm{N}_{L/K}(c)$ in A liegen.

Sei nun $\overline{K}$ ein algebraischer Abschluss von K mit $K \subseteq L \subseteq \overline{K}$ und sei $n = [L : K]$. Seien weiter $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Homomorphismen $L \to \overline{K}$. Wir nehmen an, dass $\mathrm{N}_{L/K}(b) \in A^*$ für ein $b \in B$ ist. Dann gibt es $c \in A^*$, sodass $\mathrm{N}_{L/K}(b) \cdot c = 1$. Mit Satz 1.12 folgt

$$1 = \mathrm{N}_{L/K}(b) \cdot c = \sigma_1(b) \cdot \ldots \cdot \sigma_n(b) \cdot c.$$

Da die Identität auf L ein K-Homomorphismus $L \to \overline{K}$ ist, gilt $\sigma_k(b) = b$ für ein k. Somit ist

$$b \cdot \Big[c \cdot \prod\nolimits_{i \neq k} \sigma_i(b)\Big] = 1.$$

Wir behaupten, dass $\sigma_i(b) \in B$ für alle i. Sei dazu $f \in A[x]$ ein normiertes, nicht-triviales Polynom mit $f(b) = 0$. Offensichtlich gilt

$$f(\sigma_i(b)) = \sigma_i(f(b)) = 0,$$

und somit $\sigma_i(b) \in B$. Es folgt $b \in B^*$. □

Sei nun $\alpha \in \mathcal{O}_K$ reduzibel. Dann ist α insbesondere keine Einheit in $\mathcal{O}_K$, und es gibt eine Zerlegung $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathcal{O}_K$, wobei β und γ keine Einheiten sind. Es gilt

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \mathrm{N}_{K/\mathbb{Q}}(\beta) \cdot \mathrm{N}_{K/\mathbb{Q}}(\gamma).$$

Dabei ist $\mathrm{N}_{K/\mathbb{Q}}(\delta) \in \mathbb{Z}$ für alle $\delta \in \mathcal{O}_K$ nach Satz 1.11. Ferner gilt für $\delta \in \mathcal{O}_K$ nach Satz 2.1, dass $|\,\mathrm{N}_{K/\mathbb{Q}}(\delta)| = 1$ genau dann, wenn δ eine Einheit in $\mathcal{O}_K$ ist, und nach Satz 1.12 ist $\mathrm{N}_{K/\mathbb{Q}}(\delta) \neq 0$ für alle $\delta \in K$. Es folgt

$$1 < |\,\mathrm{N}_{K/\mathbb{Q}}(\beta)| < |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \quad \text{und} \quad 1 < |\,\mathrm{N}_{K/\mathbb{Q}}(\gamma)| < |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)|.$$

Sind β und γ nicht irreduzibel, so setzt man die Zerlegung fort und erhält dadurch eine Zerlegung von α in endlich viele irreduzible Faktoren.

Beispiel. Sei $K = \mathbb{Q}(\sqrt{-5}\,)$. Dann ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$, da $-5 = 3 \bmod 4$ ist. Wir behaupten, dass die Faktoren in der Zerlegung

$$21 = 3 \cdot 7 = \left(1 + 2\sqrt{-5}\,\right) \cdot \left(1 - 2\sqrt{-5}\,\right)$$

irreduzibel sind. Um dies einzusehen, sei $3 = \alpha\beta$ mit $\alpha, \beta \in \mathcal{O}_K$. Dann ist

$$9 = \mathrm{N}_{K/\mathbb{Q}}(3) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\,\mathrm{N}_{K/\mathbb{Q}}(\beta).$$

Sei $\alpha = x + y\sqrt{-5}$. Da die Gleichung

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = x^2 + 5y^2 = \pm 3$$

keine Lösung in $\mathbb{Z}$ besitzt, ist $|\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = 1$ oder $|\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = 9$. Im zweiten Fall ist $|\,\mathrm{N}_{K/\mathbb{Q}}(\beta)| = 1$. Somit ist entweder α oder β eine Einheit, und daher 3 irreduzibel über K. Analog lässt sich zeigen, dass auch 7 und $1 \pm 2\sqrt{-5}$ irreduzible Elemente in K sind.

Weiterhin behaupten wir, dass 3 auch nicht zu $1 \pm 2\sqrt{-5}$ assoziiert ist. Um dies zu zeigen nehmen wir an es gäbe $\alpha \in \mathcal{O}_K^*$, sodass $3 = \alpha \cdot (1 \pm 2\sqrt{-5}\,)$. Dann ist

$$9 = \mathrm{N}_{K/\mathbb{Q}}(3) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\,\mathrm{N}_{K/\mathbb{Q}}\left(1 \pm 2\sqrt{-5}\,\right) = 21 \cdot \mathrm{N}_{K/\mathbb{Q}}(\alpha),$$

und damit $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = 3/7 \notin \mathbb{Z}$. Dies ist ein Widerspruch.

Also besitzt das Element 21 in $K = \mathbb{Q}(\sqrt{-5}\,)$ keine eindeutige Zerlegung in irreduzible Faktoren.

Wir haben bereits gesehen, dass faktorielle Integritätsbereiche immer ganz abgeschlossen in ihrem Quotientenkörper sind. Das folgende Theorem besagt unter Anderem, dass der ganze Abschluss $\mathcal{O}_K$ von $\mathbb{Z}$ in K auch abgeschlossen in seinem eigenen Quotientenkörper ist, obwohl $\mathcal{O}_K$ im Allgemeinen kein faktorieller Integritätsbereich ist.

Theorem 2.2. *Sei K ein algebraischer Zahlkörper. Dann ist $\mathcal{O}_K$ ganz abgeschlossen, noethersch und jedes nicht-triviale Primideal p in $\mathcal{O}_K$ ist maximal.*

Beweis. Wir zeigen zunächst, dass $\mathcal{O}_K$ ganz abgeschlossen ist. Sei dazu L der Quotientenkörper von $\mathcal{O}_K$. Dieser ist der kleinste Körper, in welchen $\mathcal{O}_K$ eingebettet werden kann. Es gilt also $L \subseteq K$. Nach Satz 1.7 ist jedes Element in K von der Form a/b mit $a \in \mathcal{O}_K$ und $b \in \mathbb{Z}$, $b \neq 0$, also gilt auch $K \subseteq L$, und damit $K = L$. Also ist $\mathcal{O}_K$ ganz abgeschlossen, da $\mathcal{O}_K$ nach Definition ganz abgeschlossen in seinem Quotientenkörper K ist.

Als nächstes zeigen wir, dass $\mathcal{O}_K$ noethersch ist. Sei $a \subseteq \mathcal{O}_K \subseteq K$ ein Ideal in $\mathcal{O}_K$. Nach Satz 1.18 ist $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul von endlichem Rang $n = [K : \mathbb{Q}]$, und nach Satz 1.17 ist a damit ebenfalls ein freier $\mathbb{Z}$-Modul vom Rang $m \leq n$. Insbesondere ist a also endlich erzeugt als $\mathbb{Z}$-Modul, und somit erst recht endlich erzeugt als $\mathcal{O}_K$-Modul, denn $\mathbb{Z} \subseteq \mathcal{O}_K$. Also ist $\mathcal{O}_K$ auch nothersch.

Es bleibt zu zeigen, dass jedes nicht-triviale Primideal p in $\mathcal{O}_K$ maximal ist. Sei dazu $p \subsetneq \mathcal{O}_K$, $p \neq \{0\}$, ein Primideal und sei $m \subsetneq \mathcal{O}_K$ ein Ideal mit $p \subseteq m$. Wir wollen zeigen, dass $p = m$ gilt. Sei zunächst $y \in p$, $y \neq 0$. Dann erfüllt y eine Gleichung der Form

$$y^n + c_1 y^{n-1} + \ldots + c_{n-1} y + c_n = 0$$

für geeignete $c_i \in \mathbb{Z}$, $c_n \neq 0$. Also ist $c_n \in p$, und damit $p \cap \mathbb{Z}$ nicht trivial. Andererseits ist $p \cap \mathbb{Z}$ aber auch nicht ganz $\mathbb{Z}$, da ansonsten $p = \mathcal{O}_K$ wäre. Weiterhin ist $p \cap \mathbb{Z}$ ein Primideal in $\mathbb{Z}$, da p ein Primideal in $\mathcal{O}_K$ ist. Somit ist das Ideal $p \cap \mathbb{Z}$ maximal in $\mathbb{Z}$, denn $\mathbb{Z}$ ist ein Hauptidealring, und da $p \cap \mathbb{Z} \subseteq m \cap \mathbb{Z}$ gilt, ist entweder $p \cap \mathbb{Z} = m \cap \mathbb{Z}$ oder $m \cap \mathbb{Z} = \mathbb{Z}$. Letzteres widerspricht $m \subsetneq \mathcal{O}_K$, also gilt $p \cap \mathbb{Z} = m \cap \mathbb{Z}$. Es bleibt zu zeigen, dass dies auch $p = m$ impliziert.

Sei dazu $y \in m \setminus p$. Dann ist $y \in \mathcal{O}_K$, daher y ist ganz über $\mathbb{Z}$, und $y \neq 0$. Es gilt also

$$y^n + c_1 y^{n-1} + \ldots + c_{n-1} y + c_n = 0$$

für geeignete $c_i \in \mathbb{Z}$. Da m ein Ideal in $\mathcal{O}_K$ ist, gilt somit $c_n \in m$, also auch

$$c_n \in m \cap \mathbb{Z} = p \cap \mathbb{Z},$$

und damit $c_n \in p$. Weiter ergibt sich daher aus obiger Gleichheit, dass

$$y \cdot \left(y^{n-1} + c_1 y^{n-2} + \ldots + c_{n-1}\right) = -c_n \in p.$$

Da aber p ein Primideal ist und $y \notin p$ ist, folgt

$$y^{n-1} + c_1 y^{n-2} + \ldots + c_{n-1} \in p \subseteq m.$$

Das Argument lässt sich nun induktiv fortsetzen, sodass schließlich $c_1, c_2, \ldots, c_n \in p$ ist. Es folgt

$$y^n = -\left(c_1 y^{n-1} + \ldots + c_{n-1} y + c_n\right) \in p.$$

Da p ein Primideal ist, impliziert dies $y \in p$, was ein Widerspruch ist. Also gibt es kein solches $y \in m \setminus p$, das heißt es gilt $p = m$. □

Wir wollen Ringen, welche die Eigenschaften aus dem vorhergehenden Theorem erfüllen, einen eigenen Namen geben: Sei A ein Integritätsbereich. Ist A ganz abgeschlossen, noethersch und ist jedes nicht-triviale Primideal in A maximal, so bezeichnen wir A als **Dedekindring**. Theorem 2.2 lässt sich damit folgendermaßen formulieren:

Korollar 2.3. *Sei K ein algebraischer Zahlkörper. Dann ist $\mathcal{O}_K$ ein Dedekindring.*

Weiterhin wissen wir aus der Algebra, dass Hauptidealringe noethersch und faktoriell sind, und dass in Hauptidealringen Primideale maximal sind. Zusammen mit Satz 1.6 ergibt sich daher:

Theorem 2.4. *Sei A ein Integritätsbreich. Ist A ein Hauptidealring, so ist A auch ein Dedekindring.*

Sei $\mathcal{O}$ ein Dedekindring und seien $a, b \subseteq \mathcal{O}$ Ideale in $\mathcal{O}$. Wir definieren

$$ab := \left\{ \sum_{i=1}^{n} a_i b_i \colon a_i \in a, b_i \in b, n \in \mathbb{N} \right\}.$$

Offensichtlich gilt $ab \subseteq a$ und $ab \subseteq b$. Weiterhin schreiben wir $a|b$, falls $b \subseteq a$ ist. Ist $p \subseteq \mathcal{O}$ ein Primideal, so gilt

$$p|ab \quad \Longrightarrow \quad p|a \text{ oder } p|b.$$

Satz 2.5. *Sei $\mathcal{O}$ ein Dedekindring und a ein nicht-triviales Ideal in $\mathcal{O}$. Dann gibt es nicht-triviale Primideale $p_1, \ldots, p_n$ in $\mathcal{O}$, sodass gilt*

$$p_1 \ldots p_n \subseteq a.$$

Beweis. Sei M die Menge der nicht-trivialen Ideale in $\mathcal{O}$, für die es keine nicht-trivialen Primideale $p_1, \ldots, p_n$ mit $p_1 \ldots p_n \subseteq a$ gibt. Insbesondere enthält M also keine Primideale. Wir nehmen an, dass M nicht-leer ist. Da $\mathcal{O}$ noethersch ist, besitzt M ein bezüglich Inklusion maximales Element B. Dieses Element ist kein Primideal, da $B \in M$ ist. Es gibt also $b_1, b_2 \in \mathcal{O}$ mit $b_1 b_2 \in B$ und $b_1 \notin B$, $b_2 \notin B$. Wir setzen

$$B_1 := B + (b_1) \quad \text{und} \quad B_2 := B + (b_2).$$

Dann ist $B \subsetneq B_1$ und $B \subsetneq B_2$. Auf Grund der Maximalität von B sind B_1 und B_2 daher keine Elemente von M. Also enthalten B_1 und B_2 Produkte von Primidealen, und wegen

$$B_1 B_2 \subseteq B + B(b_1) + B(b_2) + (b_1 b_2) \subseteq B$$

gilt dies auch für B. Somit liegt B nicht in M, das heißt M ist leer. □

Satz 2.6. *Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K und $p \subseteq \mathcal{O}$ ein nicht-triviales Primideal in $\mathcal{O}$. Wir definieren*

$$p^{-1} = \{x \in K \colon xp \subseteq \mathcal{O}\}.$$

Dann gilt für jedes nicht-triviale Ideal a in $\mathcal{O}$, dass

$$a \subsetneq ap^{-1} := \left\{ \sum_{i=1}^{n} a_i x_i \colon a_i \in a, x_i \in p^{-1}, n \in \mathbb{N} \right\}.$$

Insbesondere ist

$$pp^{-1} = \mathcal{O}.$$

Beweis. Wir zeigen zunächst, dass $\mathcal{O} \subsetneq p^{-1}$ ist. Offensichtlich gilt $\mathcal{O} \subseteq p^{-1}$, denn es ist $xp \subseteq p$ für alle $x \in \mathcal{O}$. Es bleibt also ein Element in p^{-1} zu finden, welches nicht in $\mathcal{O}$ liegt. Sei dazu $a \in p$, $a \neq 0$. Nach dem vorhergehenden Satz gibt es Primideale $p_1, \ldots, p_n$ in $\mathcal{O}$, sodass $p_1 \ldots p_n \subseteq (a)$ gilt. Wir können annehmen, dass n minimal ist. Da $(a) \subseteq p$ ist, gilt auch $p_1 \ldots p_n \subseteq p$, und da p ein Primideal ist, folgt $p_i \subseteq p$ für ein i. Somit ist $p_i = p$, denn $\mathcal{O}$ ist ein Dedekindring und p_i daher maximal. Da wir n minimal gewählt haben, gilt weiterhin

$$\prod_{j \neq i} p_j \nsubseteq (a).$$

Also gibt es ein $b \in \prod_{j \neq i} p_j$ mit $b \notin (a) = \mathcal{O}a$, das heißt $a^{-1}b \notin \mathcal{O}$. Andererseits gilt aber

$$bp \subseteq \left(\prod_{j \neq i} p_j \right) p_i \subseteq (a) = \mathcal{O}a.$$

Also ist $a^{-1}bp \subseteq \mathcal{O}$, daher $a^{-1}b \in p^{-1}$ und damit $\mathcal{O} \subsetneq p^{-1}$.

Sei nun $a \subseteq \mathcal{O}$ ein nicht-triviales Ideal in $\mathcal{O}$. Wir wollen zeigen, dass $a \subsetneq ap^{-1}$ gilt. Offensichtlich gilt $a \subseteq ap^{-1}$ wegen $1 \in p^{-1}$. Wir nehmen an, dass $a = ap^{-1}$. Da $\mathcal{O}$ noethersch ist, ist a endlich erzeugt, das heißt es gilt

$$a = \mathcal{O}\alpha_1 + \ldots + \mathcal{O}\alpha_n$$

für geeignete $\alpha_i \in a$. Sei $x \in p^{-1}$. Dann gibt es $a_{ij} \in \mathcal{O}$, sodass für alle i gilt

$$\alpha_i x = \sum_{j=1}^{n} a_{ij}\alpha_j,$$

und damit

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})\alpha_j = 0.$$

Mit $A := (\delta_{ij}x - a_{ij})_{ij}$ erhalten wir daher $A\alpha = 0$. Sei B die zu A komplementäre Matrix. Dann gilt $BA = \det(A)E_n$ nach Theorem 1.2, also $\det(A)\alpha = BA\alpha = 0$ und damit $\det(A)\alpha_j = 0$ für alle j. Es folgt, dass $\det(A) = 0$ ist, da K als Körper nullteilerfrei ist und $a \neq \{0\}$. Weiterhin ist

$$0 = \det(A) = x^n + c_1 x^{n-1} + \ldots + c_{n-1}x + c_n$$

für geeignete $c_i \in A$. Somit ist x ganz über A, das heißt $x \in \mathcal{O}$. Da wir $x \in p^{-1}$ beliebig gewählt haben, folgt $p^{-1} \subseteq \mathcal{O}$ im Widerspruch zu $\mathcal{O} \subsetneq p^{-1}$. Also gilt in der Tat $a \subsetneq ap^{-1}$. Insbesondere gilt damit auch $p \subsetneq pp^{-1}$.

Es bleibt zu zeigen, dass $pp^{-1} = \mathcal{O}$ ist. Nach Definition von p^{-1} gilt $xp \subseteq \mathcal{O}$ für alle $x \in p^{-1}$. Also ist

$$p \subsetneq pp^{-1} \subseteq \mathcal{O}.$$

Da p als Primideal aber bereits maximal in $\mathcal{O}$ ist, folgt $pp^{-1} = \mathcal{O}$, falls pp^{-1} ein Ideal in $\mathcal{O}$ ist. Dies ist aber klar, wegen $\mathcal{O}(pp^{-1}) = (\mathcal{O}p)p^{-1} = pp^{-1}$. □

Theorem 2.7. *Sei $\mathcal{O}$ ein Dedekindring. Dann zerfällt jedes nicht-triviale Ideal a in $\mathcal{O}$ in ein Produkt*

$$a = p_1 \dots p_n$$

aus eindeutig bestimmten Primidealen $p_i \subseteq \mathcal{O}$.

Beweis. Wir beginnen damit, die Existenz einer solchen Faktorisierung zu zeigen. Sei dazu M die Menge aller nicht-trivialen Ideale in $\mathcal{O}$, welche sich nicht als Produkt endlich vieler Primideale schreiben lassen. Wir nehmen an, dass M nicht-leer ist. Dann besitzt M ein bezüglich Inklusion maximales Element a, da $\mathcal{O}$ noethersch ist. Wegen $a \in M$ ist a kein Primideal, also auch nicht maximal. Wir wissen aus der Algebra, dass jedes nicht-triviale Ideal in einem maximalen Ideal enthalten ist. Also gibt es ein maximales Ideal p in $\mathcal{O}$, sodass $a \subsetneq p \subsetneq \mathcal{O}$ ist. Insbesondere ist p als maximales Ideal auch ein Primideal. Nach Satz 2.6 gilt somit

$$a \subsetneq ap^{-1} \subseteq pp^{-1} = \mathcal{O}.$$

Wäre $ap^{-1} = \mathcal{O}$, so würde dies $p = \mathcal{O}p = ap^{-1}p = a\mathcal{O} = a$ implizieren. Da aber $a \subsetneq p$ ist, folgt $ap^{-1} \subsetneq \mathcal{O}$. Weiterhin ist ap^{-1} kein Element von M, da a bereits maximal in M ist und $a \subsetneq ap^{-1}$ gilt. Also gibt es Primideale $p_1, \dots, p_n$ in $\mathcal{O}$, sodass gilt

$$ap^{-1} = p_1 \dots p_n.$$

Damit folgt aber

$$a = a\mathcal{O} = ap^{-1}p = p_1 \dots p_n p.$$

Dies widerspricht $a \in M$. Also ist die Menge M leer.

Es verbleibt, die Eindeutigkeit einer solchen Zerlegung zu zeigen. Sei a ein nicht-triviales Ideal in $\mathcal{O}$ und

$$a = p_1 \dots p_n = q_1 \dots q_m$$

mit Primidealen $p_1, \dots, p_n$ und $q_1, \dots, q_m$ in $\mathcal{O}$. Dann ist

$$p_1 \supseteq p_1 \dots p_n = q_1 \dots q_m,$$

also $p_1 | q_1 \dots q_m$ und damit $p_1 | q_j$ für ein q_j, da p_1 prim ist. Da q_j als Primideal auch maximal ist, folgt bereits $p_1 = q_j$. Wir können ohne Beschränkung der Allgemeinheit annehmen, dass $j = 1$ ist. Es folgt

$$p_2 \dots p_n = p_1^{-1}(p_1 \dots p_n) = q_1^{-1}(q_1 \dots q_m) = q_2 \dots q_m.$$

Per Induktion und möglicher weiterer Umnummerierung ergibt sich nun $p_i = q_i$ für alle i, sowie $n = m$. □

Wir möchten an dieser Stelle kurz bemerken, dass sogar die Umkehrung von Theorem 2.7 gilt:

Theorem 2.8. *Sei $\mathcal{O}$ ein Integritätsbereich. Zerfällt jedes nicht-triviale Ideal in $\mathcal{O}$ in ein endliches Produkt von eindeutig bestimmten Primidealen, so ist $\mathcal{O}$ ein Dedekindring.*

Wir verzichten hier auf den Beweis und zeigen stattdessen, dass faktorielle Dedekindringe bereits Hauptidealringe sind. Aus der Algebra is außerdem bekannt, dass ein Integritätsbereich, der Hauptidealring ist, faktoriell ist. Wir weiter oben bemerkt sind diese Ringe ferner auch Dedekindringe. Das heißt, ein Integritätsbereich ist genau dann ein Hauptidealring, wenn er ein faktorieller Dedekindring ist.

Satz 2.9. *Sei $\mathcal{O}$ ein Dedekindring. Ist $\mathcal{O}$ faktoriell, so ist $\mathcal{O}$ ein Hauptidealring.*

Beweis. Sei P ein nicht-triviales Primideal in $\mathcal{O}$. Sei $x \in P$, $x \neq 0$. Dann ist $x \notin \mathcal{O}^*$ wegen $P \neq \mathcal{O}$. Da $\mathcal{O}$ faktoriell ist, zerfällt x in ein Produkt $x = p_1 \dots p_n$ von Primelementen $p_i \in \mathcal{O}$. Da P prim ist, folgt $p_i \in P$ für ein p_i. Damit gilt auch $(p_i) \subseteq P$. Das Ideal (p_i) ist prim, da p_i selbst prim ist, und somit maximal, da $\mathcal{O}$ ein Dedekindring ist. Also gilt $(p_i) = P$.

Sei nun a ein nicht-triviales Ideal in $\mathcal{O}$. Dann lässt sich a als Produkt von Primidealen $P_1, \dots, P_m$ schreiben, und wie zuvor gezeigt, gibt es zu jedem Primideal P_i ein Element $p_i \in P_i$ mit $(p_i) = P$. Somit ist

$$a = P_1 \dots P_m = (p_1) \dots (p_m) = (p_1 \dots p_m),$$

und damit $\mathcal{O}$ ein Hauptidealring. □

Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K. Wir nennen einen endlich erzeugten $\mathcal{O}$-Untermodul a von K, $a \neq \{0\}$, ein **gebrochenes Ideal** von K. Offensichtlich sind die nicht-Null Ideale in $\mathcal{O}$ gebrochene Ideale von K. Wir werden diese im Folgenden auch **ganzzahlige Ideale** von K nennen, und bemerken, dass $\{0\}$ zwar ein Ideal in $\mathcal{O}$ ist, aber nach Definition kein gebrochenes Ideal und damit auch kein ganzzahliges Ideal ist.

Satz 2.10. *Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K und $a \subseteq K$, $a \neq \{0\}$, ein $\mathcal{O}$-Modul. Dann sind die folgenden beiden Aussagen äquivalent:*

(1) Der $\mathcal{O}$-Modul a ist ein gebrochenes Ideal.

(2) Es gibt ein Element $c \in \mathcal{O}$, $c \neq 0$, sodass $ca \subseteq \mathcal{O}$ gilt.

Beweis. Wir nehmen zunächst an, dass a ein gebrochenes Ideal ist. Dann ist a endlich erzeugt, das heißt $a = \mathcal{O}\alpha_1 + \dots \mathcal{O}\alpha_n$ für geeignete $\alpha_i \in a \subseteq K$. Zu jedem α_i gibt es ein $c_i \in \mathcal{O}$, $c_i \neq 0$, sodass $c_i\alpha_i \in \mathcal{O}$ ist. Setze $c := c_1 \dots c_n$. Dann ist $c \neq 0$ und $ca \subseteq \mathcal{O}$. Dies zeigt die Hinrichtung.

Wir nehmen nun an, dass es ein Element $c \in \mathcal{O}$, $c \neq 0$, gibt, sodass $ca \subseteq \mathcal{O}$ ist. Dann ist ca ein $\mathcal{O}$-Modul in $\mathcal{O}$, und somit ein Ideal in $\mathcal{O}$. Dieses ist endlich erzeugt als $\mathcal{O}$-Modul, weil $\mathcal{O}$ noethersch ist. Damit ist aber auch a selbst ein endlich erzeugter $\mathcal{O}$-Modul. Dies zeigt die Rückrichtung. □

Sei $\mathcal{O}$ wie zuvor ein Dedekindring mit Quotientenkörper K. Dann definiert $a \in K^*$ das gebrochene Ideal $(a) = \mathcal{O}a$. Ferner definieren wir die Multiplikation von gebrochenen Idealen in K analog zur Multiplikation von ganzzahligen Idealen, das heißt

$$ab := \left\{ \sum_{i=1}^{n} a_i b_i \colon a_i \in a, b_i \in b, n \in \mathbb{N} \right\}$$

für gebrochene Ideale a und b von K. Wir wollen kurz nachprüfen, dass ab wieder ein gebrochenes Ideal von K ist. Zunächst ist klar, dass ab wieder ein $\mathcal{O}$-Modul ist. Weiter gibt es nach dem vorangegangenen Satz zu a und b Elemente $c, d \in \mathcal{O}$, $c, d \neq 0$, sodass $ca \subseteq \mathcal{O}$ und $db \subseteq \mathcal{O}$ gilt. Also ist wegen

$$cd \cdot ab = [ca] \cdot [db] \subseteq \mathcal{O}$$

auch ab ein gebrochenes Ideal von K. Die angegebene Multiplikation ist daher eine wohldefinierte Operation auf der Menge der gebrochenen Ideale.

Satz 2.11. *Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K. Dann bilden die gebrochenen Ideale in K eine abelsche Gruppe bezüglich der Multiplikation. Diese wird als* ***Idealgruppe*** *$\mathcal{J}_K$ bezeichnet. Die Identität ist durch*

$$(1) = \mathcal{O}$$

gegeben und das Inverse eines gebrochenen Ideals a ist

$$a^{-1} := \{x \in K \colon xa \subseteq \mathcal{O}\}.$$

Beweis. Wir bemerken zunächst, dass die Multiplikation von gebrochenen Idealen offensichtlich assoziativ und kommutativ ist. Sei a ein gebrochenes Ideal. Dann gilt

$$a(1) = \left\{\sum\nolimits_{i=1}^{n} a_i b_i \colon a_i \in a, b_i \in \mathcal{O}, n \in \mathbb{N}\right\} = a.$$

Also ist (1) die Identität der Multiplikation.

Sei nun p ein nicht-triviales Primideal von $\mathcal{O}$. Dann gilt $pp^{-1} = (1)$ nach Satz 2.6. Also besitzt p ein Inverses. Sei weiter a ein beliebiges nicht-triviales Ideal von $\mathcal{O}$. Dann ist $a = p_1 \dots p_n$ für geeignete Primideale p_i von $\mathcal{O}$. Setze

$$b := p_1^{-1} \dots p_n^{-1}.$$

Dann gilt $ab = (1)$ auf Grund der Assoziativität und Kommutativität der Multiplikation. Also ist $a\beta \subseteq \mathcal{O}$ für alle $\beta \in b$, und somit $b \subseteq a^{-1}$. Andererseits gilt aber

$$a^{-1} = a^{-1}(1) = a^{-1}ab \subseteq b,$$

da nach Definition $aa^{-1} \subseteq \mathcal{O}$ ist. Also ist $a^{-1} = b$, das heißt a^{-1} ist das Inverse von a.

Sei schließlich $a \subseteq K$ ein beliebiges gebrochenes Ideal von K. Dann gibt es $c \in \mathcal{O}$, $c \neq 0$, sodass $ca = (c)a \subseteq \mathcal{O}$ gilt. Weil ca somit ein Ideal in $\mathcal{O}$ ist, folgt

$$a(c)(ca)^{-1} = (ca)(ca)^{-1} = (1).$$

Es gilt also $a\beta \subseteq \mathcal{O}$ für alle $\beta \in (c)(ca)^{-1}$, und somit

$$(c)(ca)^{-1} \subseteq a^{-1}.$$

Andererseits gilt aber auch

$$a^{-1} = a^{-1}\mathcal{O} = a^{-1}a(c)(ca)^{-1} \subseteq \mathcal{O}(c)(ca)^{-1} = (c)(ca)^{-1}$$

wegen $aa^{-1} \subseteq \mathcal{O}$. Somit ist $a^{-1} = (c)(ca)^{-1}$. Das heißt, a^{-1} ist in der Tat das Inverse von a, denn $aa^{-1} = a(c)(ca)^{-1} = (1)$. □

Korollar 2.12. *Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K und $a \subseteq K$ ein gebrochenes Ideal. Dann besitzt a eine eindeutige Darstellung der Form*

$$a = \prod_p p^{\nu_p(a)},$$

*wobei das Produkt über alle nicht-trivialen Primideale p in $\mathcal{O}$ läuft und $\nu_p(a) \in \mathbb{Z}$ ist, sodass $\nu_p(a) = 0$ für fast alle Primideale p. Die Idealgruppe $\mathcal{J}_K$ ist also die **freie abelsche Gruppe** erzeugt von den nicht-trivialen Primidealen in $\mathcal{O}$.*

Beweis. Sei $a \subseteq K$ ein gebrochenes Ideal und sei $c \in \mathcal{O}$, $c \neq 0$, sodass $b := ca = (c)a$ ein ideal in $\mathcal{O}$ ist. Dann ist $a = b(c)^{-1}$ und wir wissen bereits, dass sich b und (c) eindeutig als Produkt von nicht-trivialen Primidealen in $\mathcal{O}$ schreiben lassen. Somit besitzt a eine Zerlegung der angebebenen Form. Die Eindeutigkeit dieser Zerlegung ist klar. □

Sei $\mathcal{O}$ wieder ein Dedekindring und K der Quotientenkörper von $\mathcal{O}$. Wir nennen ein gebrochenes Ideal A von K **gebrochenes Hauptideal**, wenn es ein $a \in K^*$ gibt, sodass $A = (a) := \mathcal{O}a$ ist. Weiter bezeichnen wir die Menge aller gebrochenen Hauptideale von K mit $\mathcal{P}_K$. Da die Abbildung

$$f\colon K^* \to \mathcal{J}_K,\ a \mapsto (a) := \mathcal{O}a$$

einen Gruppenhomomorphismus darstellt und $\mathcal{P}_K$ gerade das Bild von f ist, ist $\mathcal{P}_K$ eine Untergruppe der Idealgruppe $\mathcal{J}_K$. Da $\mathcal{J}_K$ abelsch ist, ist $\mathcal{P}_K$ normal, und wir können die Gruppe

$$\mathrm{CL}_K = \mathcal{J}_K/\mathcal{P}_K$$

definieren. Diese nennen wir **Idealklassengruppe** von K. Weiterhin ist

$$\ker(f) = \{a \in K^*\colon f(a) = (1)\} = \mathcal{O}^*,$$

denn gilt $\mathcal{O}a = \mathcal{O}$ für ein $a \in K^*$, so ist $a \in \mathcal{O}$ und es gibt $b \in \mathcal{O}$ mit $ab = 1$. Dadurch erhalten wir eine exakte Sequenz

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \xrightarrow{f} \mathcal{J}_K \longrightarrow \mathrm{CL}_K \longrightarrow 1\cdot$$

Der folgende Satz beschreibt die Bedeutung der Idealklassengruppe.

Satz 2.13. *Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K. Dann ist die Idealklassengruppe CL_K genau dann trivial, das heißt $\mathrm{CL}_K = \{(1)\}$, wenn $\mathcal{O}$ ein Hauptidealring ist.*

Beweis. Wir nehmen zunächst an, dass CL_K trivial ist. Sei a ein Ideal in $\mathcal{O}$. Dann ist die Nebenklasse von a in CL_K trivial, das heißt es gibt $x \in K^*$ mit $a = (x) = \mathcal{O}x$. Insbesondere gilt also $x \in a \subseteq \mathcal{O}$. Somit wir das Ideal a von $x \in \mathcal{O}$ erzeugt. Dies zeigt die Hinrichtung.

Nehme nun an, dass $\mathcal{O}$ ein Hauptidealring ist. Sei a ein gebrochenes Ideal von K und $c \in \mathcal{O}$, $c \neq 0$, sodass $ca \subseteq \mathcal{O}$ ist. Dann ist ca ein Ideal in $\mathcal{O}$, also $ca = (b)$ für ein $b \in \mathcal{O}$. Es folgt

$$a = c^{-1}(b) = \mathcal{O}c^{-1}b = (c^{-1}b).$$

Damit ist jedes Element in $\mathcal{J}_K$ ein gebrochenes Hauptideal, und CL_K somit trivial. □

Die Idealklassengruppe beschreibt also die Abweichung von $\mathcal{O}$ von einem Hauptidealring. Sei K nun ein algebraischer Zahlkörper und $\mathcal{O}_K$ der Ring der ganzen Zahlen in K. Wir werden sehen, dass CL_K in diesem Fall eine endliche Gruppe ist. Weiter werden wir die Ordnung $h_k := |\,\mathrm{CL}_K\,|$ der Gruppe als **Klassenzahl** von K bezeichnen. Es gilt:

Theorem 2.14 (Heegner, Stark)**.** *Sei $K = \mathbb{Q}(\sqrt{d}\,)$ mit $d < 0$ quadratfrei. Dann gilt genau dann $h_K = 1$, wenn*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Dies wurde größtenteils 1952 von Kurt Heegner gezeigt, und die noch vorhandenen Lücken im Beweis wurden 1969 von Harold Stark ergänzt. Zuvor hatte Stark im Jahre 1967 bereits einen eigenen unabhängigen Beweis des Problems gegeben.

Satz 2.15. *Sei $\mathcal{O}$ ein Dedekindring und seien $a, b \subseteq \mathcal{O}$ nicht-triviale Ideale in $\mathcal{O}$.*

(1) Es gilt genau dann $a \subseteq b$, wenn es ein Ideal c in $\mathcal{O}$ mit $a = bc$ gibt.

(2) Die Ideale in $\mathcal{O}$, welche a enthalten, sind gerade die Ideale der Form

$$\prod_p p^{r(p)}$$

mit $0 \leq r(p) \leq \nu_p(a)$ für alle p.

(3) Es gilt

$$\nu_p(a + b) = \min\left(\nu_p(a), \nu_p(b)\right), \tag{i}$$
$$\nu_p(a \cap b) = \max\left(\nu_p(a), \nu_p(b)\right), \tag{ii}$$
$$\nu_p(ab) = \nu_p(a) + \nu_p(b). \tag{iii}$$

Beweis. Wir beginnen mit der Hinrichtung in (1). Sei $a \subseteq b$. Setze $c = b^{-1}a$. Dann ist $c \subseteq b^{-1}b = \mathcal{O}$, und damit c ein Ideal in $\mathcal{O}$ mit $a = bc$. Die Rückrichtung ist klar, da $a = bc \subseteq b$ wegen $c \subseteq \mathcal{O}$ ist.

Für (2) sei b ein Ideal in $\mathcal{O}$, welches a enthält. Offensichtlich gilt $\nu_p(b) \geq 0$ für alle nicht-trivialen Primideale p in $\mathcal{O}$, da b ein Ideal in $\mathcal{O}$ ist. Es bleibt also zu zeigen, dass auch $\nu_p(b) \leq \nu_p(a)$ für alle p gilt. Nach (1) gibt es zunächst ein Ideal c in $\mathcal{O}$ mit $a = bc$. Es gilt

$$a = \prod_p p^{\nu_p(a)}$$

und

$$\prod_p p^{\nu_p(bc)} = bc = \left(\prod_p p^{\nu_p(b)}\right)\left(\prod_p p^{\nu_p(c)}\right) = \prod_p p^{\nu_p(b)+\nu_p(c)}.$$

Aus der Eindeutigkeit der Zerlegung in nicht-triviale Primideale folgt

$$\nu_p(a) = \nu_p(bc) = \nu_p(b) + \nu_p(c) \quad \text{für alle } p,$$

und wegen $\nu_p(c) \geq 0$ ist damit auch $\nu_p(b) \leq \nu_p(a)$ für alle p.

Es verbleibt die Gleichungen in (3) zu zeigen. Für (i) bemerken wir, dass $a + b$ das kleinste Ideal ist, welches a und b enthält. Dies trifft gerade auf

$$\prod_p p^{\min(\nu_p(a),\nu_p(b))}$$

zu. Analog ergibt sich Gleichung (ii) dann aus der Tatsache, dass $a \cap b$ gerade das größte Ideal ist, das in a und b enthalten ist. Gleichung (iii) ist klar. □

3 Gitter

Sei V ein n-dimensionaler Vektorraum über $\mathbb{R}$. Ein **Gitter** in V ist eine Untergruppe der Form

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

mit linear unabhängigen Vektoren $v_1, \ldots, v_m$ in V. Die Menge $\{v_1, \ldots, v_m\}$ wird als eine **Basis** von Γ und

$$\Phi = \{x_1v_1 + \ldots + x_mv_m \colon x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

als **Fundamentalparallelotop** bezeichnet. Wir nennen ein Gitter Γ **vollständig**, wenn $m = n$ ist. Offensichtlich gilt genau dann $V = \bigcup_{\gamma\in\Gamma}(\gamma + \Phi)$, wenn Γ vollständig ist.

Theorem 3.1. *Sei V ein n-dimensionaler hausdorffscher topologischer Vektorraum über $\mathbb{R}$. Ist $f \colon V \to \mathbb{R}^n$ ein linearer Isomorphismus, so ist f ein Homöomorphismus bezüglich der Standardtopologie des $\mathbb{R}^n$.*

Wir verzichten hier auf einen Beweis. Im Folgenden wird V immer einen n-dimensionalen hausdorffschen topologischen Vektorraum über $\mathbb{R}$ bezeichnen, und nach obigem Theorem können wir annehmen, dass dieser mit der Standardtopologie versehen ist.

Theorem 3.2. *Sei V ein n-dimensionaler Vektorraum über $\mathbb{R}$ und sei Γ eine Untergruppe von V. Dann ist Γ genau dann ein Gitter in V, wenn Γ diskret in V ist.*

Beweis. Sei zunächst Γ ein Gitter in V und $\gamma \in \Gamma$. Wir wollen zeigen, dass es eine offene Menge $U \subseteq V$ mit $U \cap \Gamma = \{\gamma\}$ gibt. Sei $\{v_1, \ldots, v_m\}$ eine Basis von Γ. Wir erweitern diese zu einer Basis $\{v_1, \ldots, v_n\}$ von V. Dann ist $\gamma = \sum_{i=1}^m a_iv_i$ für geeignete $a_i \in \mathbb{R}$. Wir definieren

$$U = \{x_1v_1 + \ldots + x_nv_n \colon x_1, \ldots, x_n \in \mathbb{R} \text{ und } |x_i - a_i| < 1 \text{ für } i = 1, \ldots, m\}.$$

Sei $\mu = \sum_{i=1}^m x_iv_i \in U \cap \Gamma$. Dann ist

$$\gamma - \nu = \sum_{i=1}^m (a_i - x_i)v_i \in \Gamma.$$

Wegen $|a_i - x_i| < 1$ folgt $x_i = a_i$ für $i = 1, \ldots, m$, und damit $\mu = \gamma$. Dies zeigt die Hinrichtung.

Für die Rückrichtung sei Γ eine diskrete Untergruppe von V. Wir zeigen zunächst, dass Γ abgeschlossen in V ist. Sei dazu U eine offene Umgebung von 0. Dann gibt es eine offene Umgebung $U' \subseteq U$ von 0 mit $U' = -U'$ und $U' + U' \subseteq U$. Sei $x \in \overline{\Gamma} \setminus \Gamma$. Dann

gibt es eine Folge $(x_i)_i$ in Γ mit $x_i \to x$ und $x_i \neq x_j$ für alle $i \neq j$, da V hausdorffsch ist. Insbesondere gibt es also ein $k \in \mathbb{N}$, sodass $x_i \in x + U'$ für alle $i \geq k$ gilt. Setze $y := x_k - x_{k+1}$. Dann ist $y \in \Gamma$ und $y \neq 0$ wegen $x_k \neq x_{k+1}$. Weiter gilt

$$y = (x_k - x) - (x_{k+1} - x) \in U' - U' = U' + U' \subseteq U.$$

Es ist also

$$y \in (U \cap \Gamma) \setminus \{0\}.$$

Da wir U beliebig gewählt haben, gibt es für jede Nullumgebung U ein solches Element. Dies widerspricht der Tatsache, dass Γ diskret in V ist, da 0 in diesem Fall kein isolierter Punkt wäre. Also ist $\overline{\Gamma} \setminus \Gamma$ leer und somit Γ abgeschlossen in V.

Als nächstes zeigen wir, dass die Untergruppe Γ ein Gitter Γ_0 enthält, sodass $|\Gamma/\Gamma_0|$ endlich ist. Sei dazu V_0 der von Γ erzeugte Untervektorraum von V, und m die Dimension von V_0. Wir können eine Basis $\{u_1, \ldots, u_m\}$ von V_0 wählen, welche in Γ enthalten ist. Definiere

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

Dann ist Γ_0 ein Gitter. Es gilt

$$\Gamma = \bigcup_{\mu \in \Gamma/\Gamma_0} \mu + \Gamma_0.$$

Offensichtlich können wir die Repräsentanten μ der Nebenklassen in

$$\Phi_0 = \{x_1u_1 + \ldots + x_mu_m \colon x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

wählen. Da Γ diskret und abgeschlossen in V ist, und

$$\overline{\Phi_0} = \{x_1u_1 + \ldots + x_mu_m \colon x_i \in \mathbb{R}, 0 \leq x_i \leq 1\}$$

kompakt in V ist, ist der Schnitt $\Phi_0 \cap \Gamma$ endlich. Damit gibt es auch nur endlich viele verschiedene Repräsentanten für Nebenklassen, das heißt $|\Gamma/\Gamma_0|$ ist endlich.

Schließlich zeigen wir, dass Γ ein Gitter ist: Sei $q = |\Gamma/\Gamma_0|$. Dann ist $q(\mu + \Gamma_0) = \Gamma_0$ für beliebiges $\mu \in \Gamma$, also $q\mu \in \Gamma_0$ für jeden $\mu\Gamma$ und damit $q\Gamma \subseteq \Gamma_0$. Es folgt

$$\Gamma \subseteq \frac{1}{q}\,\Gamma_0 = \mathbb{Z}\,\frac{1}{q}\,u_1 + \ldots + \mathbb{Z}\,\frac{1}{q}\,u_m.$$

Die Gruppe Γ ist also ein Untermodul des freien $\mathbb{Z}$-Moduls $q^{-1}\Gamma_0$. Nach Theorem 1.17 ist Γ somit ein freier $\mathbb{Z}$-Modul vom Rang $r \leq m$. Sei $\{v_1, \ldots, v_r\}$ eine Basis von Γ. Dann gilt

$$\operatorname{span}(v_1, \ldots, v_r) = \operatorname{span}(\Gamma) = V_0,$$

das heißt die Vektoren $v_1, \ldots, v_r$ erzeugen bereits den Untervektorraum V_0. Es folgt $r = m$. Damit müssen $v_1, \ldots, v_r$ auch linear unabhängig sein, da diese ansonsten nicht V_0 erzeugen könnten. Also ist Γ ein Gitter in V. □

Wir nennen eine Teilmenge M eines Vektorraums V **beschränkt**, wenn es für jede offene Umgebung U von 0 ein $s > 0$ gibt, sodass $M \subseteq tU$ für alle $t > s$ gilt.

Satz 3.3. *Sei V ein n-dimensionaler Vektorraum über $\mathbb{R}$ und $\Gamma \subseteq V$ ein Gitter. Dann ist Γ genau dann vollständig, wenn es eine beschränkte Teilmenge M von V gibt, sodass gilt*

$$V = \bigcup_{\gamma \in \Gamma} (\gamma + M).$$

Beweis. Sei zunächst Γ vollständig. Sei weiterhin $\{v_1, \ldots, v_n\}$ eine Basis von Γ. Wir setzen

$$M := \Phi = \{x_1 v_1 + \ldots + x_n v_n \colon x_i \in \mathbb{R}, 0 \leq x_i < 1\}.$$

Dann ist M beschränkt und es gilt offensichtlich $V = \bigcup_{\gamma \in \Gamma}(\gamma + M)$. Dies zeigt die Hinrichtung.

Sei nun $M \subseteq V$ beschränkt mit $V = \bigcup_{\gamma \in \Gamma}(\gamma + M)$ und sei V_0 der von Γ erzeugte Untervektorraum. Dann gibt es zu $v \in V$ und $m \in \mathbb{N}$ Elemente $\mu_m \in M$ und $\gamma_m \in \Gamma$ mit

$$mv = \mu_m + \gamma_m.$$

Somit ist $v = m^{-1}\mu_m + m^{-1}\gamma_m$ und es folgt

$$v = \lim_{m \to \infty} \frac{1}{m} \mu_m + \lim_{m \to \infty} \frac{1}{m} \gamma_m.$$

Da M beschränkt ist, gilt $m^{-1}\mu_m \to 0$, und damit $m^{-1}\gamma_m \to v$. Da ferner $m^{-1}\gamma_m \in V_0$ für jedes m gilt, und V_0 als Untervektorraum abgeschlossen ist, folgt $v \in V_0$. Also gilt $V = V_0$ und somit ist das Gitter Γ vollständig, was die Rückrichtung beweist. □

Sei nun V ein n-dimensionaler euklidischer Vektorraum mit zugehöriger Bilinearform

$$(\ ,\ ) \colon V \times V \to \mathbb{R}.$$

Ferner sei $\{e_1, \ldots, e_n\}$ eine Orthonormalsbasis von V. Dann lässt sich für Parallelotope

$$\Phi(v_1, \ldots, v_n) := \{x_1 v_1 + \ldots + x_n v_n \colon x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

mit $v_1, \ldots, v_n$ linear unabhängig ein natürlicher Volumenbegriff erklären, nämlich

$$\mathrm{vol}(\Phi(v_1, \ldots, v_n)) = |\det((a_{ij})_{ij})|,$$

wobei $a_{ij} \in \mathbb{R}$ mit $v_i = \sum_{j=1}^{n} a_{ij} e_j$ für $i = 1, \ldots, n$. Insbesondere besitzt der Einheitswürfel $\Phi(e_1, \ldots, e_n)$ Volumen 1. Allgemeiner lässt sich V bei festgehaltener Basis $\{e_1, \ldots, e_n\}$ mit dem Vektorraum $\mathbb{R}^n$ identifizieren. Der eingeführte Volumenbegriff fällt dann mit dem Lebesgue Maß zusammen. Dadurch können wir beliebigen (meßbaren) Teilmengen von V ein Volumen zuordnen.

Sei Γ ein vollständiges Gitter in V mit Basis $\{v_1, \ldots, v_n\}$ und mit Fundamentalparallelotop Φ. Wir definieren das Volumen des Gitters Γ als das Volumen seines Fundamentalparallelotops Γ, das heißt

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(\Phi) = |\det((a_{ij})_{ij})|,$$

wobei $a_{ij} \in \mathbb{R}$ mit $v_i = \sum_{j=1}^{n} a_{ij} e_j$ für $i = 1, \ldots, n$. Dies ist wohldefiniert, das heißt unabhängig von der Wahl der Basis von Γ, da eine entsprechende Transformationsmatrix ganzzahlig invertierbar ist, und damit Determinante ± 1 besitzt.

Wir setzen $A := (a_{ij})_{ij}$. Weiter setzen wir $d_{ij} = (v_i, v_j)$ und $D := (d_{ij})_{ij}$. Dann gilt

$$d_{ij} = \sum_{k,l} (a_{ik} e_k, a_{jl} e_l) = \sum_{k,l} a_{ik} a_{jl} \delta_{kl} = \sum_{k} a_{ik} a_{jk}.$$

Es folgt $D = AA^T$ und damit

$$\mathrm{vol}(\Gamma) = |\det(A)| = \sqrt{|\det(D)|}.$$

Die Matrix D wird als **Grammatrix** von Γ bezeichnet und es lässt sich zeigen, dass die Determinante von D unabhängig von der Wahl der Basis von Γ ist. Wir definieren

$$\det(\Gamma) := \det(D).$$

Schließlich nennen wir eine Teilmenge X von V **symmetrisch**, falls $X = -X$ gilt, und **konvex**, falls für alle $x, y \in X$, $t \in [0, 1]$ auch $tx + (1 - t)y \in X$ gilt.

Theorem 3.4 (Minkowski's Theorem)**.** *Sei V ein n-dimensionaler euklidischer Vektorraum, $X \subseteq V$ symmetrisch und konvex und $\Gamma \subseteq V$ ein vollständiges Gitter. Ist*

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

so enthält X mindestens ein $\gamma \in \Gamma$, $\gamma \neq 0$.

Beweis. Wir nehmen an, dass $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma)$ erfüllt ist. Es reicht zu zeigen, dass es zwei voneinander verschiedene Gitterpunkte γ_1, γ_2 in Γ gibt, sodass

$$\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_2 + \frac{1}{2}X\right) \neq \emptyset. \qquad (\star)$$

Denn ist τ ein Element im Schnitt, so gilt $\tau = \gamma_1 + \frac{1}{2}x_1 = \gamma_2 + \frac{1}{2}x_2$ für geeignete $x_1, x_2 \in X$, und damit

$$\gamma_1 - \gamma_2 = \frac{1}{2}x_2 + \frac{1}{2}(-x_1) \in \Gamma \cap X,$$

da X symmetrisch und konvex ist.

Wir nehmen nun an, dass $(\star)$ nicht gilt, daher dass die Mengen $\gamma+\frac{1}{2}X$ für unterschiedliche $\gamma \in \Gamma$ disjunkt sind. Dann gilt dies natürlich auch für die Mengen $(\gamma_i + \frac{1}{2}X) \cap \Phi$, wobei Φ ein Fundamentalparallelotop von Γ ist. Es folgt

$$\operatorname{vol}(\Gamma) \geq \operatorname{vol}\left[\bigcup\nolimits_{\gamma\in\Gamma}\left(\left(\gamma+\frac{1}{2}X\right)\cap\Phi\right)\right] = \sum_{\gamma\in\Gamma}\operatorname{vol}\left[\left(\gamma+\frac{1}{2}X\right)\cap\Phi\right].$$

Weiterhin ist für alle $\gamma \in \Gamma$

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

Da das Volumen translationsinvariant ist, gilt somit für alle $\gamma \in \Gamma$, dass

$$\operatorname{vol}\left[\left(\gamma+\frac{1}{2}X\right)\cap\Phi\right] = \operatorname{vol}\left[\frac{1}{2}X\cap(-\gamma+\Phi)\right],$$

und mit $V = \bigcup_{\gamma\in\Gamma}(-\gamma+\Phi)$ folgt

$$\sum_{\gamma\in\Gamma}\operatorname{vol}\left[\frac{1}{2}X\cap(-\gamma+\Phi)\right] \geq \operatorname{vol}\left[\frac{1}{2}X\cap\left(\bigcup\nolimits_{\gamma\in\Gamma}(-\gamma+\Phi)\right)\right] = \operatorname{vol}\left(\frac{1}{2}X\right).$$

Zusammengesetzt ergibt dies

$$\operatorname{vol}(\Gamma) \geq \sum_{\gamma\in\Gamma}\operatorname{vol}\left[\left(\gamma+\frac{1}{2}X\right)\cap\Phi\right] \geq \operatorname{vol}\left(\frac{1}{2}X\right) = 2^{-n}\operatorname{vol}(X),$$

was der Annahme $\operatorname{vol}(X) > 2^n \operatorname{vol}(\Gamma)$ widerspricht. Damit folgt $(\star)$ und somit die Aussage des Theorems. □

4 Minkowski-Theorie

Aus der Algebra ist bekannt, dass die Zahlen $z \in \mathbb{C}$, welche algebraisch über $\mathbb{Q}$ sind, einen algebraischen Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ bilden. Sei K ein algebraischer Zahlkörper vom Grad $n = [K : \mathbb{Q}]$. Dann ist K als endliche Körpererweiterung von $\mathbb{Q}$ insbesondere algebraisch über $\mathbb{Q}$. Also können wir annehmen, dass

$$\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$$

gilt. Der algebraische Abschluss $\overline{\mathbb{Q}}$ ist dann natürlich auch ein algebraischer Abschluss von K, das heißt wir können annehmen, dass $\overline{K} = \overline{\mathbb{Q}}$ ist. Als nächstes zerlegen wir die $\mathbb{Q}$-Homomorphismen von K nach $\overline{K}$ in reelle und komplexe Einbettungen

$$\delta_1, \dots, \delta_r \colon K \to \mathbb{R} \quad \text{und} \quad \sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s} \colon K \to \mathbb{C}$$

mit $n = r + 2s$. Dabei ist $\overline{\sigma}_i(a) = \overline{\sigma_i(a)}$ für alle i und alle $a \in K$. Sei $K_{\mathbb{C}} := \mathbb{C}^n$. Wir definieren die Abbildungen

$$j \colon K \to K_{\mathbb{C}},\ a \mapsto (\delta_1(a), \dots, \delta_r(a), \sigma_1(a), \overline{\sigma_1}(a), \dots, \sigma_s(a), \overline{\sigma_s}(a))$$

und

$$F \colon K_{\mathbb{C}} \to K_{\mathbb{C}},\ (x_1, \dots, x_n) \mapsto (\overline{x_1}, \dots, \overline{x_r}, \overline{x_{r+2}}, \overline{x_{r+1}}, \dots, \overline{x_n}, \overline{x_{n-1}})\,.$$

Weiterhin versehen wir $K_{\mathbb{C}}$ mit dem kanonischen Skalarprodukt $(x, y) = \sum_{i=1}^{n} x_i \overline{y_i}$. Dann ist $(Fx, Fy) = \overline{(x, y)}$. Sei

$$\mathrm{Tr} \colon K_{\mathbb{C}} \to \mathbb{C},\ x \mapsto \sum_{i=1}^{n} x_i.$$

Dann gilt für $a \in K$, dass

$$\mathrm{Tr}_{K/\mathbb{Q}}(a) = \sum_{i=1}^{r} \delta_i(a) + \sum_{i=1}^{s} (\sigma_i(a) + \overline{\sigma_i}(a)) = \mathrm{Tr}(j(a)).$$

Wir definieren $K_{\mathbb{R}} = (K_{\mathbb{C}})^+ := \{x \in K_{\mathbb{C}} \colon Fx = x\}$. Offenbar ist

$$K_{\mathbb{R}} = \{(x_1, \dots, x_n) \in K_{\mathbb{C}} \colon x_1, \dots, x_r \in \mathbb{R} \text{ und } x_{r+1} = \overline{x_{r+2}}, \dots, x_{n-1} = \overline{x_n}\}\,.$$

Die Einschränkung des Skalarprodukts $(\cdot, \cdot)$ auf $K_{\mathbb{R}}$ liefert ein Skalarprodukt auf dem Raum $K_{\mathbb{R}}$, denn für $x, y \in K_{\mathbb{R}}$ ist $(x, y) = (Fx, Fy) = \overline{(x, y)}$, also $(x, y) \in \mathbb{R}$. Weiterhin ist $j(K) \subseteq K_{\mathbb{R}}$, und für $x \in K_{\mathbb{R}}$ ist

$$\mathrm{Tr}(x) = \mathrm{Tr}(Fx) = \sum_{i=1}^{n} \overline{x_i} = \overline{\mathrm{Tr}(x)},$$

also $\mathrm{Tr}(K_{\mathbb{R}}) \subseteq \mathbb{R}$. Versehen wir $\mathbb{R}^{r+2s}$ mit dem Skalarprodukt

$$(x, y) := \sum_{i=1}^{r} x_i y_i + 2 \sum_{i=r+1}^{n} x_i y_i,$$

so definiert die Abbildung

$$f\colon K_{\mathbb{R}} \to \mathbb{R}^{r+2s},\ (x_1, \ldots, x_n) \mapsto \begin{array}{l} \big(x_1, \ldots, x_r, \mathrm{Re}(x_{r+1}), \mathrm{Im}(x_{r+1}), \\ \quad \mathrm{Re}(x_{r+3}), \mathrm{Im}(x_{r+3}), \ldots, \mathrm{Re}(x_{n-1}), \mathrm{Im}(x_{n-1})\big) \end{array}$$

eine Isometrie euklidischer Vektorräume, denn die Abbildung f ist offensichtlich bijektiv und für $x, y \in K_{\mathbb{R}}$ gilt

$$\begin{aligned} (f(x), f(y)) &= \sum_{i=1}^{r} x_i y_i + 2 \sum_{i=1}^{s} \mathrm{Re}(x_{r+2i-1}) \,\mathrm{Re}(y_{r+2i-1}) + 2 \sum_{i=1}^{s} \mathrm{Im}(x_{r+2i-1}) \,\mathrm{Im}(y_{r+2i-1}) \\ &= \sum_{i=1}^{r} x_i y_i + 2 \sum_{i=1}^{s} \mathrm{Re}\left(x_{r+2i-1}\ \overline{y_{r+2i-1}}\right) \\ &= \sum_{i=1}^{r} x_i y_i + \sum_{i=1}^{s} \left(x_{r+2i-1}\ \overline{y_{r+2i-1}} + x_{r+2i}\ \overline{y_{r+2i}}\right) \\ &= (x, y). \end{aligned}$$

Mit Hilfe dieser Isometrie können wir den durch das Skalarprodukt auf $K_{\mathbb{R}}$ induzierten kanonischen Volumenbegriff in ein Verhältnis zu dem durch das Lebesgue-Maß gegebenen Volumenbegriff auf $\mathbb{R}^{r+2s}$ setzen. Genauer gilt

$$\mathrm{vol}(X) = 2^s \cdot \lambda(f(X))$$

für eine meßbare Menge $X \subseteq K_{\mathbb{R}}$, wobei λ das Lebesgue-Maß auf $\mathbb{R}^{r+2s}$ bezeichnet.

Satz 4.1. *Sei K ein algebraischer Zahlkörper und a ein ganzzahliges Ideal in K. Dann ist durch $\Gamma := j(a)$ ein vollständiges Gitter in $K_{\mathbb{R}}$ gegeben und es gilt*

$$\mathrm{vol}(\Gamma) = \sqrt{|d(a)|}.$$

Beweis. Als Ideal in $\mathcal{O}_K$ ist a auch ein $\mathcal{O}_K$-Modul. Dieses ist endlich erzeugt, da $\mathcal{O}_K$ als Dedekindring noethersch ist. Nach Satz 1.18 ist a damit ein freier $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von a. Dann ist

$$\Gamma = \mathbb{Z} j(\alpha_1) + \ldots + \mathbb{Z} j(\alpha_n),$$

das heißt Γ ist ein Gitter in $K_{\mathbb{R}}$. Weiter lässt sich zeigen, dass die $j(\alpha_i)$ auch linear unabhängig sind. Somit ist das Gitter Γ vollständig. Wir setzen

$$A := \begin{pmatrix} \delta_1(\alpha_1) & \cdots & \delta_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \overline{\sigma_s}(\alpha_1) & \cdots & \overline{\sigma_s}(\alpha_n) \end{pmatrix}.$$

Die Diskriminante von a ist dann gegeben durch $d(a) = d(\alpha_1, \ldots, \alpha_n) = \det(A)^2$. Weiterhin setzen wir $D := (d_{ik})_{ik}$ mit

$$\begin{aligned} d_{ik} &= (j(\alpha_i), j(\alpha_k)) \\ &= \delta_1(\alpha_i)\overline{\delta_1(\alpha_k)} + \ldots + \delta_r(\alpha_i)\overline{\delta_r(\alpha_k)} + \sigma_1(\alpha_i)\overline{\sigma_1(\alpha_k)} + \ldots + \overline{\sigma_s(\alpha_k)}\sigma_s(\alpha_i). \end{aligned}$$

Dann ist $D = A\overline{A}^T$, und es gilt $\mathrm{vol}(\Gamma) = \det(D)^{1/2}$, da D gerade die in Kapitel 3 definierte Grammatrix von Γ ist. Es folgt

$$\mathrm{vol}(\Gamma) = \left(\det(A)\,\overline{\det\,(A^T)}\right)^{1/2} = |\det(A)| = \sqrt{|d(a)|}. \qquad \square$$

Theorem 4.2. *Sei K ein algebraischer Zahlkörper, $n = [K : \mathbb{Q}]$ und a ein ganzzahliges Ideal in K. Dann gibt es zu gegebenen positiven reellen Zahlen $c_1, \ldots, c_n$ mit*

$$c_{r+1} = c_{r+2}, c_{r+3} = c_{r+4}, \ldots, c_{n-1} = c_n \quad \textit{und} \quad \prod_{i=1}^{n} c_i > \left(\frac{2}{\pi}\right)^s \sqrt{|d(a)|}$$

ein Element $x \in a$, $x \neq 0$, mit

$$|\delta_1(x)| < c_1, \ldots, |\delta_r(x)| < c_r, |\sigma_1(x)| < c_{r+1}, |\sigma_2(x)| < c_{r+3}, \ldots, |\sigma_s(x)| < c_{n-1}.$$

Wir bemerken, dass in der Situation des Theorems natürlich auch

$$|\overline{\sigma_1}(x)| < c_{r+2}, |\overline{\sigma_2}(x)| < c_{r+4}, \ldots, |\overline{\sigma_s}(x)| < c_n$$

gilt. Dies ist klar wegen $|\overline{\sigma_i}(x)| = |\sigma_i(x)|$ und $c_{r+2i-1} = c_{r+2i}$ für $i = 1, \ldots, s$.

Beweis. Sei $X := \{x \in K_{\mathbb{R}} \colon |x_i| < c_i\}$. Dann ist

$$f(X) = \left\{ y \in \mathbb{R}^{r+2s} \colon \begin{array}{l} |y_i| < c_1 \text{ für } i = 1, \ldots, r \text{ und} \\ \left(y_{r+i}^2 + y_{r+i+1}^2\right)^{1/2} < c_{r+i} \text{ für } i = 1, 3, 5, \ldots, 2s-1 \end{array} \right\}$$

und damit

$$\mathrm{vol}(f(X)) = \prod_{i=1}^{r} 2c_i \cdot \prod_{i=1}^{s} \pi c_{r+2i-1}^2 = 2^r \pi^s \prod_{i=1}^{n} c_i$$

wegen $_{r+1} = c_{r+2}, \ldots, c_{n-1} = c_n$. Nach Voraussetzung gilt also

$$\mathrm{vol}(f(X)) > 2^{r+s}\sqrt{|d(a)|}.$$

Wir setzen $\Gamma := j(a)$. Dann ist durch Γ nach Satz 4.1 ein vollständiges Gitter gegeben und es gilt $\mathrm{vol}(\Gamma) = |d(a)|^{1/2}$. Schließlich lässt sich zeigen, dass das Volumen von X gerade das 2^s-fache des Volumens von $f(X)$ ist. Es folgt

$$\mathrm{vol}(X) = 2^s \,\mathrm{vol}(f(X)) > 2^n \,\mathrm{vol}(\Gamma).$$

Da X auch symmetrisch und konvex ist, lässt sich Theorem 3.4 anwenden. Das heißt, es gibt ein $\gamma \in X \cap \Gamma$, $\gamma \neq 0$. Da alle δ_i und alle σ_i als Körperhomomorphismen injektiv sind, ist auch j eine injektive Abbildung. Somit gibt es ein eindeutiges $x \in a$ mit $j(x) = \gamma$. Offensichtlich ist $x \neq 0$ und wegen $j(x) \in X$ erfüllt x gerade die Bedingungen des Theorems. $\square$

5 Die Klassenzahl

Sei K ein algebraischer Zahlkörper und a ein ganzzahliges Ideal in K. Wir setzen

$$\mathfrak{N}(a) := |\mathcal{O}_K/a|.$$

Im Folgenden werden wir zeigen, dass $\mathfrak{N}$ eine Norm auf der Menge der gebrochenen Ideale $\mathcal{J}_K$ in K induziert. Diese erweitert die Norm $\mathrm{N}_{K/\mathbb{Q}}$ auf natürliche Art:

Satz 5.1. *Sei K ein algebraischer Zahlkörper und $x \in \mathcal{O}_K$. Dann gilt*

$$\mathfrak{N}((x)) = \left|\mathrm{N}_{K/\mathbb{Q}}(x)\right|.$$

Beweis. Das Ideal $(x) = \mathcal{O}_K x$ ist ein ganzzahliges Ideal in K. Nach dem Elementarteilersatz (Theorem 1.21) gibt es eine $\mathbb{Z}$-Basis $\{\omega_1, \ldots, \omega_n\}$ von $\mathcal{O}_K$ und ganze Zahlen $c_1, \ldots, c_n$, $c_i \neq 0$, sodass $\{c_1\omega_1, \ldots, c_n\omega_n\}$ eine Basis von (x) ist. Wir haben also

$$\begin{array}{ccccccc} \mathcal{O}_K & = & \mathbb{Z}\omega_1 & + & \ldots & + & \mathbb{Z}\omega_n, \\ K & = & \mathbb{Q}\omega_1 & + & \ldots & + & \mathbb{Q}\omega_n, \\ (x) & = & \mathbb{Z}c_1\omega_1 & + & \ldots & + & \mathbb{Z}c_n\omega_n. \end{array}$$

Dann gilt

$$x\omega_i = \sum_{j=1}^{n} a_{ij}c_j\omega_j$$

für geeignete $a_{ij} \in \mathbb{Z}$. Da die Elemente $\{x\omega_1, \ldots, x\omega_n\}$ ebenfalls eine $\mathbb{Z}$-Basis von (x) bilden ist die Matrix $(a_{ij})_{ij}$ ganzzahlig invertierbar, das heißt es gilt $\det((a_{ij})_{ij}) = \pm 1$. Es folgt

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| = |\det((a_{ij}c_j)_{ij})| = |c_1 \ldots c_n| \cdot |\det((a_{ij})_{ij})| = |c_1 \ldots c_n|.$$

Andererseits ist auch $|\mathcal{O}_K/(x)| = |c_1 \ldots c_n|$, wie im Beweis von Satz 1.20 zu sehen ist. Also gilt $|\mathrm{N}_{K/\mathbb{Q}}(x)| = \mathfrak{N}((x))$. □

Satz 5.2. *Sei K ein algebraischer Zahlkörper. Sind a, b ganzzahlige Ideale in K, so gilt*

$$\mathfrak{N}(ab) = \mathfrak{N}(a)\mathfrak{N}(b).$$

Die Normabbildung $\mathfrak{N}$ kann also zu einem Homomorphismus

$$\mathfrak{N}\colon \mathcal{J}_K \to (0, \infty)$$

fortgesetzt werden.

Für einen Beweis verweisen wir auf [Neu99, Seite 35].

Lemma 5.3. *Sei K ein algebraischer Zahlkörper und a ein ganzzahliges Ideal in K. Dann gibt es ein Element $x \in a$, $x \neq 0$, mit*

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d(a)|}$$

wobei $[K : \mathbb{Q}] = n = r + 2s$ wie im vorangegangenen Kapitel ist.

Beweis. Sei $\varepsilon > 0$. Wähle $c_1, \ldots, c_n > 0$ mit $c_{r+1} = c_{r+2}, \ldots, c_{n-1} = c_n$ und

$$\prod_{i=1}^{n} c_i = \left(\frac{2}{\pi}\right)^s \sqrt{|d(a)|} + \varepsilon.$$

Dann gibt es nach Theorem 4.2 ein $x_\varepsilon \in a$, $x_\varepsilon \neq 0$, mit

$$|\mathrm{N}_{K/\mathbb{Q}}(x_\varepsilon)| = \prod_{i=1}^{r} |\delta_i(x_\varepsilon)| \cdot \prod_{i=1}^{s} |\sigma_i(x_\varepsilon)|^2 < \prod_{i=1}^{n} c_i = \left(\frac{2}{\pi}\right)^s \sqrt{|d(a)|} + \varepsilon.$$

Da dies für alle $\varepsilon > 0$ gilt und $|\mathrm{N}_{K/\mathbb{Q}}(x_\varepsilon)|$ eine positive ganze Zahl ist, gibt es auch ein Element $x \in a$, $x \neq 0$, mit $|\mathrm{N}_{K/\mathbb{Q}}(x)| \leq (2/\pi)^s |d(a)|^{1/2}$. □

Wir benutzen dieses Lemma um das folgende wichtige Theorem zu beweisen.

Theorem 5.4. *Sei K ein algebraischer Zahlkörper. Dann ist die Idealklassengruppe $\mathrm{CL}_K = \mathcal{J}_K/\mathcal{P}_K$ endlich.*

Beweis. Sei P ein nicht-triviales Primideal in $\mathcal{O}_K$. Dann ist $P \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{Z}$. Da P als Primideal auch maximal in $\mathcal{O}_K$ ist, ist $\mathcal{O}_K/P$ ein endlicher Körper mit Primkörper $\mathbb{F}_p$, das heißt $\mathcal{O}_K/P$ ist eine endliche Erweiterung von $\mathbb{F}_p$. Es folgt $\mathfrak{N}(P) = p^f$ für ein $f \in \mathbb{N}$.

Für eine gegebene Primzahl $p \in \mathbb{Z}$ gibt es aber nur endlich viele nicht-triviale Primideale P in $\mathcal{O}_K$ mit $P \cap \mathbb{Z} = p\mathbb{Z}$, denn in diesem Fall ist $p \in P$, also $(p) \subseteq P$ und damit $0 \leq \nu_q(P) \leq \nu_q((p))$ für alle nicht-trivialen Primideale q in $\mathcal{O}_K$. Es folgt, dass es für eine gegebene Schranke $M > 0$ nur endlich viele nicht-triviale Primideale P mit $\mathfrak{N}(P) \leq M$ gibt, da es auch nur endlich viele Primzahlen p mit $p \leq M$ gibt.

Weiter wissen wir, dass jedes ganzzahlige Ideal in K eindeutig in ein Produkt von nicht-trivialen Primidealen zerfällt. Auf Grund der Multiplikativität der Norm $\mathfrak{N}$ gibt es zu einer gegebenen Schranke $M > 0$ somit auch nur endlich viele ganzzahlige Ideale A in K mit $\mathfrak{N}(A) \leq M$. Es reicht daher zu zeigen, dass jede Klasse $[A] \in \mathcal{J}_K/\mathcal{P}_K$ ein ganzzahliges Ideal A mit

$$\mathfrak{N}(A) \leq M := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

enthält, wobei $[K : \mathbb{Q}] = n = r + 2s$ wie zuvor ist.

Sei dazu $A \in \mathcal{J}_K$ ein beliebiger Repräsentant einer Klasse $[A] \in \mathcal{J}_K/\mathcal{P}_K$. Dann gibt es nach Satz 2.10 ein Element $\gamma \in \mathcal{O}_K$, $\gamma \neq 0$, sodass $B := \gamma A^{-1} \subseteq \mathcal{O}_K$ ein ganzzahliges Ideal in K ist. Nach Lemma 5.3 gibt es zu B ein Element $b \in B$, $b \neq 0$, mit

$$|\mathrm{N}_{K/\mathbb{Q}}(b)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, \mathfrak{N}(B).$$

Setze $B' := bB^{-1}$. Dann ist B' ein ganzzahliges Ideal in K wegen $B' \subseteq BB^{-1} = \mathcal{O}_K$ und B' liegt in der selben Klasse $[A]$ wie A, denn $B' = b\gamma^{-1}A = (b\gamma^{-1})A$. Weiter gilt

$$\mathfrak{N}(B') = \mathfrak{N}\left((b)B^{-1}\right) = \mathfrak{N}((b))\ \mathfrak{N}\left(B^{-1}\right) = \frac{\mathrm{N}_{K/\mathbb{Q}}(b)}{\mathfrak{N}(B)} \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} = M.$$

Dies zeigt die Behauptung. □

Im Folgenden wenden wir uns nun quadratischen Erweiterungen von $\mathbb{Q}$ zu. Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$ und $K = \mathbb{Q}(\sqrt{d}\,)$. Wir wissen bereits, dass für $z = x + y\sqrt{d} \in K$ gilt

$$\mathrm{Tr}_{K/\mathbb{Q}}(z) = 2x \quad \text{und} \quad \mathrm{N}_{K/\mathbb{Q}}(z) = x^2 - dy^2.$$

Weiterhin haben wir gezeigt, dass $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ mit

$$\omega = \begin{cases} (1+\sqrt{d})/2, & \text{falls } d = 1 \bmod 4, \\ \sqrt{d}, & \text{falls } d = 2, 3 \bmod 4, \end{cases}$$

und dass

$$d_K = \begin{cases} d, & \text{falls } d = 1 \bmod 4, \\ 4d, & \text{falls } d = 2, 3 \bmod 4. \end{cases}$$

Satz 5.5. *Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$ und $K = \mathbb{Q}(\sqrt{d}\,)$. Sei weiter A ein ganzzahliges Ideal in K und definiere $a > 0$ durch $A \cap \mathbb{Z} = a\mathbb{Z}$. Schließlich sei*

$$a_2 = \min\{y \in \mathbb{N} \colon x + y\omega \in A\},$$
$$a_1 = \min\{x \in \mathbb{N}_0 \colon x + a_2\omega \in A\}.$$

Dann ist $a_1 < a$, $A = a\mathbb{Z} + (a_1 + a_2\omega)\mathbb{Z}$ und $\mathfrak{N}(A) = aa_2$.

Beweis. Wir bemerken zunächst, dass A als ganzzahliges Ideal in K ein Ideal in $\mathcal{O}_K$ ist, das heißt es gilt $A \subseteq \mathbb{Z} + \mathbb{Z}\omega$. Sei nun $x + y\omega \in A$. Wir werden im Folgenden zeigen, dass a_2 sowohl x als auch y teilt. Division mit Rest ergibt $y = qa_2 + r$ mit $0 \leq r < a_2$. Es folgt

$$(x - qa_1) + r\omega = (x + y\omega) - q(a_1 + a_2\omega) \in A,$$

da $a_1 + a_2\omega$ nach Konstruktion in A liegt, und damit $r = 0$ wegen der Minimalität von a_2. Also ist $y = qa_2$, das heißt a_2 teilt y.

Für $d = 2, 3 \bmod 4$ ist $\omega^2 = d \in \mathbb{Z}$. Daher folgt aus

$$yd + x\omega = \omega(x + y\omega) \in A$$

bereits, dass a_2 auch x teilt. Im Falle $d = 1 \bmod 4$ ist $\omega^2 = \omega + (d-1)/4$. Hier folgt aus

$$\frac{d-1}{4}y + (x+y)\omega = \omega(x + y\omega) \in A$$

zunächst, dass $x + y$ von a_2 geteilt wird, und damit dann dass a_2 auch x teilt.

Insbesondere teilt a_2 somit die Elemente a und a_1, denn nach Konstruktion ist $a \in A$ und $a_1 + a_2\omega \in A$. Weiterhin bemerken wir in diesem Zusammenhang, dass wegen $(a_1 - a) + a_2\omega \in A$ und wegen der Minimalität von a_1, $a_1 - a < 0$ gelten muss.

Sei nun $x + y\omega \in A$ wieder beliebig. Dann ist

$$x - \frac{a_1}{a_2}y = (x + y\omega) - \frac{y}{a_2}(a_1 + a_2\omega) \in \mathbb{Z} \cap A = a\mathbb{Z},$$

das heißt $x - ya_1/a_2 = ma$ für ein $m \in \mathbb{Z}$, und damit

$$x + y\omega = ma + \frac{y}{a_2}(a_1 + a_2\omega).$$

Es folgt

$$A \subseteq \mathbb{Z}a + \mathbb{Z}(a_1 + a_2\omega) \subseteq A + A = A,$$

also $A = \mathbb{Z}a + \mathbb{Z}(a_1 + a_2\omega)$. Setze $\alpha_1 := a$ und $\alpha_2 := a_1 + a_2\omega$. Dann ist durch $\{\alpha_1, \alpha_2\}$ eine $\mathbb{Z}$-Basis von A gegeben. Im Falle $d = 2, 3 \bmod 4$ ergibt sich

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^2) = 2a^2, \quad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_2) = 2aa_1, \quad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_2^2) = 2(a_1^2 + da_2^2).$$

Also ist

$$d(A) = \det\left[\begin{pmatrix} 2a^2 & 2aa_1 \\ 2aa_1 & 2(a_1^2 + da_2^2) \end{pmatrix}\right] = 4da^2a_2^2$$

und

$$\mathfrak{N}(A)^2 = |\mathcal{O}_K/A|^2 = \frac{d(A)}{d_K} = a^2a_2^2.$$

Ist $d = 1 \bmod 4$ so findet man analog

$$d(A) = da^2a_2^2 \quad \text{und} \quad \mathfrak{N}(A) = a^2a_2^2. \qquad \square$$

Zum Abschluss dieses Abschnitts benutzen wir den vorangegangenen Satz um beispielhaft die Klassenzahl eines bestimmten algebraischen Zahlkörpers zu bestimmen.

Satz 5.6. *Die Klassenzahl des algebraischen Zahlkörpers $K = \mathbb{Q}(\sqrt{-5}\,)$ ist $h_K = 2$.*

Beweis. Wir bemerken zunächst, dass die $\mathbb{Q}$-Homomorphismen $K \to \overline{K}$ gerade durch die Identität und die Konjugation $x + y\sqrt{-5} \mapsto x - y\sqrt{-5}$ gegeben sind. Insbesondere ist damit $r = 0$ und $s = 1$. Weiterhin gilt $\omega = \sqrt{-5}$ und $d_K = -20$.

Im Beweis von Theorem 5.4 haben wir gezeigt, dass jede Idealklasse in CL_K einen ganzzahligen Repräsentanten A besitzt mit

$$\mathfrak{N}(A) \leq M := \frac{2}{\pi}\sqrt{20} < 3.$$

Sei A ein ganzzahliges Ideal. Ist $\mathfrak{N}(A) = 1$, so folgt $A = \mathcal{O}_K$ per Definition der Normabbildung. Sei $\mathfrak{N}(A) = 2$. Dann ist A ein maximales Ideal in $\mathcal{O}_K$, also auch ein Primideal, und es gilt $A \cap \mathbb{Z} = 2\mathbb{Z}$. Insbesondere gilt damit $2 \in A$, also $(2) = 2\mathcal{O}_K \subseteq A$. Nach Satz 5.5 ist damit

$$A = 2\mathbb{Z} + (a_1 + a_2\omega)\mathbb{Z}$$

mit $0 \leq a_1 < 2$ und $a_2 = \mathfrak{N}(A)/a = 1$. Wegen $\omega^2 = -5 \notin 2\mathbb{Z}$ ist $2\mathbb{Z} + \omega\mathbb{Z}$ kein Ideal in $\mathcal{O}_K$. Also ist $a_1 = 1$ und $A = 2\mathbb{Z} + (1 + \omega)\mathbb{Z}$. Es lässt sich leicht nachprüfen, dass dieses A tatsächlich ein Ideal in $\mathcal{O}_K$ mit $\mathfrak{N}(A) = 2$ ist.

Es kann also höchstens zwei unterschiedliche Idealklassen in CL_K geben, da es überhaupt nur zwei unterschiedliche ganzzahlige Ideale A in K mit $\mathfrak{N}(A) < 3$ gibt. Also gilt $h_K = 1$ oder $h_K = 2$. Angenommen die Klassenzahl ist $h_K = 1$. Dann ist $\mathcal{O}_K$ ein Hauptidealring. Also gibt es $a = x + y\omega \in \mathcal{O}_K$, sodass $(a) = A := 2\mathbb{Z} + (1 + \omega)\mathbb{Z}$. Dann gilt aber

$$x^2 + 5y^2 = \mathrm{N}_{K/\mathbb{Q}}(a) = \mathfrak{N}(A) = 2.$$

Da dies ein Widerspruch ist, folgt $h_K = 2$. □

6 Dirichlet's Einheitensatz

Sei K ein algebraischer Zahlkörper. In diesem Abschnitt untersuchen wir die Einheitengruppe von $\mathcal{O}_K$.

Beispiel. Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$ und $K = \mathbb{Q}(\sqrt{d}\,)$. Es ist

$$\mathcal{O}_K^* = \left\{x \in \mathcal{O}_K \colon |\mathrm{N}_{K/\mathbb{Q}}(x)| = 1\right\}.$$

Für negative d zeigt man leicht, dass

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1, \pm i\}, & \text{falls } d = -1, \\ \{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}, & \text{falls } d = -3, \\ \{\pm 1\}, & \text{ansonsten} \end{cases}$$

wegen $\mathrm{N}_{K/\mathbb{Q}}(x + y\omega) = x^2 + (-d)y^2$. Für $d > 0$ ist die Bestimmung der Einheitengruppe $\mathcal{O}_K^*$ deutlich schwieriger. Es gilt beispielsweise

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2}\,)}^* = \left\{\pm\left(1 + \sqrt{2}\right)^n : n \in \mathbb{Z}\right\}.$$

Man beachte, dass die Einheitengruppe in diesem Fall nicht endlich ist.

Satz 6.1. *Sei K ein algebraischer Zahlkörper. Dann bilden die Einheitswurzeln*

$$\mu(K) = \{x \in K \colon x^m = 1 \text{ für ein } m \in \mathbb{N}\}$$

eine endliche Untergruppe von $\mathcal{O}_K^*$.

Beweis. Wegen $x^{m_x} - 1 = 0$ für $x \in \mu(K)$ bilden die Einheitswurzeln eine Untergruppe von $\mathcal{O}_K^*$. Ist ξ eine primitive m-te Einheitswurzel in K, so gilt

$$[K : \mathbb{Q}] \geq [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

wobei φ die Eulersche Phi-Funktion bezeichnet. Dies impliziert die Behauptung. □

Wir einnern nun an die Notation aus Kapitel 4: Sei K ein algebraischer Zahlkörper mit $\overline{K} \subseteq \mathbb{C}$ und $[K : \mathbb{Q}] = n$. Seien weiter

$$\delta_1, \ldots, \delta_r \colon K \to \mathbb{R} \quad \text{und} \quad \sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} \colon K \to \mathbb{C}$$

die reellwertigen und komplexwertigen $\mathbb{Q}$-Homomorphismen $K \to \overline{K}$, wobei $r + 2s = n$. Wie zuvor definieren wir $K_{\mathbb{C}} := \mathbb{C}^n$ und die Abbildung

$$j \colon K \to K_{\mathbb{C}},\ a \mapsto (\delta_1(a), \ldots, \delta_r(a), \sigma_1(a), \overline{\sigma_1}(a), \ldots, \sigma_s(a), \overline{\sigma_s}(a)).$$

Wir setzen neu $K_{\mathbb{C}}^* := (\mathbb{C}^*)^n$. Dies ist eine multiplikative Gruppe und die Einschränkung von j auf K^* ist ein Gruppenhomomorphismus $j\colon K^* \to K_{\mathbb{C}}^*$. Weiter definieren wir die Gruppenhomomorphismen

$$N\colon K_{\mathbb{C}}^* \to \mathbb{C}^*,\ (x_1,\dots,x_n) \mapsto \prod_{i=1}^{n} x_i \quad \text{und} \quad l\colon \mathbb{C}^* \to (\mathbb{R},+),\ z \mapsto \log|z|.$$

Letzterer induziert dabei den Gruppenhomomorphismus

$$l\colon K_{\mathbb{C}}^* \to (\mathbb{R}^n,+),\ (x_1,\dots,x_n) \mapsto (l(x_1),\dots,l(x_n)).$$

Setzen wir schließlich noch $\mathrm{Tr}(x) = \sum_{i=1}^{n} x_i$ für $x \in \mathbb{R}^n$, so erhalten wir das folgende kommutative Diagramm:

$$\begin{array}{ccccc} K^* & \xrightarrow{\ j\ } & K_{\mathbb{C}}^* & \xrightarrow{\ l\ } & \mathbb{R}^n \\ {\scriptstyle \mathrm{N}_{K/\mathbb{Q}}}\downarrow & & {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow{\ l\ } & \mathbb{R} \end{array}$$

Das Diagramm kommutiert tatsächlich, da offensichtlich $N(j(a)) = \mathrm{N}_{K/\mathbb{Q}}(a)$ für alle $a \in K$ und $\mathrm{Tr}(l(x)) = l(N(x))$ für alle $x \in K_{\mathbb{C}}^*$ ist. Wie in Kapitel 4 definieren wir weiter die Abbildung

$$F\colon K_{\mathbb{C}} \to K_{\mathbb{C}},\ (x_1,\dots,x_n) \mapsto (\overline{x_1},\dots,\overline{x_r},\overline{x_{r+2}},\overline{x_{r+1}},\dots,\overline{x_n},\overline{x_{n-1}})$$

und setzen $K_{\mathbb{R}} = (K_{\mathbb{C}})^+ := \{x \in K_{\mathbb{C}}\colon F(x) = x\}$. Wegen $F(j(a)) = j(a)$ für alle $a \in K$ lässt sich j als Gruppenhomomorphismus $K^* \to K_{\mathbb{R}}^*$ betrachten. Analog zu $(K_{\mathbb{C}})^+$ setzen wir $(\mathbb{R}^n)^+ := \{x \in \mathbb{R}^n\colon F(x) = x\}$. Da auch $F(l(x)) = l(F(x))$ für alle $x \in K_{\mathbb{C}}^*$ ist, und damit $F(l(x)) = l(x)$ für alle $x \in K_{\mathbb{R}}^*$, erhalten wir das folgende kommutative Diagramm:

$$\begin{array}{ccccc} K^* & \xrightarrow{\ j\ } & K_{\mathbb{R}}^* & \xrightarrow{\ l\ } & (\mathbb{R}^n)^+ \\ {\scriptstyle \mathrm{N}_{K/\mathbb{Q}}}\downarrow & & {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{\ l\ } & \mathbb{R} \end{array}$$

Sei weiterhin

$$\begin{aligned} \mathcal{O}_K^* &:= \left\{x \in \mathcal{O}_K\colon |\mathrm{N}_{K/\mathbb{Q}}(x)| = 1\right\}, \\ S &:= \left\{y \in K_{\mathbb{R}}^*\colon |N(y)| = 1\right\}, \\ H &:= \left\{x \in (\mathbb{R}^n)^+\colon \mathrm{Tr}(x) = 0\right\}. \end{aligned}$$

Dies sind jeweils Untergruppen von K^*, $K_{\mathbb{R}}^*$ und $(\mathbb{R}^n)^+$ und wir erhalten

$$\mathcal{O}_K^* \xrightarrow{\ j\ } S \xrightarrow{\ l\ } H\cdot$$

Weiter lässt sich leicht einsehen, dass l die Menge S surjektiv auf H abbildet. Setze schließlich $\lambda := l \circ j\colon \mathcal{O}_K^* \to H$ und $\Gamma := \lambda(\mathcal{O}_K^*) \subseteq H$.

Satz 6.2. *Sei K ein algebraischer Zahlkörper. Dann ist die Sequenz*

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

exakt.

Beweis. Es ist zu zeigen, dass $\ker(\lambda) = \mu(K)$ ist. Sei $x \in \mu(K)$. Dann gilt $x^m = 1$ für ein $m \in \mathbb{N}$. Sei $\tau\colon K \to \mathbb{C}$ eine beliebige Einbettung. Dann ist $\tau(x)^m = \tau(x^m) = 1$, also

$$m \log|\tau(x)| = \log|\tau(x)^m| = 0$$

und damit

$$\lambda(x) = (\log|\tau_1(x)|, \ldots, \log|\tau_n(x)|) = 0,$$

wobei $\tau_1, \ldots, \tau_n\colon K \to \mathbb{C}$ die verschiedenen Einbettungen sind. Also ist $\mu(K) \subseteq \ker(\lambda)$.

Sei nun $x \in \ker(\lambda)$. Dann ist $\lambda(x) = l(j(x)) = 0$, das heißt $\log|\tau(x)| = 0$ für jede Einbettung $\tau\colon K \to \mathbb{C}$, und damit auch $|\tau(x)| = 1$ für jede solche Einbettung. Es folgt, dass $j(\ker(\lambda))$ in einem beschränkten Teil von $j(\mathcal{O}_K) \subseteq K_{\mathbb{R}}$ liegt. Nach Satz 4.1 ist $j(\mathcal{O}_K)$ ein Gitter in $K_{\mathbb{R}}$, und nach Satz 3.2 ist jedes Gitter diskret. Also ist $j(\ker(\lambda))$ als beschränkte Teilmenge einer diskreten Menge endlich. Damit ist aber auch der Kern von λ selbst endlich, da die Abbildung j injektiv ist. Dies impliziert seinerseits, dass $\ker(\lambda)$ nur Einheitswurzeln enthalten kann, da dies die einzigen Elemente endlicher (multiplikativer) Ordnung in K^* sind. □

Lemma 6.3. *Sei K ein algebraischer Zahlkörper. Dann gibt es zu gegebenem $a \in \mathbb{Z}$ bis auf Multiplikation mit Einheiten nur endlich viele $\alpha \in \mathcal{O}_K$ mit $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a$.*

Beweis. Sei $a \in \mathbb{Z}$, $a > 1$. Sei weiter $n = [K : \mathbb{Q}]$. Wegen

$$|\mathcal{O}_K/(a\mathcal{O}_K)| = |\mathcal{O}_K/(a)| = \mathfrak{N}((a)) = \left|\mathrm{N}_{K/\mathbb{Q}}(a)\right| = a^n$$

ist die Anzahl der Nebenklassen von $a\mathcal{O}_K$ in $\mathcal{O}_K$ endlich. Wir behaupten, dass es in jeder dieser Nebenklassen bis auf Multiplikation mit Einheiten höchstens ein α mit Norm $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = a$ gibt. Seien dazu α, β zwei Elemente, welche in der selben Nebenklasse liegen, das heißt $\beta = \alpha + a\gamma$ für ein $\gamma \in \mathcal{O}_K$, und $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = |\mathrm{N}_{K/\mathbb{Q}}(\beta)| = a$ erfüllen. Dann gilt

$$\frac{\beta}{\alpha} = 1 \pm \frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha)}{\alpha}\gamma.$$

Seien $\tau_1 = \mathrm{id}, \tau_2, \ldots, \tau_n$ die $\mathbb{Q}$-Homomorphismen $K \to \mathbb{C}$. Dann ist

$$\frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha)}{\alpha} = \prod_{i=2}^{n} \tau_i(\alpha) \in \mathcal{O}_K,$$

und damit auch $\beta/\alpha \in \mathcal{O}_K$. Setze $u := \beta/\alpha$. Dann ist $\beta = \alpha u$ und wegen

$$a = |\mathrm{N}_{K/\mathbb{Q}}(\beta)| = |\mathrm{N}_{K/\mathbb{Q}}(\alpha u)| = a \cdot |\mathrm{N}_{K/\mathbb{Q}}(u)|$$

ist $|\mathrm{N}_{K/\mathbb{Q}}(u)| = 1$, das heißt u ist eine Einheit in $\mathcal{O}_K$. □

Theorem 6.4. *Sei K ein algebraischer Zahlkörper. Dann ist $\Gamma := \lambda(\mathcal{O}_K^*)$ ein vollständiges Gitter in dem Vektorraum H.*

Wir bemerken an dieser Stelle kurz, dass

$$(\mathbb{R}^n)^+ = \{x \in \mathbb{R}^n \colon F(x) = x\} = \{x \in \mathbb{R}^n \colon x_{r+1} = x_{r+2}, x_{r+3} = x_{r+4}, \dots, x_{n-1} = x_n\},$$

wobei $[K : \mathbb{Q}] = n = r + 2s$ wie zuvor, und damit

$$H = \{x \in (\mathbb{R}^n)^+ \colon \operatorname{Tr}(x) = 0\} \cong \mathbb{R}^{r+s-1}.$$

Beweis. Wir zeigen zuerst, dass Γ ein Gitter in H ist. Da $\lambda \colon \mathcal{O}_K^* \to H$ ein Gruppenhomomorphismus ist, ist Γ offensichtlich eine Untergruppe von H. Nach Theorem 3.2 reicht es damit zu zeigen, dass Γ diskret in H ist. Zunächst erinnern wir daran, dass die Abbildung λ durch Einschränkung von

$$K^* \xrightarrow{\ j\ } K_{\mathbb{C}}^* \xrightarrow{\ l\ } \mathbb{R}^n$$

entsteht. Setze $B_c := \{x \in \mathbb{R}^n \colon |x_i| < c \text{ für alle } i\}$ für $c > 0$. Dann reicht es zu zeigen, dass für jedes solche $c > 0$ der Schnitt $\Gamma \cap B_c$ endlich ist. Das Urbild von B_c unter l ist gegeben durch

$$l^{-1}(B_c) = \left\{z \in K_{\mathbb{C}}^* \colon e^{-c} < |z_i| < e^c \text{ für alle } i\right\}.$$

Nach Satz 4.1 ist $j(\mathcal{O}_K)$ ein Gitter in $K_{\mathbb{R}}$ und damit auch diskret in $K_{\mathbb{R}}$. Insbesondere liegt $j(\mathcal{O}_K)$ also diskret in $K_{\mathbb{C}}$ und enthält daher nur endlich viele Elemente der beschränkten Menge $l^{-1}(B_c)$. Schließlich lässt sich leicht nachprüfen, dass

$$\Gamma \cap B_c \subseteq l(l^{-1}(B_c) \cap j(\mathcal{O}_K^*))$$

ist, und somit auch $\Gamma \cap B_c$ für alle $c > 0$ endlich ist. Es folgt, dass Γ ein Gitter ist.

Damit bleibt zu zeigen, dass Γ als Gitter vollständig ist. Nach Satz 3.3 ist dies genau dann der Fall, wenn es eine beschränkte Teilmenge M von H mit $H = \bigcup_{\gamma \in \Gamma}(\gamma + M)$ gibt. Wir werden diese Menge durch ihr Urbild unter dem surjektiven Gruppenhomomorphismus $l \colon S \to H$ konstruieren. Genauer werden wir eine beschränkte Menge T in S mit

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} j(\varepsilon)T$$

konstruieren. Für diese gilt dann

$$H = l(S) = \bigcup_{\varepsilon \in \mathcal{O}_K^*} l(j(\varepsilon)T) = \bigcup_{\varepsilon \in \mathcal{O}_K^*} (\lambda(\varepsilon) + l(T)) = \bigcup_{\gamma \in \Gamma}(\gamma + l(T)).$$

Außerdem sind die einzelnen Komponenten x_i eines Elementes $x \in T$ wegen der Beschränktheit von T von oben beschränkt und wegen $\prod_{i=1}^n |x_i| = |N(x)| = 1$ auch von unten. Damit ist auch das Bild $l(T)$ beschränkt und wir wären fertig.

Es bleibt eine solche beschränkte Menge T zu konstruieren: Zunächst wählen wir reelle Zahlen $c_1, \dots, c_n > 0$ mit $c_{r+1} = c_{r+2}, c_{r+3} = c_{r+4}, \dots, c_{n-1} = c_n$ und

$$C := \prod_{i=1}^{n} c_i > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Weiter definieren wir die Menge $X := \{x \in K_{\mathbb{R}}^* \colon |x_i| < c_i \text{ für alle } i\}$. Für $y \in S$ gilt dann

$$yX = \{x \in K_{\mathbb{R}}^* \colon |x_i| < c_i' \text{ für alle } i\}$$

mit $c_i' := c_i|y_i|$. Natürlich ist $c_{r+1}' = c_{r+2}', \dots, c_{n-1}' = c_n'$ und wegen $|N(y)| = 1$ auch

$$\prod_{i=1}^{n} c_i' = \prod_{i=1}^{n} c_i \prod_{i=1}^{n} |y_i| = C.$$

Nach Theorem 4.2 gibt es zu $c_1', \dots, c_n'$ ein Element $a \in \mathcal{O}_K$, $a \neq 0$, mit $j(a) \in yX$. Ferner gibt es nach Lemma 6.3 Elemente $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$, sodass jedes $\alpha \in \mathcal{O}_K$ mit Norm $0 < |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq C$ zu einem dieser Elemente α_i assoziiert ist. Insbesondere ist also $a^{(y)}$ zu einem α_i assoziiert, denn $j(a) \in yX$ impliziert

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| = |N(j(a))| = \prod_{i=1}^{n} |(j(a))_i| \leq \prod_{i=1}^{n} c_i' = C.$$

Wir behaupten nun, dass die Menge

$$T := S \cap \bigcup_{i=1}^{N} j(\alpha_i)^{-1} X$$

die gewünschten Eigenschaften erfüllt. Zunächst ist klar, dass T beschränkt ist, da die Menge X nach Konstruktion beschränkt ist, und somit auch die einzelnen $j(\alpha_i)^{-1}X$. Es bleibt also zu zeigen, dass $S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} j(\varepsilon)T$ gilt. Wegen $j(\varepsilon) \in S$ für alle $\varepsilon \in \mathcal{O}_K^*$ und $T \subseteq S$ ist die Vereinigung der $j(\varepsilon)T$ offensichtlich in S enthalten. Wir zeigen die umgekehrte Inklusion:

Sei $y \in S$. Dann ist $y^{-1} \in S$ und wir finden ein $a \in \mathcal{O}_K$, $a \neq 0$ mit $j(a) = y^{-1}X$, das heißt $j(a) = y^{-1}x$ für ein $x \in X$. Wie weiter oben bemerkt, ist a assoziiert zu einem der α_i, das heißt es gilt $\alpha_i = \varepsilon a$ für ein $\varepsilon \in \mathcal{O}_K^*$. Betrachte nun $y = j(a)^{-1}x = j(\varepsilon)j(\alpha_i)^{-1}x$. Da y und $j(\varepsilon)$ in S liegen, gilt

$$j(\alpha_i)^{-1}x \in S \cap j(\alpha_i)^{-1}X \subseteq T,$$

und damit $y \in j(\varepsilon)T$. Dies endet den Beweis. □

Theorem 6.5. *Sei K ein algebraischer Zahlkörper. Dann ist die Einheitengruppe $\mathcal{O}_K^*$ von $\mathcal{O}_K$ das direkte Produkt der endlichen zyklischen Gruppe $\mu(K)$ und einer freien*

abelschen Gruppe vom Rang $t := r + s - 1$*. Das heißt, es gibt Einheiten* $\varepsilon_1, \ldots, \varepsilon_t$*, sodass jede Einheit* $\varepsilon \in \mathcal{O}_K^*$ *eine eindeutige Darstellung der Form*

$$\varepsilon = \xi\, \varepsilon_1^{\nu_1} \ldots \varepsilon_t^{\nu_t}$$

mit $\xi \in \mu(K)$ *und* $\nu_i \in \mathbb{Z}$ *besitzt. Die* ε_i *werden dabei als fundamentale Einheiten bezeichnet.*

Beweis. Nach Satz 6.2 ist die Sequenz

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

exakt und nach Theorem 6.4 ist Γ ein vollständiges Gitter in $H \cong \mathbb{R}^t$, also eine freie abelsche Gruppe vom Rang t. Sei $\{v_1, \ldots, v_t\}$ eine $\mathbb{Z}$-Basis von Γ und seien $\varepsilon_1, \ldots, \varepsilon_t$ Urbilder der v_i unter λ. Sei weiter A die von $\varepsilon_1, \ldots, \varepsilon_t$ erzeugte Untergruppe von $\mathcal{O}_K^*$. Dann ist

$$A \cap \mu(K) = \{1\},$$

da obige Sequenz exakt ist, also da $\mu(K)$ gerade der Kern der Abbildung λ ist.

Sei $x \in \mathcal{O}_K^*$ beliebig. Dann ist $\lambda(x) = \lambda(a)$ für ein $a \in A$, und damit $0 = \lambda(xa^{-1})$ da λ ein Gruppenhomomorphismus ist. Also gilt $xa^{-1} \in \ker(\lambda) = \mu(K)$, das heißt es gibt eine Einheitswurzel $\xi \in \mu(K)$ mit $x = \xi a$. Somit ist $\mathcal{O}_K^*$ tatsächlich das direkte Produkt aus $\mu(K)$ und A. □

7 Erweiterungen von Dedekindringen

Sei K ein algebraischer Zahlkörper und P ein nicht-triviales Primideal in $\mathcal{O}_K$. Dann ist $P \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{N}$. Insbesondere gilt $p \in P$, also $(p) = \mathcal{O}_K p \subseteq P$. Wir werden nun untersuchen, wie das ganzzahlige Ideal (p) in $\mathcal{J}_K$ in Primfaktoren zerfällt. Da die entsprechende Theorie auch in einem allgemeineren Rahmen funktioniert, betrachten wir im Folgenden Erweiterungen beliebiger Dedekindringe.

Theorem 7.1. *Sei A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung. Ferner sei B der ganze Abschluss von A in L. Dann ist B ein Dedekindring.*

Im Beweis werden wir das folgende aus der Algebra bekannte Resultat verwenden:

Theorem 7.2. *Sei R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann ist M noethersch.*

Beweis von Theorem 7.1. Wir zeigen zuerst, dass B ganz abgeschlossen ist. Sei dazu L' der Quotientenkörper von B. Da dieser der kleinste Körper ist, in welchen B eingebettet werden kann, gilt $L' \subseteq L$. Andererseits ist nach Satz 1.7 jedes Element in L von der Form b/a mit $b \in B$ und $a \in A$. Also gilt $L = L'$, und damit ist B ganz abgeschlossen.

Als nächstes zeigen wir, dass B noethersch ist. Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L. Mit Hilfe von Satz 1.7 können wir annehmen, dass die α_i in B liegen. Sei weiter $d := d(\alpha_1, \ldots, \alpha_n)$ die Diskriminante der Basis $\{\alpha_1, \ldots, \alpha_n\}$. Dann ist $d \neq 0$ (vergleiche Seite 12) und nach Satz 1.16 gilt

$$B \subseteq A\alpha_1/d + \ldots + A\alpha_n/d =: C.$$

Nach Theorem 7.2 ist der A-Modul C noethersch, da A als Dedekindring noethersch ist. Sei nun I ein Ideal in B. Dann ist I als A-Untermodul des noetherschen Moduls C endlich erzeugt über A und damit auch endlich erzeugt als B-Modul. Das heißt, jedes Ideal in B ist endlich erzeugt als B-Modul. Somit ist B noethersch.

Es bleibt zu zeigen, dass jedes nicht-triviale Primideal in B maximal ist. Sei P ein solches nicht-triviales Primideal in B und setze $p := P \cap A$. Dann ist p ein nicht-triviales Primideal in A, und da A ein Dedekindring ist, ist p maximal in A. Sei Q ein Ideal in B mit $P \subsetneq Q$. Wir behaupten, dass dann auch

$$p = P \cap A \subsetneq Q \cap A$$

gilt. Um dies zu zeigen sei $y \in Q \setminus P$. Da B ganz über A ist, ist

$$y^m + a_1 y^{m-1} + \ldots + a_{m-1} y + a_m = 0$$

für geeignete $a_i \in A$. Insbesondere gilt $a_m \in Q \cap A$. Ist $a_m \notin P$, so haben wir ein Element gefunden, welches in $Q \cap A$, aber nicht in $P \cap A$ liegt. Ist andererseits $a_m \in P$, so gibt es ein $k \in \mathbb{N}$ mit $a_k \notin P$ und $a_{k+1}, \ldots, a_m \in P$, da y selbst nicht in P ist. Es gilt dann

$$y^{m-k}\left(y^k + a_1 y^{k-1} + \ldots + a_k\right) = -a_{k+1}y^{m-(k+1)} - \ldots - a_{m-1}y - a_m \in P.$$

Da y nicht in P liegt und P ein Primideal ist, folgt $y^k + a_1 y^{k-1} + \ldots + a_k \in P \subseteq Q$. Somit ist $a_k \in Q$ und damit $a_k \in (Q \cap A) \setminus (P \cap A)$. Also gilt $p \subsetneq Q \cap A$ wie behauptet. Da p maximal in A ist, folgt schließlich $Q \cap A = A$, also $1 \in Q$ und daher $Q = B$. Damit ist gezeigt, dass P maximal ist. □

Satz 7.3. *Sei A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung. Ferner sei B der ganze Abschluss von A in L und p ein nicht-triviales Primideal in A. Dann gilt $Bp \neq B$.*

Beweis. Sei $p^{-1} = \{x \in K \colon xp \subseteq A\}$ wie in Satz 2.6. Dann ist $pp^{-1} = A$ und offensichtlich $A \subsetneq p^{-1}$. Sei $x \in p^{-1} \setminus A$ und nehme an, dass $Bp = B$ ist. Dann gilt

$$x \in Bx = Bpx \subseteq Bpp^{-1} = BA = B.$$

Somit ist $x \in B \cap K = A$. Dies widerspricht aber der Wahl von x. Also gilt $Bp \neq B$. □

Satz 7.4. *Sei A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung. Ferner sei B der ganze Abschluss von A in L, p ein nicht-triviales Primideal in A und*

$$Bp = P_1^{e_1} \ldots P_r^{e_r}$$

die Zerlegung des Ideals Bp in Primideale in B. Dann sind die P_i gerade die nicht-trivialen Primideale P in B mit $P \cap A = p$.

Wir bemerken, dass eine solche Zerlegung nach Theorem 2.7 existiert, wobei B unser Dedekindring ist und Bp ein nicht-triviales Ideal in B.

Beweis. Für alle i ist $p \subseteq Bp \subseteq P_i$ und damit $p \subseteq P_i \cap A$. Der Schnitt $P_i \cap A$ ist ein Ideal in A mit $P_i \cap A \subsetneq A$, weil $1 \notin P_i$ ist. Da p als Primideal in dem Dedekindring A maximal ist, folgt $p = P_i \cap A$.

Ist umgekehrt P ein nicht-triviales Primideal in B mit $P \cap A = p$, so gilt

$$Bp = B(P \cap A) \subseteq BP = P.$$

Also teilt P das Ideal Bp und ist somit Teil der Darstellung von Bp als Produkt von Primidealen. □

Einen Exponenten e_i aus dem vorangegangenen Satz nennen wir **Verzweigungsindex** von P_i über p. Wegen $A \cap P_i = p$ ist

$$A/p = A/(A \cap P_i) \cong (A + P_i)/P_i.$$

Ist $\{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L, welche in B enthalten ist, und $d := d(\alpha_1, \ldots, \alpha_2)$ die entsprechende Diskriminante, so gilt $B \subseteq A\alpha_1/d + \ldots + A\alpha_n/d =: C$, und da der A-Modul C nach Theorem 7.2 noethersch ist, ist der Untermodul B endlich erzeugt über A. Damit ist auch B/P_i endlich erzeugt über $(A+P_i)/P_i$, denn ist $B = A\alpha_1 + \ldots + A\alpha_n$, so wird B/P_i durch $\alpha_1 + P_i, \ldots, \alpha_n + P_i$ erzeugt.

Wegen $A/p \cong (A + P_i)/P_i$ können wir B/P_i somit als endlich erzeugte Körpererweiterung von A/p betrachten. Wir bezeichnen den Index

$$f_i = [B/P_i : A/p]$$

als **Trägheitsgrad** von P_i über p.

Theorem 7.5. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche separable Erweiterung und B der ganze Abschluss von A in L. Ferner sei p ein nichttriviales Primideal in A, $Bp = P_1^{e_1} \ldots P_r^{e_r}$ die Zerlegung des Ideals Bp in Primideale in B und seien $f_1, \ldots, f_r$ die Trägheitsgrade von den P_i über p. Dann gilt*

$$\sum_{i=1}^{r} e_i f_i = [L : K].$$

Wir unterteilen den Beweis in mehrere Lemmata:

Lemma 7.6. *Für alle $\nu \in \mathbb{N}_0$ gilt*

$$\dim_{A/p}(P_i^\nu / P_i^{\nu+1}) = f_i,$$

wobei $P_i^0 = B$ ist.

Beweis. Wegen $(a + P_i)(x + P_i^{\nu+1}) = ax + P_i^{\nu+1}$ für $a \in A$, $x \in P_i^\nu$ ist $P_i^\nu/P_i^{\nu+1}$ ein Modul über $(A+P_i)/P_i$. Weiterhin ist $(A+P_i)/P_i \cong A/p$ ein Körper, da p als Primideal maximal in A ist. Also ist $P_i^\nu/P_i^{\nu+1}$ sogar ein Vektorraum über A/p.

Sei $x \in P_i^\nu \setminus P_i^{\nu+1}$. Dann ist $Bx \subseteq P_i^\nu$ und $Bx \not\subseteq P_i^{\nu+1}$, das heißt P_i^ν teilt Bx, aber nicht $P_i^{\nu+1}$. Nach Satz 2.15 gilt für ein beliebiges Primideal P in B

$$\nu_P(Bx + P_i^{\nu+1}) = \min\left(\nu_P(Bx), \nu_P(P_i^{\nu+1})\right).$$

Offensichtlich ist $\nu_{P_i}(P_i^{\nu+1}) = \nu + 1$ und $\nu_P(P_i^{\nu+1}) = 0$ für $P \neq P_i$. Nach den vorhergehenden Bemerkungen ist außerdem $\nu_{P_i}(Bx) = \nu$, und damit $Bx + P_i^{\nu+1} = P_i^\nu$. Der Ringhomomorphismus

$$\varphi\colon B \to P_i^\nu/P_i^{\nu+1},\ b \mapsto bx + P_i^{\nu+1}$$

ist also surjektiv. Weiterhin ist P_i im Kern von φ enthalten, und da P_i als Primideal maximal in B ist und φ nicht trivial ist, folgt $\ker(\varphi) = P_i$. Die Abbildung

$$B/P_i \to P_i^\nu/P_i^{\nu+1},\ b + P_i \mapsto bx + P_i^{\nu+1}$$

ist also ein Ringisomorphismus. Da dieser auch $(A + P_i)/P_i$-linear ist, folgt

$$\dim_{A/p}(P_i^\nu/P_i^{\nu+1}) = \dim_{A/p}(B/P_i) = [B/P_i : A/p] = f_i. \qquad \square$$

Lemma 7.7. *Es gilt*

$$\dim_{A/p}(B/(Bp)) = \sum_{i=1}^{r} e_i f_i.$$

Beweis. Da A/p ein Körper ist, ist $B/(Bp)$ ein Vektorraum über A/p mit der Multiplikation $(a+p)(b+Bp) = ab+Bp$ für $a \in A$, $b \in B$. Die Inklusionen

$$P_i^{e_i} \subseteq P_i^{e_i-1} \subseteq \ldots \subseteq P_i \subseteq P_i^0 = B$$

liefern die Kette

$$P_i^{e_i-1}/P_i^{e_i} \subseteq \ldots \subseteq P_i/P_i^{e_i} \subseteq B/P_i^{e_i}.$$

Weiter ist auch $B/P_i^{e_i}$ ein Vektorraum über A/p, weil $Bp \subseteq P_i^{e_i}$ ist. Es folgt

$$\begin{aligned}\dim_{A/p}(B/P_i^{e_i}) &= \dim_{A/p}\left(\frac{B/P_i^{e_i}}{P_i/P_i^{e_i}}\right) + \dim_{A/p}\left(\frac{P_i/P_i^{e_i}}{P_i^2/P_i^{e_i}}\right) + \ldots + \dim_{A/p}\left(\frac{P_i^{e_i-1}/P_i^{e_i}}{P_i^{e^i}/P_i^{e_i}}\right) \\ &= \dim_{A/p}(B/P_i) + \dim_{A/p}(P_i/P_i^2) + \ldots + \dim_{A/p}(P_i^{e_i-1}/P_i^{e_i}).\end{aligned}$$

Nach dem vorangegangenen Lemma gilt damit $\dim_{A/p}(B/P_i^{e_i}) = e_i f_i$, da jeder Summand gleich f_i ist. Für $i \neq j$ ist $P_i^{e_i} + P_j^{e_j} = B$, da $\nu_P(P_i^{e_i} + P_j^{e_j}) = 0$ für alle nicht-trivialen Primideale P in B gilt. Wir benutzen nun den chinesischen Restsatz. Dieser besagt, dass die Abbildung

$$B/(Bp) = B/\left(\prod\nolimits_{i=1}^{r} P_i^{e_i}\right) \to \bigoplus_{i=1}^{r} B/(P_i^{e_i}), \quad b+Bp \mapsto \left(b+P_i^{e_i}\right)_{i=1,\ldots,r}$$

ein Isomorphismus ist. Da die Abbildung auch A/p-linear ist, ergibt sich

$$\dim_{A/p}(B/(Bp)) = \dim_{A/p}\left(\bigoplus\nolimits_{i=1}^{r} B/(P_i^{e_i})\right) = \sum_{i=1}^{r} \dim_{A/p}\left(B/(P_i^{e_i})\right) = \sum_{i=1}^{r} e_i f_i. \quad \square$$

Lemma 7.8. *Sei $\{v_1+Bp, \ldots, v_m+Bp\}$ eine Basis von $B/(Bp)$ über A/p. Dann ist $\{v_1, \ldots, v_m\}$ bereits eine Basis von L über K.*

Beweis. Wir zeigen zunächst, dass die Elemente $v_1, \ldots, v_m$ linear unabhängig über K sind. Sei $a_1v_1 + \ldots + a_mv_m = 0$ mit $a_i \in K$ eine nicht-triviale Darstellung der 0. Da K der Quotientenkörper von A ist, können wir ohne Beschränkung der Allgemeinheit annehmen, dass die a_i in A liegen. Sei $a := (a_1, \ldots, a_m)$ das von den a_i erzeugte Ideal in A. Weiter sei $y \in a^{-1} = \{x \in K \colon xa \subseteq A\}$. Dann ist $ya_i \in A$ für alle i und es folgt

$$\sum_{i=1}^{m}(ya_i+p)(v_i+Bp) = \sum_{i=1}^{m}((ya_i)v_i+Bp) = y\sum_{i=1}^{m} a_iv_i + Bp = Bp.$$

Da $ya_i+p \in A/p$ ist, und die v_i+Bp linear unabhängig über A/p sind, folgt $ya_i+p = 0$ in A/p, das heißt $ya_i \in p$. Da dies für alle $y \in a^{-1}$ und für alle i gilt, ist $A = aa^{-1} \subseteq p$.

Dies ist aber ein Widerspruch, da p ein nicht-triviales Primideal in A ist. Also sind die v_i linear unabhängig über K.

Es bleibt zu zeigen, dass die v_i den K-Vektorraum L erzeugen. Sei $V := \sum_{i=1}^{m} Av_i$ und $W := B/V$, wobei wir V als A-Modul betrachten und W als Quotient von A-Moduln. Sei weiter $b \in B$. Dann ist

$$b + Bp = \sum_{i=1}^{m} (a_i + p)(v_i + Bp) = \sum_{i=1}^{m} a_i v_i + Bp \in V + Bp$$

für geeignete $a_i \in A$. Das heißt es gibt $b_1, b_2 \in Bp$ und $v \in V$, sodass

$$b = v + (b_1 - b_2) \in V + Bp.$$

Andererseits gilt offensichtlich $V + Bp \subseteq B$ und damit ist $B = V + Bp$. Wir möchten dies benutzen, um zu zeigen, dass $pW = W$ ist:

Sei $x \in pW$. Dann gibt es $N \in \mathbb{N}$, $a_i \in p$ und $w_i \in W$, sodass $x = \sum_{i=1}^{N} a_i w_i$ ist. Wegen $W = B/V$ gibt es weiter $b_i \in B$, sodass gilt

$$x = \sum_{i=1}^{N} a_i (b_i + V) = \sum_{i=1}^{N} a_i b_i + V.$$

Elemente der Form $\sum_{i=1}^{N} a_i b_i$ sind aber gerade die Elemente in Bp, und da $B = V + Bp$ ist, entsprechen die durch Bp definierten Nebenklassen von V den durch B definierten Nebenklassen von V. Also ist $pW = W$ wie behauptet.

Ist $\{\alpha_1, \ldots, \alpha_n\}$ eine K-Basis von L, welche in B enthalten ist, und $d := d(\alpha_1, \ldots, \alpha_2)$ die entsprechende Diskriminante, so gilt $B \subseteq A\alpha_1/d + \ldots + A\alpha_n/d =: C$, und da der A-Modul C nach Theorem 7.2 noethersch ist, ist der Untermodul B endlich erzeugt über A. Dies übertraägt sich auf $W = B/V$, das heißt W ist endlich erzeugt über A. Sei $W = \sum_{i=1}^{s} Az_i$ mit $z_i \in W$. Aus

$$W = pW = p \sum_{i=1}^{s} Az_i = \sum_{i=1}^{s} pz_i$$

folgt $z_i = \sum_{j=1}^{s} a_{ij} z_j$ für geeignete $a_{ij} \in p$. Dann ist

$$\sum_{j=1}^{s} (a_{ij} - \delta_{ij}) z_j = 0$$

für alle i und damit $Mz = 0$, wobei $M := (a_{ij} - \delta_{ij})_{ij}$ und $z := (z_1, \ldots, z_s)$. Weiter ist

$$\det(M) = \det((a_{ij} - \delta_{ij})_{ij}) = (-1)^s \mod p,$$

also $d \neq 0$. Sei N die zu M komplementäre Matrix. Dann gilt $\det(M)z = NMz = 0$, also $\det(M)z_i = 0$ für alle i und damit

$$(\det(M)B)/V = \det(M)W = \{0\}.$$

Das heißt, es ist $\det(M)B \subseteq V$. Da $\det(M) \neq 0$ in K invertierbar ist, gilt somit

$$B \subseteq \det(M)^{-1}V = \sum_{i=1}^{m} A \det(M)^{-1} v_i \subseteq \sum_{i=1}^{m} K v_i.$$

Wir wissen aber, dass L eine in B enthaltene K-Basis besitzt, also $L = KB$ gilt. Daher folgt $L \subseteq \sum_{i=1}^{m} K v_i$, und somit erzeugen die Elemente $v_1, \ldots, v_m$ den Vektorraum L über K. □

Beweis von Theorem 7.5. Nach Lemma 7.7 gilt $\dim_{A/p}(B/(Bp)) = \sum_{i=1}^{r} e_i f_i$ und nach Lemma 7.8 gilt $\dim_{A/p}(B/(Bp)) = \dim_K(L)$. Damit folgt die Behauptung des Theorems. □

Wir nennen zwei Ideale a, b in einem Ring R **teilerfremd**, wenn $a + b = R$ gilt. Dies ist äquivalent dazu, dass es $x \in a$ und $y \in b$ mit $x + y = 1$ gibt. Sind a, b teilerfremd, so lässt sich zeigen, dass $ab = a \cap b$ gilt.

Bemerkung. Sei A ein Dedekindring und seien p_1, p_2 Primideale in A, $p_1 \neq p_2$. Dann sind p_1 und p_2 teilerfremd, da $p_1 \subsetneq p_1 + p_2$ ist, und p_1 maximal in A ist. Es lässt sich weiter zeigen, dass zwei Ideale a, b in A genau dann teilerfremd sind, wenn es kein nicht-triviales Primideal p in A gibt, welches sowohl a als auch b teilt. Insbesondere sind damit ein nicht-triviales Primideal p und ein beliebiges Ideal a genau dann teilerfremd, wenn p das Ideal a nicht teilt.

Sei A wieder ein Dedekindring mit Quotientenkörper K, L/K eine endliche separable Erweiterung und B der ganze Abschluss von A in L. Nach dem Satz vom primitiven Element ist $L = K(\theta)$ für ein $\theta \in L$, und nach Satz 1.7 können wir annehmen, dass $\theta \in B$ ist. Sei f das Minimalpolynom von θ über K. Nach Satz 1.8 liegt f in $A[x]$. Setze

$$F := \{x \in B \colon xB \subseteq A[\theta]\},$$

das heißt F ist das größte Ideal in B, welches in $A[\theta]$ enthalten ist. Wir behaupten, dass $F \neq \{0\}$ ist: Sei $n = [L : K]$. Dann ist $\{1, \theta, \ldots, \theta^{n-1}\}$ eine in B enthaltene Basis von L über K und es gilt

$$d(1, \theta, \ldots, \theta^{n-1})B \subseteq A + A\theta + \ldots + A\theta^{n-1} = A[\theta]$$

nach Satz 1.16. Damit ist $d(1, \theta, \ldots, \theta^{n-1}) \in F$ und wegen $d(1, \theta, \ldots, \theta^{n-1}) \neq 0$ (vergleiche Seite 12) auch $F \neq \{0\}$. Genauer gilt sogar $F \cap A \neq \{0\}$, da die Diskriminante $d(1, \theta, \ldots, \theta^{n-1})$ nach Satz 1.16 in A liegt. Wir bemerken außerdem, dass $F = B$ durchaus möglich ist.

Theorem 7.9. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche separable Erweiterung mit $L = K(\theta)$, $\theta \in B$, und $f \in A[x]$ das Minimalpolynom von θ über K. Sei weiter B der ganze Abschluss von A in L, p ein nicht-triviales Primideal in A, welches teilerfremd zu $F \cap A$ ist, und*

$$\overline{f} = \overline{p_1}^{e_1} \ldots \overline{p_r}^{e_r}$$

die Zerlegung von $\overline{f} \in (A/p)[x]$ *in irreduzible normierte Komponenten* $\overline{p_i}$*. Dann sind die*

$$P_i := Bp + Bp_i(\theta)$$

die verschiedenen Primideale in B *über* p *mit Trägheitsgraden* $f_i = \operatorname{grad}(\overline{p_i})$ *und es gilt*

$$Bp = P_1^{e_1} \dots P_r^{e_r}.$$

Wir zeigen zunächst, das folgende Lemma:

Lemma 7.10. *In der Situation des Theorems ist* p *genau dann teilerfremd zu* $F \cap A$*, wenn* Bp *teilerfremd zu* F *ist.*

Beweis. Ist p teilerfremd zu $F \cap A$, so gilt $p + (F \cap A) = A$ und damit

$$B = Bp + B(F \cap A) \subseteq Bp + BF = Bp + F \subseteq B,$$

also $Bp + F = B$. Es bleibt die Rückrichtung zu zeigen. Sei dazu $Bp + F = B$. Ist $F = B$, so folgt wegen $p + (F \cap A) = p + A = A$ die Behauptung. Sei also $F \subsetneq B$. Weiterhin sei $F = Q_1^{j_1} \dots Q_s^{j_s}$ die Zerlegung von F in Primideale Q_i in B. Dann ist $q_i := Q_i \cap A$ ein Primideal in A und es gilt

$$F \cap A = \left(Q_1^{j_1} \dots Q_s^{j_s}\right) \cap A \supseteq (Q_1 \cap A)^{j_1} \dots (Q_s \cap A)^{j_s},$$

das heißt $F \cap A$ teilt $q_1^{j_1} \dots q_s^{j_s}$. Angenommen p teilt $F \cap A$, dann folgt $p = q_i$ für ein i und damit

$$Bp = Bq_i = B(Q_i \cap A) \subseteq BQ_i = Q_i.$$

Also teilt Q_i das Ideal Bp, was der Teilerfremdheit von Bp und F widerspricht. Es folgt, dass p nicht $F \cap A$ teilt. Da p prim ist ist, sind p und $F \cap A$ damit teilerfremd. □

Beweis von Theorem 7.9. Setze $B' := A[\theta]$ und $\overline{A} := A/p$. Wir werden im Folgenden zeigen, dass die Abbildung

$$B' \to B/(Bp),\ b \mapsto b + Bp$$

ein surjektiver Homomorphismus mit Kern $B' \cap (Bp) = B'p$ ist. Wir beginnen mit der Surjektivität: Nach Annahme sind p und $F \cap A$ teilerfremd, und nach dem vorangegangenen Lemma sind dadurch auch Bp und F teilerfremd, das heißt es gilt $Bp + F = B$. Wegen $F \subseteq B'$ ist somit auch $Bp + B' = B$, was die Surjektivität zeitgt.

Betrachten wir nun den Kern der dargestellten Abbildung, welcher offensichtlich durch $B' \cap (Bp)$ gegeben ist: Die Inklusion $B'p \subseteq B' \cap (Bp)$ ist klar. Andererseits gilt

$$\begin{aligned} B' \cap (Bp) \subseteq A(B' \cap (Bp) &= (p + (F \cap A))(B' \cap (Bp)) \\ &= p(B' \cap (Bp)) + (F \cap A)(B' \cap (Bp)). \end{aligned}$$

Mit $(F \cap A)(B' \cap (Bp)) \subseteq FBp = Fp$ folgt dann $B' \cap (Bp) \subseteq B'p + Fp = B'p$. Somit ist die Abbildung

$$B'/(B'p) \to B/(Bp),\ b + B'p \mapsto b + Bp$$

ein Isomorphismus.

Weiterhin behaupten wir, dass die Abbildung

$$\overline{A}[x] \to B'/(B'p),\ \overline{g} \mapsto g(\theta) + B'p$$

ein wohldefinierter surjektiver Homomorphismus mit Kern $\overline{A}[x]\,\overline{f}$ ist. Wir zeigen zunächst die Wohldefiniertheit: Seien $g, h \in A[x]$ mit $\overline{g} = \overline{h}$ in $\overline{A}[x]$. Dann gilt $a_{g,i} = a_{h,i} + y_i$ mit $y_i \in p$ für die Koeffizienten $a_{g,i}$ bzw. $a_{h,i}$ von g bzw. h, das heißt $k := g - h$ ist ein Polynom mit Koeffizienten in p. Somit ist $k(\theta) = \sum_i y_i\theta^i \in B'p$ und daher

$$g(\theta) + B'p = h(\theta) + k(\theta) + B'p = h(\theta) + B'p.$$

Also ist die Abbildung wohldefiniert. Damit ist sie aber offensichtlich auch surjektiv, da die Menge $B' = A[\theta]$ gerade durch $\{g(\theta)\colon g \in A[x]\}$ gegeben ist.

Es verbleibt zu zeigen, dass der Kern der Abbildung das von $\overline{f}$ erzeugte Ideal in $\overline{A}[x]$ ist. Sei dazu $g \in A[x]$ mit $\overline{g} \in (\overline{f})$. Dann gibt es ein Polynom $h \in A[x]$ mit $\overline{g} = \overline{h}\,\overline{f}$. Damit ist $g - hf \in p[x]$, also

$$g(\theta) = (g - hf)(\theta) \in p[\theta] \subseteq B'p.$$

Daher liegt $\overline{g}$ im Kern der Abbildung. Sei umgekehrt $g \in A[x]$ mit $g(\theta) \in B'p$. Polynomdivision mit Rest ergibt $g = hf + r$ mit $h, r \in A[x]$ und $0 \leq \operatorname{grad}(r) < \operatorname{grad}(f)$, wobei $\operatorname{grad}(f)$ dem Grad der Erweiterung L/K entspricht. Es ist

$$r(\theta) = g(\theta) \in B'p = A[\theta]p.$$

Damit folgt sogar $r \in A[x]p$, weil $1, \theta, \ldots, \theta^{n-1}$ linear unabhängig über A sind. Also ist $\overline{r} = 0$ in $\overline{A}[x]$ und daher $\overline{g} = \overline{h}\,\overline{f} \in (\overline{f})$. Dies zeigt die Behauptung. Die Abbildung

$$\overline{A}[x]/(\overline{f}) \to B'/(B'p),\ \overline{g} + (\overline{f}) \mapsto g(\theta) + B'p$$

ist somit ein Isomorphismus.

Mit Hilfe des weiter oben angegebenen Isomorphismus $B'/(B'p) \to B/(Bp)$ erhalten wir, dass die Abbildung

$$\overline{A}[x]/(\overline{f}) \to B/(Bp),\ \overline{g} + (\overline{f}) \mapsto g(\theta) + Bp$$

ebenfalls einen Isomorphismus darstellt.

Wir werden nun die Primideale des Ringes $R := \overline{A}[x]/(\overline{f})$ bestimmen. Die Projektion

$$\pi\colon \overline{A}[x] \to R$$

liefert eine Bijektion zwischen den $(\overline{f})$ enthaltenden Idealen in $\overline{A}[x]$ und den Idealen in R. Sie liefert sogar eine Bijektion zwischen den entsprechenden Primidealen. Weiterhin ist R ein Hauptidealring, da $\overline{A}[x]$ als Polynomring einer Variablen über dem Körper $\overline{A}$ ein Hauptidealring ist.

Sei nun I ein Primideal in R. Dann ist $\pi^{-1}(I)$ ein Primideal in $\overline{A}[x]$, welches $(\overline{f})$ enthält, und es gilt $\pi^{-1}(I) = (\overline{q})$ für ein $\overline{q} \in \overline{A}[x]$, da $\overline{A}[x]$ ein Hauptidealring ist. Weiterhin ist $\overline{q}$ prim, da $\pi^{-1}(I)$ prim ist, und wegen $(\overline{f}) \subseteq (\overline{q})$ teilt $(\overline{q})$ das Ideal $(\overline{f})$. Somit teilt $\overline{q}$ selbst auch das Polynom $\overline{f}$, das heißt $\overline{q}$ ist ein Primteiler von $\overline{f}$. Natürlich gilt auch

$$\pi((\overline{q})) = \pi(\pi^{-1}(I)) = I.$$

Ist andererseits $\overline{q}$ ein beliebiger Primteiler von $\overline{f}$, so ist $I := \pi((\overline{q}))$ ein Primideal in R. Es folgt, dass die Primideale in R gerade von der Form $\pi((\overline{q})) = (\pi(\overline{q}))$ sind, wobei $\overline{q}$ ein Primteiler von $\overline{f}$ ist. Nach Voraussetzung gilt $\overline{f} = \overline{p_1}^{e_1} \dots \overline{p_r}^{e_r}$. Die Menge der Primideale in R ist daher gegeben durch

$$\big\{\big(\pi(\overline{p_1})\big), \dots, \big(\pi(\overline{p_r})\big)\big\}. \tag{$\star^1$}$$

Wegen $(\overline{f}) \subseteq (\overline{p_i}) \subseteq \overline{A}[x]$ können wir $(\overline{f})$ auch als Ideal in dem Ring $(\overline{p_i})$ betrachten. Es gilt

$$\frac{R}{\pi((\overline{p_i}))} = \frac{\overline{A}[x]/(\overline{f})}{(\overline{p_i})/(\overline{f})} \cong \overline{A}[x]/(\overline{p_i}) = \overline{A} + \overline{A}x + \ldots + \overline{A}x^{n_i - 1}$$

mit $n_i := \operatorname{grad}(\overline{p_i})$. Somit können wir $R/(\pi(\overline{p_i}))$ als Körpererweiterung über $\overline{A}$ vom Grad n_i betrachten, das heißt

$$\Big[R/\big(\pi(\overline{p_i})\big) : \overline{A}\Big] = \operatorname{grad}(\overline{p_i}). \tag{$\star^2$}$$

Weiterhin gilt

$$(\pi(\overline{p_i}))^{e_i} + (\pi(\overline{p_j}))^{e_j} = \pi\Big((\overline{p_i})^{e_i} + (\overline{p_j})^{e_j}\Big) = \pi\Big(\overline{A}[x]\Big) = R$$

für $i \neq j$, das heißt die Elemente $(\pi(\overline{p_i}))^{e_i}$ und $(\pi(\overline{p_j}))^{e_j}$ sind teilerfremd in R. Damit gilt $(\pi(\overline{p_i}))^{e_i} \cap (\pi(\overline{p_j}))^{e_j} = (\pi(\overline{p_i}))^{e_i}(\pi(\overline{p_j}))^{e_j}$ und allgemeiner

$$\bigcap_{i=1}^{r} (\pi(\overline{p_i}))^{e_i} = \prod_{i=1}^{r} (\pi(\overline{p_i}))^{e_i} = \prod_{i=1}^{r} (\pi(\overline{p_i}^{e_i})) = \pi\left(\prod\nolimits_{i=1}^{r} \overline{p_i}^{e_i}\right) = \pi((\overline{f})) = \{0\}. \tag{$\star^3$}$$

Nun nutzen wir den weiter oben angegebenen Isomorphismus $\overline{g} + (\overline{f}) \mapsto g(\theta) + Bp$ um die Ergebnisse $(\star^1)$, $(\star^2)$ und $(\star^3)$ von R nach $\overline{B} := B/(Bp)$ zu übertragen. Mit Hilfe von $(\star^1)$ sehen wir zunächst, dass die Primideale in $\overline{B}$ gerade die Ideale erzeugt von Elementen der Form $p_i(\theta) + Bp$ sind. Setze $\overline{P_i} := (p_i(\theta) + Bp)$. Dann ist die Menge der Primideale in $\overline{B}$ gegeben durch $\{\overline{P_1}, \dots, \overline{P_r}\}$ und nach $(\star^2)$ und $(\star^3)$ gilt

$$\Big[\overline{B}\Big/\overline{P_i} : \overline{A}\Big] = \operatorname{grad}(\overline{p_i}) \tag{$\sharp^2$}$$

$$\bigcap_{i=1}^{r} \overline{P_i}^{e_i} = \{0\}. \tag{$\sharp^3$}$$

Sei nun P_i das Urbild von $\overline{P_i}$ unter der Projektion $\sigma\colon B \to \overline{B} = B/(Bp)$. Dann gilt wegen $0 + Bp \in \overline{P_i}$ insbesondere $Bp \subseteq P_i$, das heißt P_i teilt Bp. Wir behaupten, dass $P_1, \ldots, P_r$ bereits alle Primteiler des Ideals Bp in B sind. Znächst bemerken wir aber, dass wegen $B/P_i \cong (B/(Bp))/(P_i/(Bp))$ und ($\sharp^2$) der Trägheitsgrad von P_i über p gegeben ist durch

$$f_i = \left[B/P_i : A/p\right] = \left[\overline{B}\Big/\overline{P_i} : \overline{A}\right] = \operatorname{grad}(\overline{p_i}). \tag{$\dagger$}$$

Weiterhin folgt aus $\sigma(P_i^{e_1}) = \overline{P_i}^{e_i}$, dass $P_i^{e_1} \subseteq \sigma^{-1}(\overline{P_i}^{e_i})$ gilt, und zusammen mit ($\sharp^3$) ergibt sich

$$\bigcap_{i=1}^{r} P_i^{e_i} \subseteq \bigcap_{i=1}^{r} \sigma^{-1}\left(\overline{P_i}^{e_i}\right) = \sigma^{-1}\left(\bigcap_{i=1}^{r} \overline{P_i}^{e_i}\right) = \sigma^{-1}(\{0\}) = Bp.$$

Da die Ideale $P_i^{e_i}$ offensichtlich teilerfremd sind, gilt außerdem $\bigcap_{i=1}^{r} P_i^{e_i} = \prod_{i=1}^{r} P_i^{e_i}$. Also teilt Bp das Produkt $\prod_{i=1}^{r} P_i^{e_i}$, das heißt $P_1, \ldots, P_r$ sind tatsächlich bereits alle Primteiler von Bp, wie weiter oben behauptet. Genauer gilt $Bp = P_1^{d_1} \ldots P_r^{d_r}$ mit $1 \leq d_i \leq e_i$, wobei e_i der Verzweigungsindex von P_i über p ist. Wegen $\overline{f} = \overline{p_1}^{e_1} \ldots \overline{p_r}^{e_r}$ und ($\dagger$) ist ferner

$$[L : K] = \operatorname{grad}(f) = \operatorname{grad}(\overline{f}) = \sum_{i=1}^{r} e_i \operatorname{grad}(\overline{p_i}) = \sum_{i=1}^{r} e_i f_i.$$

Da $\sum_{i=1}^{r} d_i f_i = [L : K]$ nach Theorem 7.5 gilt, folgt $e_i = d_i$ für alle i und damit die Aussage des Theorems. □

Wir wiederholen kurz die Idee des Beweises: Wir haben gesehen, dass die Primteiler von Bp gerade die Urbilder der Primideale in $B/(Bp)$ unter der Projektion $B \to B/(Bp)$ sind. Den Ring $B/(Bp)$ konnten wir dabei mit Hilfe des Isomorphismus

$$\overline{A}[x]/(\overline{f}) \to B/(Bp),\ \overline{g} + (\overline{f}) \mapsto g(\theta) + Bp$$

untersuchen.

Sei wie zuvor p ein nicht-triviales Primideal in A und $Bp = P_1^{e_1} \ldots P_r^{e_r}$ die Zerlegung des ganzzahligen Ideals $(p) = Bp$ in L. Wir nennen p **vollständig zerlegt**, wenn r der Grad der Körpererweiterung L/K ist, das heißt wenn $r = n = [L : K]$ ist. In diesem Fall gilt $e_i = f_i = 1$ für alle $i = 1, \ldots, n$, da $\sum_{i=1}^{n} e_i f_i = n$ nach Theorem 7.5 ist und e_i und f_i positive ganze Zahlen sind. Weiterhin nennen wir p **unzerlegt**, wenn $r = 1$ gilt.

Ist $e_i = 1$ und B/P_i eine separable Erweiterung über A/p, so nennen wir P_i **unverzweigt**. Ansonsten wird P_i als **verzweigt** bezeichnet. Weiter nennen wir p selbst **unverzweigt**, falls alle P_i über p unverzweigt sind. Entsprechend heißt die Erweiterung L/K **unverzweigt**, wenn alle nicht-trivialen Primideale p in A unverzweigt sind.

Satz 7.11. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche separable Erweiterung und B der ganze Abschluss von A in L. Dann gibt es nur endlich viele ganzzahlige Primideale p in K, die in L verzweigen.*

Bevor wir zum Beweis dieses Satzes kommen, wiederholen wir ein Resultat aus der Algebra, welches uns von Nutzen sein wird.

Satz 7.12. *Sei R ein Ring und $f \in R[x]$ ein normiertes Polynom. Ist $f = \prod_{i=1}^{n}(x - a_i)$ die Faktorisierung von f über einem Erweiterungsring R' von R, so ist die Diskriminante von f gegeben durch*

$$D(f) = \prod_{i<j}(a_i - a_j)^2.$$

Ist R zusätzlich Integritätsbereich, so verschwindet die Diskriminante von f genau dann, wenn f eine mehrfache Nullstelle besitzt.

Beweis von Satz 7.11. Sei $L = K(\theta)$ mit $\theta \in B$ und sei $f \in A[x]$ das Minimalpolynom von θ über K. Seien weiter $\sigma_1, \ldots, \sigma_n \colon L \to \overline{K}$ die verschiedenen K-Homomorphismen von $L \to \overline{K}$. Setze $\theta_i := \sigma_i(\theta)$. Dann ist

$$f = \prod_{i=1}^{n}(x - \theta_i),$$

da $f(\theta_i) = 0$ ist für alle i wegen $\sigma_i \circ f = f \circ \sigma_i$. Nach obigem Satz aus der Algebra ist die Diskriminante von f daher $D(f) = \prod_{i<j}(\theta_i - \theta_j)^2$. Andererseits lässt sich zeigen, dass die Diskriminante der Basis $\{1, \theta, \ldots, \theta^{n-1}\}$ von L über K ebenfalls durch

$$d := d(1, \theta, \ldots, \theta^{n-1}) = \left[\det\left(\left(\theta_i^{j-1}\right)_{ij}\right)\right]^2 = \prod_{i<j}(\theta_i - \theta_j)^2 = D(f)$$

gegeben ist.

Sei nun p ein ganzzahliges Primideal in K, welches in A teilerfremd zu dem von d erzeugten Ideal ist. Dann ist

$$B = B(p + Ad) = Bp + Bd \subseteq Bp + F \subseteq B.$$

Also sind Bp und F teilerfremd als Ideale in B. Sei $\overline{f}$ das Bild von f unter der Projektion $A[x] \to (A/p)[x]$. Dann ist

$$D(\overline{f}) = D(f) = d \neq 0 \mod p.$$

Nach Satz 7.12 hat $\overline{f}$ somit nur einfache Nullstellen. Sei $Bp = P_1^{e_1} \ldots P_r^{e_r}$ die Zerlegung von Bp in Primideale P_i in B. Da $\overline{f}$ nur einfache Nullstellen besitzt, impliziert Theorem 7.9, dass $e_i = 1$ für alle i ist.

Wir zeigen weiter, dass B/P_i über $(A + P_i)/P_i \cong A/p =: \overline{A}$ von $\theta + P_i$ erzeugt wird: Sei π die Projektion von B auf $\overline{B} := B/(Bp)$. Wir setzen $\overline{\theta} := \pi(\theta)$ und $\overline{P_i} := \pi(P_i)$. Dann wird $\overline{B}$ als A-Modul von den Elementen $1, \overline{\theta}, \ldots, \overline{\theta}^{\,n-1}$ erzeugt, und somit $\overline{B}/\overline{P_i}$ über A/p von $\overline{\theta} + \overline{P_i}$. Wegen

$$B/P_i \cong \frac{B/(Bp)}{P_i/(Bp)} = \overline{B}/\overline{P_i}$$

wird B/P_i über $(A+P_i)/P_i$ also wie behauptet von $\theta + P_i$ erzeugt.

Es ist $\overline{f} \in \overline{A}[x]$ und $\overline{A} = A/p \cong (A+P_i)/P_i$, sodass

$$\overline{f}(\theta + P_i) = f(\theta) = 0 \mod P_i$$

gilt, weil $Bp \subseteq P_i$ ist. Also teilt das Minimalpolynom von $\theta + P_i$ über A/p das separable Polynom $\overline{f}$. Die Erweiterung B/P_i über A/p ist daher separabel, und p somit unverzweigt. □

Beispiel. Sei $K := \mathbb{Q}(i)$. Dann ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}i = \mathbb{Z}[i]$ und die Basis $\{1, i\}$ von K über $\mathbb{Q}$ hat Diskriminante $d = -4$.

Wir betrachten zunächst das von 2 erzeugte Ideal p in A, also $p := 2A$. Dieses ist offensichtlich prim in A und es lässt sich zeigen, dass $Bp = 2\mathcal{O}_K = P^2$ mit $P := (1+i)$ die Zerlegung von Bp in Primideale in B ist. Da diese nur aus einem Faktor besteht, ist p unzerlegt, und da der Verzweigungsindex dieses Faktors 2 ist, ist p verzweigt.

Sei p nun das von 3 erzeugte Primideal in A. Dann ist $Bp = 3\mathcal{O}_K$ auch prim in $\mathcal{O}_K$, das heißt in diesem Fall ist p unzerlegt und unverzweigt.

Schließlich sei p das von 5 erzeugte Primideal in A. Dann lässt sich zeigen, dass $Bp = P_1P_2$ mit $P_1 = (2+i)$ und $P_2 = (2-i)$ gilt, so dass p unverzweigt und vollständig zerlegt ist.

Sei A wie zuvor ein Dedekindring mit Quotientenkörper K, L/K eine endliche separable Erweiterung und B der ganze Abschluss von A in L. Die **Diskriminante** D von B über A ist definiert als das Ideal in A erzeugt von den Diskriminanten $d(\omega_1, \ldots, \omega_n)$ aller in B enthaltenen Basen von L über K, das heißt

$$D = \Big(\big\{d(\omega_1, \ldots, \omega_n) \colon \{\omega_1, \ldots, \omega_n\} \subseteq B \text{ ist Basis von } L \text{ über } K\big\}\Big) \subseteq A.$$

Die Primteiler von D sind genau die Primideale in A, die verzweigen.

Sei nun p eine ungerade Primzahl in $\mathbb{Z}$. Für $a \in \mathbb{Z}$ definieren wir $\left(\frac{a}{p}\right) = 0$, falls p die Zahl a teilt, und ansonsten

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } x^2 = a \bmod p \text{ eine Lösung in } \mathbb{Z} \text{ hat,} \\ -1, & \text{falls } x^2 = a \bmod p \text{ keine Lösung in } \mathbb{Z} \text{ hat.} \end{cases}$$

Der Ausdruck $\left(\frac{a}{p}\right)$ wird als **Legendre-Symbol** bezeichnet. Es gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Wir behaupten, dass $(\mathbb{F}_p^*)^2 = \{a^2 \colon a \in \mathbb{F}_p^*\}$ eine Untergruppe von $\mathbb{F}_p^*$ vom Index 2 ist: Seien dazu $a, b \in \mathbb{F}_p^*$ mit $a^2 = b^2$. Dann ist $(a+b)(a-b) = 0$ und deswegen $a = \pm b$. Das heißt, es gilt

$$\left|(\mathbb{F}_p^*)^2\right| = \frac{1}{2}\left|\mathbb{F}_p^*\right| = \frac{p-1}{2}.$$

Insbesondere ist $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$. Das Legendre-Symbol beschreibt also gerade den natürlichen Homomorphismus

$$\mathbb{F}_p^* \to (\mathbb{F}_p^*)/(\mathbb{F}_p^*)^2.$$

Weiterhin behaupten wir, dass gilt

$$a^{(p-1)/2} = \left(\frac{a}{p}\right) \mod p.$$

Sei dazu $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$ und $\left(\frac{a}{p}\right) = 1$. Dann ist $a = x^2 \mod p$ für ein $x \in \mathbb{Z}$ und es gilt $\mathrm{ggT}(x,p) = 1$. Damit folgt

$$a^{(p-1)/2} = x^{p-1} = 1 \mod p.$$

Sei umgekehrt $a^{(p-1)/2} = 1 \mod p$ für eine $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$. Sei weiterhin $x \in \mathbb{Z}$ mit $x \neq a$ und $\mathrm{ggT}(x,p) = 1$. Dann ist $a = x^j \mod p$ für ein $j \in \mathbb{Z}$, $j \neq 1$, da x die Gruppe $\mathbb{F}_p^*$ erzeugt. Es folgt

$$x^{j(p-1)/2} = a^{(p-1)/2} = 1 \mod p,$$

sodass $j(p-1)/2$ ein Vielfaches von $p-1$ sein muss. Damit ist j gerade und $a = (x^{j/2})^2 \mod p$ impliziert $\left(\frac{a}{p}\right) = 1$.

Wir bemerken, dass ich sich außerdem

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

zeigen lässt.

Satz 7.13. *Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0,1$ und $K = \mathbb{Q}(\sqrt{d}\,)$. Sei weiter p eine Primzahl mit $\mathrm{ggT}(p,2d) = 1$. Dann gilt die folgende Äquivalenz:*

$$p\mathbb{Z} \text{ ist vollständig zerlegt in } K \quad \Longleftrightarrow \quad \left(\frac{d}{p}\right) = 1$$

Beweis. Wir betrachten zunächst den Fall $d = 2,3 \mod 4$. Offensichtlich ist $\sqrt{d}$ ein primitives Element der Erweiterung $K/\mathbb{Q}$ und es gilt $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d} = \mathbb{Z}[\sqrt{d}]$, sodass $F = \mathcal{O}_K$ ist. Es folgt $p\mathcal{O}_K + F = \mathcal{O}_K$. Nach Definition ist $p\mathbb{Z}$ genau dann vollständig zerlegt in K, wenn das Ideal $p\mathcal{O}_K$ in K in Primideale $P_1 \neq P_2$ zerfällt. (Die Erweiterung $K/\mathbb{Q}$ ist vom Grad 2.) Nach Theorem 7.9 ist dies genau dann der Fall, wenn das Minimalpolynom $f \in \mathbb{Z}[x]$ von $\sqrt{d}$ über $\mathbb{F}_p$ in zwei verschiedene Primelemente zerfällt. Das Minimalpolynom von $\sqrt{d}$ ist aber gerade $f = x^2 - d$. Dieses zerfällt genau dann über $\mathbb{F}_p$, wenn $x^2 = d$ eine ganzzahlige Lösung mod p besitzt. Dies zeigt die Behauptung im Fall $d = 2,3 \mod 4$.

Sei nun $d = 1 \mod 4$. Auch hier können wir $\sqrt{d}$ als primitves Element der Erweiterung $K/\mathbb{Q}$ wählen. Es ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega = (1+\sqrt{d}\,)/2$, und daher

$$2 \in F = \{x \in \mathcal{O}_K \colon x\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}\,]\}.$$

Also teilt F das Ideal $2\mathcal{O}_K$. Andererseits gilt aber $1 \notin F$, und somit ist $F \subsetneq \mathcal{O}_K$ und $F \cap \mathbb{Z} \neq \mathbb{Z}$. Es folgt $F \cap \mathbb{Z} = 2\mathbb{Z}$. Wegen $(p, 2d) = 1$ ist p ungerade. Also gilt

$$p\mathbb{Z} + (F \cap \mathbb{Z}) = \mathbb{Z},$$

das heißt $p\mathbb{Z}$ und $F \cap \mathbb{Z}$ sind teielrfremd. Wir können somit Theorem 7.9 verwenden. Die Behauptung folgt dann analog zur Argumentation im ersten Fall. □

Zum Abschluss dieses Abschnitts zitieren wir noch ein Resultat, welches die Berechnung des Legendre-Symbols ermöglicht. Wir verzichten auf einen Beweis.

Theorem 7.14. *Seien p und q ungerade, voneinander verschiedene Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

und

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

8 Hilberts Verzweigungstheorie

Wir spezialisieren nun die Betrachtungen aus dem vorhergehenden Kapitel auf Galoiserweiterungen. Wir beginnen mit einigen rein algebraischen Resultaten, welche wir im Folgenden benötigen werden.

Satz 8.1. *Sei L/K eine algebraische Körpererweiterung und*

$$K_s = \{a \in L \colon a \text{ separabel über } K\}.$$

Dann ist K_s/K eine separabele Körpererweiterung und es gilt $[L : K]_s = [K_s : K]$. Ist L/K eine normale Erweiterung, so auch K_s/K.

Wir verzichten auf den Beweis.

Satz 8.2. *Sei L/K eine endliche normale Körpererweiterung. Dann ist die Abbildung*

$$\mathrm{Aut}_K(L) \to \mathrm{Aut}_K(K_s),\ f \mapsto f|_{K_s}$$

eine Bijektion.

Beweis. Sei $a \in K_s$. Dann ist das Minimalolynom $m_{a,K}$ von a über K separabel. Also ist auch $m_{f(a),K}$ für ein $f \in \mathrm{Aut}_K(L)$ separabel und somit $f(K_s) \subseteq K_s$. Die gegebene Abbildung ist daher wohldefiniert.

Da die Erweiterung L/K normal ist, gilt $|\mathrm{Aut}_K(L)| = [L : K]_s$, und nach dem vorhergehenden Satz ist $[L : K]_s = [K_s : K]$. Ferner besagt der Satz, dass die Erweiterung K_s/K separabel und normal ist, das heißt es gilt

$$|\mathrm{Aut}_K(L)| = [K_s : K] = [K_s : K]_s = |\mathrm{Aut}_K(K_s)|.$$

Es reicht daher zu zeigen, dass die Abbildung surjektiv ist. Sei dazu $\sigma \in \mathrm{Aut}_K(K_s)$. Dann lässt sich σ als Abbildung $K_s \to \overline{L}$ betrachten. Zu dieser existiert eine Fortsetzung $\sigma' \colon L \to \overline{L}$, und da die Erweiterung L/K normal ist, folgt $\sigma'(L) \subseteq L$, also $\sigma' \in \mathrm{Aut}_K(L)$. Offensichtlich gilt $\sigma'|_{K_s} = \sigma$. Damit ist die gegebene Abbildung surjektiv. □

Im Folgenden sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$ und B der ganze Abschluss von A in L. Sei $\sigma \in G$. Ist $a \in L$ ganz über A, so auch $\sigma(a)$. Es folgt $\sigma(B) \subseteq B$. Da dies auch für σ^{-1} gilt, folgt $B = \sigma(\sigma^{-1}(B)) \subseteq \sigma(B)$. Also gilt $\sigma(B) = B$.

Sei nun p ein nicht-triviales Primideal in A und P ein Primideal in B über p, das heißt $P \cap A = p$. Dann gilt

$$\sigma(P) \cap A = \sigma(P) \cap \sigma(A) = \sigma(P \cap A) = \sigma(p) = p,$$

das heißt $\sigma(P)$ ist ebenfalls ein Primideal über p. Wir nennen die Primideale der Form $\sigma(P)$, $\sigma \in G$, zu P konjugierte Primideale.

Satz 8.3. *Die Galoisgruppe G permutiert die Primideale über p transitiv.*

Beweis. Nach den vorhergehenden Bemerkungen wissen wir bereits, dass G die Primideale über P permutiert. Es bleibt zu zeigen, dass diese Permutation transitiv ist.

Sei $Bp = P_1^{e_1} \dots P_r^{e_r}$ die Zerlegung von Bp in Primideale P_i in B. Wir zeigen, dass es für alle i ein $\sigma \in G$ mit $P_i = \sigma(P_1)$ gibt. Angenommen es gibt ein i mit $P_i \neq \sigma(P_1)$ für alle $\sigma \in G$. Dann gilt

$$P_i + \prod_{\sigma \in G} \sigma(P_1) = B,$$

da P_i zu allen $\sigma(P_1)$ teilerfremd ist, also auch zu deren Produkt. Es gibt daher Elemente $a \in P_i$ und $b \in \prod_{\sigma \in G} \sigma(P_1)$ mit $a + b = 1$. Da alle $\sigma(P_1)$ Primideale sind, sind zwei Ideale $\sigma(P_1)$ und $\sigma'(P_1)$ entweder teilerfremd oder identisch. Somit ist

$$b \in \prod_{\sigma \in G} \sigma(P_1) = \bigcap_{\sigma \in G} \sigma(P_1).$$

Es folgt $a \notin \sigma(P_1)$ für alle $\sigma \in G$, denn wäre $a \in \sigma(P_1)$ für ein $\sigma \in G$, so würde $1 = a + b \in \sigma(P_1) \neq B$ einen Widerspruch ergeben. Somit ist $\sigma^{-1}(a) \notin P_1$ für alle $\sigma \in G$, und daher

$$\mathrm{N}_{L/K}(a) = \prod_{\sigma \in G} \sigma(a) = \prod_{\sigma \in G} \sigma^{-1}(a) \notin P_1,$$

da P_1 prim ist. Andererseits gilt aber

$$\mathrm{N}_{L/K}(a) = a \prod_{\sigma \in G, \sigma \neq 1} \sigma(a) \in P_i,$$

und da a ganz über A ist auch $\mathrm{N}_{L/K}(a) \in A$. Dies ergibt $\mathrm{N}_{L/K}(a) \in A \cap P_i = p$, und wegen $p \subseteq P_1$ widerspricht das $\mathrm{N}_{L/K}(a) \notin P_1$. □

Satz 8.4. *Sei p ein nicht-triviales Primideal in A und $Bp = P_1^{e_1} \dots P_r^{e_r}$ die Primfaktorzerlegung von Bp in B. Dann gilt*

$$e_1 = \dots = e_r = e \quad \textit{und} \quad f_1 = \dots = f_r = f.$$

Nach Theorem 7.5 ist die fundamentale Identität in diesem Fall also gegeben durch

$$efr = n.$$

Beweis. Sei $P = P_1$. Dann ist $P_i = \sigma(P)$ für ein $\sigma \in G$, da G transitiv auf den P_i wirkt. Dieses σ induziert einen Isomorphismus

$$B/P \to B/\sigma(P),\ b + P \mapsto \sigma(b) + \sigma(P).$$

Die Abbildung ist A/p-linear, sodass gilt

$$f_1 = [B/P : A/p] = [B/P_i : A/p] = f_i.$$

Weiterhin ist

$$Bp = \sigma(Bp) = P_{\tau(1)}^{e_1} \dots P_{\tau(r)}^{e_r}$$

mit $\tau \in S_r$ und $\tau(1) = i$. Somit folgt auch $e_i = e_1$. □

Sei P ein nicht-triviales Primideal in B. Dann wird

$$G_P = \{\sigma \in G \colon \sigma(P) = P\}$$

als **Zerlegungsgruppe** von P über K bezeichnet und der entsprechende Fixkörper

$$Z_P = L^{G_P} = \{x \in L \colon \sigma(x) = x \text{ für alle } \sigma \in G_P\}$$

wird **Zerlegungskörper** von P über K genannt. Nach dem Hauptsatz der Galoistheorie ist L/Z_P eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/Z_P) = G_P$.

Sei nun $p = P \cap A$. Dann gilt nach den beiden vorangegangenen Sätzen, dass die Zerlegung von Bp in B gerade durch

$$Bp = \prod_{\sigma \in G/G_P} \sigma(P)^e$$

gegeben ist. Es folgt

$$r = |G/G_P| = |G| \,/\, |G_P| = [L : K]/[L : Z_P] = [Z_P : K].$$

Also ist die Zerlegungsgruppe G_P genau dann trivial ist, wenn $Z_P = L$ ist. Dies ist aber genau dann der Fall, wenn p vollständig zerlegt ist. Umgekehrt gilt genau dann $G_P = G$, wenn $Z_P = K$ ist. Dies ist genau dann der Fall, wenn p unzerlegt ist. Zusammenfassend erhalten wir

$$G_P = \{1\} \quad \Longleftrightarrow \quad Z_P = L \quad \Longleftrightarrow \quad p \text{ vollständig zerlegt}$$

und

$$G_P = G \quad \Longleftrightarrow \quad Z_P = K \quad \Longleftrightarrow \quad p \text{ unzerlegt.}$$

Als nächstes definieren wir

$$P_Z = P \cap Z_P \quad \text{und} \quad B_Z = B \cap Z_P.$$

Dann ist P_Z ein Primideal in B_Z und B_Z der ganze Abschluss von A in Z_P. Nach Theorem 7.1 ist B_Z ein Dedekindring. Ferner ist Z_P ein Quotientenkörper von B_Z.

Satz 8.5. *Sei P ein nicht-triviales Primideal in B und $p := P \cap A$. Sei weiterhin e der eindeutige Verzweigungsindex und f der eindeutige Trägheitsgrad von P über p. Dann gilt:*

(1) Das Ideal P ist das einzige Primideal in B über P_Z, das heißt es gilt $BP_Z = P^{e'}$ für ein $e' \in \mathbb{N}$. Insbesondere ist P_Z unzerlegt in B.

(2) Das Ideal P hat Verzweigungsindex e und Trägheitsgrad f als Ideal über P_Z, das heißt es gilt $BP_Z = P^e$ und $[B/P : B_Z/P_Z] = f$.

(3) Der Verzweigungsindex und der Trägheitsgrad von P_Z über p sind beide 1, das heißt es gilt $B_Z p = P_Z \ldots$ und $[B_Z/P_Z : A/p] = 1$.

Beweis. Wir zeigen zunächst (1). Die Erweiterung L/Z_P ist eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/Z_P) = G_P$. Wir müssen zuerst zeigen, dass der ganze Abschluss von B_Z in L gerade B ist. Sei dazu $a \in L$ ganz über B_Z. Da B_Z ganz über A ist, ist a auch ganz über A, das heißt es gilt $a \in B$, und damit $\overline{B_Z} \subseteq B$. Die Umkehrung ist klar.

Weiterhin ist P wegen $P_Z = P \cap Z_P$ offensichtlich ein Primideal in B über P_Z und nach Satz 8.3 gibt es daher zu jedem Primteiler P' von BP_Z ein $\sigma \in \mathrm{Gal}(L/Z_P)$, sodass $P' = \sigma(P)$ ist. Wegen $\mathrm{Gal}(L/Z_P) = G_P$ ist aber $\sigma(P) = P$ für alle $\sigma \in \mathrm{Gal}(L/Z_P)$, das heißt P ist das einzige Primideal in B über P_Z.

Wir zeigen nun Teil (2) und (3) in einem. Nach Satz 8.4 gilt $efr = n$, wobei r die Anzahl der Primteiler des Ideals Bp in B ist. Wie weiter oben bemerkt, gilt außerdem $r = |G|/|G_P|$. Es folgt

$$ef = \frac{n}{r} = \frac{[L:K]}{|G|/|G_P|} = |G_P| = |\mathrm{Gal}(L/Z_P)| = [L:Z_P]. \tag{$\star$}$$

Seien e' und f' der Verzweigungsindex und Trägheitsgrad von P über P_Z und e'' und f'' der Verzweigungsindex und Trägheitsgrad von P_Z über p. Dann ist $BP_Z = P^{e'}$, da P nach (1) der einzige Primteiler von BP_Z ist, und $B_Z p = P_Z^{e''} \ldots$ Es folgt

$$Bp = B(B_Z p) = B(P_Z^{e''} \ldots) = (BP_Z)^{e''} \ldots = P^{e'e''} \ldots$$

Also ist $e = e'e''$. Entsprechend gilt für die Trägheitsgrade

$$f = [B/p : A/p], \quad f' = [B/p : B_Z/P_Z], \quad f'' = [B_Z/P_Z : A/p].$$

Mit Hilfe der Gradformel für Körpererweiterungen erhält man daher $f = f'f''$. Weiter lautet die fundamentale Identität für die Zerlegung von P_Z in B

$$e'f' = [L : Z_P].$$

Mit $(\star)$ folgt dann $e'f' = ef = e'e''f'f''$. Also ist $e''f'' = 1$, und daher $e'' = f'' = 1$. Somit gilt $e = e'e'' = e'$ und $f = f'f'' = f'$. Dies zeigt (2) und (3). □

Für $\sigma \in G_P$ ist die Abbildung

$$\overline{\sigma} \colon B/P \to B/P,\ b + P \mapsto \sigma(b) + P$$

wohldefiniert. Wir schreiben $K(P) = B/P$ und $K(p) = A/p$.

Satz 8.6. *Die Erweiterung $K(P)/K(p)$ ist normal und die Abbildung*

$$G_P \to \mathrm{Aut}_{K(p)}(K(P)),\ \sigma \mapsto \overline{\sigma}$$

ist ein surjektiver Homomorphismus.

Beweis. Sei $b \in B \subseteq L$ und $f = x^m + a_1 x^{m-1} + \ldots + a_m$ das Minimalpolynom von b über K. Dann ist $f \in A[x]$. Da L/K normal ist, gilt $f = \prod_{i=1}^{m}(x - b_i)$ für geeignete $b_i \in L$. Genauer gilt sogar $b_i \in B$, da diese als Nullstellen des normierten Polynoms $f \in A[x]$ ganz über A sind. Das Polynom

$$\overline{f} = x^m + \overline{a_1} x^{m-1} + \ldots + \overline{a_m}$$

mit $\overline{a_i} = a_i + P$ hat Koeffizienten in $(A + P)/P \cong A/(A \cap P) = A/p$ und zerfällt über B/P in Linearfaktoren. Weiterhin ist $\overline{b} = b + P$ eine Nullstelle dieses Polynoms. Das Minimalpolynom $\overline{g}$ von $\overline{b}$ über A/p ist also ein Teiler von $\overline{f}$, und zerfällt daher ebenfalls über B/P.

Sei nun $\overline{h} \in (A/p)[x]$ ein beliebiges irreduzibles Polynom, welches eine Nullstelle $\overline{b}$ in B/P besitzt. Bis auf Normiertheit ist dann $\overline{h}$ das Minimalpolynom von $\overline{b}$ über A/p, und zerfällt daher nach obiger Argumentation über B/P in Linearfaktoren. Dies beweist, dass B/P normal über A/p ist.

Sei S die maximale separable Erweiterung von A/p in B/P und $\tau \in \mathrm{Aut}_{A/p}(S)$. Wir werden zeigen, dass τ von einem Element aus G_P induziert wird. Sei dazu $\overline{\theta} = \theta + P$ ein primitives Element von S über A/p und $\overline{g} \in (A/p)[x]$ das Minimalpolynom von $\overline{\theta}$ über A/p. Dann ist $\tau(\overline{\theta})$ Nullstelle von $\overline{g}$, da $\overline{g} \circ \tau = \tau \circ \overline{g}$ gilt. Weiter gilt nach Satz 8.5, dass $[B_Z/P_Z : A/p] = 1$ und somit $B_Z/P_Z = A/p$ ist. Also können wir $\overline{g}$ auch als Polynom über B_Z/P_Z betrachten.

Sei f das Minimalpolynom von θ über Z_P. Dann ist $f \in B_Z[x]$, da θ ganz über A und damit auch ganz über B_Z ist. Sei weiter $\overline{f}$ die Projektion von f in

$$B_Z/P_Z = A/p = A/(A \cap P) \cong (A + P)/P.$$

Dann ist $\overline{\theta}$ Nullstelle von $\overline{f}$ und somit wird $\overline{f}$ vom Minimalpolynom $\overline{g}$ von $\overline{\theta}$ geteilt. Insbesondere hat f somit eine Nullstelle $\xi \in L$ mit $\xi = \tau(\overline{\theta}) \bmod P$. Da f das Minimalpolynom von θ über Z_P ist, permutiert die Galoisgruppe $\mathrm{Gal}(L/Z_P) = G_P$ die Nullstellen von f. Es gibt daher ein Element $\sigma \in G_P$ mit $\sigma(\theta) = \xi$. Damit folgt $\overline{\sigma}(\overline{\theta}) = \tau(\overline{\theta})$. □

Der Kern I_P der Abbildung

$$G_P \to \mathrm{Aut}_{A/p}(B/P)$$

wird **Trägheitsgruppe** von P über K genannt. Da die Abbildung nach dem vorangegangenen Satz surjektiv ist, gilt $G_P/I_P \cong \mathrm{Aut}_{A/p}(B/P)$ und die Sequenz

$$1 \longrightarrow I_P \longrightarrow G_P \longrightarrow \mathrm{Aut}_{A/p}(B/P) \longrightarrow 1$$

ist exakt. Wir definieren weiter

$$T_P = L^{I_P} = \{x \in L \colon \sigma(x) = x \text{ für alle } \sigma \in I_P\}$$

und bezeichnen T_P als **Trägheitskörper** von P über K. Es gilt $K \subseteq Z_P \subseteq T_P \subseteq L$. Nach dem Hauptsatz der Galoistheorie ist L/T_P eine Galoiserweiterung mit Galoisgruppe

$\mathrm{Gal}(L/T_P) = I_P$. Da I_P als Kern des obigen Gruppenhomomorphismus eine normale Untergruppe von G_P ist, ist die Erweiterung T_P/Z_P normal und somit ebenfalls eine Galoiserweiterung mit Galoisgruppe

$$\mathrm{Gal}(T_P/Z_P) \cong \mathrm{Gal}(L/Z_P)/\,\mathrm{Gal}(L/T_P) = G_P/I_P \cong \mathrm{Aut}_{A/p}(B/P).$$

Insbesondere ist $[T_P : Z_P] = [B/P : A/p]_s$.

Satz 8.7. *Sei $P_T = P \cap T_P$ und $B_T = B \cap T_P$. Sei weiter e der Verzweigungsindex und f der Trägheitsgrad von P über $p = A \cap P$. Ist die Erweiterung $K(P)/K(p)$ separabel, so gilt*

$$|I_P| = [L : T_P] = e, \quad |G_P/I_P| = [T_P : Z_P] = f$$

und

$$BP_T = P^e, \quad [B/P : B_T/P_T] = 1, \quad B_T P_Z = P_T, \quad [B_T/P_T : B_Z/P_Z] = f.$$

Beweis. Wir wählen T_P statt K als Grundkörper. Die Erweiterung L/T_P ist eine endliche Galoiserweiterung mit $\mathrm{Gal}(L/T_P) = I_P$ und wegen $I_P \subseteq G_P$ fixieren alle Elemente aus $\mathrm{Gal}(L/T_P)$ das Primideal P. Weiterhin operieren alle Elemente aus I_P nach Definition trivial auf B/P. Setze nun $K(P_T) = B_T/P_T$ und sei $\overline{\sigma} \in \mathrm{Aut}_{K(P_T)}(K(P))$. Dann kommt $\overline{\sigma}$ nach Satz 8.6 von einem $\sigma \in G_P$, und da $\overline{\sigma}$ trivial auf $K(P_T)$ wirkt, ist σ ein Element von $\mathrm{Aut}_{T_P}(L) = I_P$. Dieses wirkt aber wie weiter oben bemerkt trivial auf ganz $K(P)$. Also ist $\overline{\sigma} = 1$, und damit $|\mathrm{Aut}_{K(P_T)}(K(P))| = 1$.

Nach Satz 8.6 wissen wir außerdem, dass mit $K(P)/K(p)$ auch $K(P)/K(P_T)$ eine normale Erweiterung ist. Somit ist $K(P)/K(P_T)$ eine Galoiserweiterung, denn nach Voraussetzung ist $K(P)/K(p)$ auch separabel. Für die Galoisgruppe gilt

$$[K(P) : K(P_T)] = |\mathrm{Gal}(K(P)/K(P_T))| = \left|\mathrm{Aut}_{K(P_T)}(K(P))\right| = 1.$$

Damit folgt

$$f = [K(P) : K(p)] = [K(P) : K(P_T)] \cdot [K(P_T) : K(p)] = [K(P_T) : K(p)].$$

Weiterhin gilt $\mathrm{Gal}(T_P/Z_P) \cong G_P/I_P \cong \mathrm{Aut}_{A/p}(B/P)$, wie weiter oben gezeigt, und daher

$$|\mathrm{Gal}(T_P/Z_P)| = |G_P/I_P| = \left|\mathrm{Aut}_{K(p)}(K(P))\right| = [K(P) : K(p)] = f.$$

Sei nun kurz Z_P unser Grundkörper. Nach Teil (2) von Satz 8.5 gilt $BP_Z = P^e$ und $[K(P) : K(P_Z)] = f$. Die entsprechende fundamentale Identität ist daher gegeben durch $ef = [L : Z_P]$. Es folgt

$$ef = |\mathrm{Gal}(L/Z_P)| = |G_P| = |G_P/I_P|\ |I_P| = f \cdot |I_P|\,,$$

also $|I_P| = e$ und $|G_P/I_P| = f$.

Sei jetzt wieder T_P unser Grundkörper wie zuvor. Wir betrachten die Zerlegung von BP_T in B. Die entsprechende fundamentale Identität lautet

$$e(P/P_T)\, f(P/P_T)\, r(P/P_T) = [L : T_P] = |I_P| = e.$$

Dabei ist $f(P/P_T) = [K(P) : K(P_T)] = 1$. Weiter ist auch $r(P/P_T) = 1$, denn es gilt $BP_Z \subseteq BP_T$ und nach Teil (1) von Satz 8.5 ist P der einzige Primteiler von BP_Z. Damit folgt $e(P/P_T) = e$, und somit $BP_Z = BP_T = P^e$.

Als nächstes betrachten wir die Erweiterung T_P/Z_P. Die fundamentale Identität der Zerlegung von $B_T P_Z$ in B_T lautet

$$e(P_T/P_Z)\, f(P_T/P_Z)\, r(P_T/P_Z) = [T_P : Z_P] = |\mathrm{Gal}(T_P/Z_P)| = f.$$

Wieder nach Teil (2) von Satz 8.5 ist $[K(P) : K(P_Z)] = f$, also

$$f(P_T/P_Z) = [K(P_T) : K(P_Z)] = \frac{[K(P) : K(P_Z)]}{[K(P) : K(P_T)]} = \frac{f}{1}.$$

Damit folgt $e(P_T/P_Z) = r(P_T/P_Z) = 1$, das heißt $B_T P_Z = P_T$. □

Sei $K(P)/K(p)$ weiterhin separabel. Dann haben wir das folgende Diagramm:

$$K \xrightarrow[1]{1} Z_P \xrightarrow[f]{1} T_P \xrightarrow[1]{e} L$$

Definiere wie zuvor $P_Z = P \cap Z_P$ und $P_T = P \cap T_P$, sowie $B_Z = B \cap Z_P$ und $B_T = B \cap T_P$. Dann ist

$$\begin{array}{cccc} Bp = P^e \ldots, & B_Z p = P_Z \ldots, & B_T P_Z = P_T, & BP_T = P^e \\ [B/P : A/p] = f, & [B_Z/P_Z : A/p] = 1, & [B_T/P_T : B_Z/P_Z] = 1, & [B/P : B_T/P_T] = 1. \end{array}$$

Weiterhin gilt

$$I_P = \{1\} \quad \Longleftrightarrow \quad T_P = L \quad \Longleftrightarrow \quad p \text{ unverzweigt in } L.$$

9 Kreisteilungskörper

Wir betrachten nun die Kreisteilungskörper als Beispiel algebraischer Zahlkörper. Wir benötigen folgende grundlegende Resultate.

Satz 9.1. *Sei K ein Körper und $f = \prod_{i=1}^{n}(x - a_i)$ mit $a_i \in K$. Dann ist*

$$\prod_{i<j}(a_i - a_j)^2 = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(a_i).$$

Beweis. Es ist $f' = \sum_{i=1}^{n} \prod_{j\neq i}(x - a_j)$, sodass $f'(a_i) = \prod_{j\neq i}(a_i - a_j)$ und damit

$$\prod_{i=1}^{n} f'(a_i) = \prod_{i=1}^{n}\prod_{j\neq i}(a_i - a_j) = (1-)^{n(n-1)/2} \prod_{i<j}(a_i - a_j)^2. \qquad \square$$

Satz 9.2. *Sei $K/\mathbb{Q}$ eine endliche Körpererweiterung vom Grad n mit $K = \mathbb{Q}(a)$. Dann gilt*

$$d(1, a, \ldots, a^{n-1}) = (-1)^{n(n-1)/2}\, \mathrm{N}_{K/\mathbb{Q}}(m'_{a,\mathbb{Q}}(a)).$$

Beweis. Seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen $\mathbb{Q}$-Homomorphismen $K \to \overline{K}$. Dann ist

$$d(1, a, \ldots, a^{n-1}) = \det(A)^2$$

mit

$$A = \begin{pmatrix} \sigma_1(1) & \sigma_1(a) & \cdots & \sigma_1(a^{n-1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(a) & \cdots & \sigma_n(a^{n-1}) \end{pmatrix} = \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{pmatrix},$$

wobei wir $a_i := \sigma_i(a)$ gesetzt haben. Es folgt $\det(A) = \prod_{i<j}(a_j - a_i)$ und damit

$$d(1, a, \ldots, a^{n-1}) = \prod_{i<j}(a_i - a_j)^2 = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(a_i)$$

nach dem vorangegangenen Satz, wobei

$$f = \prod_{i=1}^{n}(x - a_i) = \prod_{i=1}^{n}(x - \sigma_i(a)) = m_{a,\mathbb{Q}}.$$

Es ergibt sich

$$\prod_{i=1}^{n} m'_{a,\mathbb{Q}}(a_i) = \prod_{i=1}^{n} m'_{a,\mathbb{Q}}(\sigma_i(a)) = \prod_{i=1}^{n} \sigma_i(m'_{a,\mathbb{Q}}(a)) = \mathrm{N}_{K/\mathbb{Q}}(m'_{a,\mathbb{Q}}(a)).$$

Dies zeigt die Behauptung des Satzes. $\square$

Sei ξ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\xi)/\mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe $G \cong (\mathbb{Z}/n\mathbb{Z})^*$. Das n-te Kreisteilungspolynom ist definiert als

$$\phi_n = \prod_{i=1}^{\varphi(n)} (x - \xi_i)$$

wobei ξ_i die primitiven n-ten Einheitswurzeln in $\overline{\mathbb{Q}}$ durchläuft und φ die Eulersche Phi-Funktion ist. Nach dem Lemma von Gauß gilt $\phi_n \in \mathbb{Z}[x]$ und damit $\xi \in \mathcal{O}$, wobei $\mathcal{O}$ den ganzen Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\xi)$ bezeichne.

Weiter ist ϕ_n irreudzibel in $\mathbb{Q}[x]$. Insbesondere ist ϕ_n somit das Minimalpolynom von ξ über $\mathbb{Q}$. Ist p eine Primzahl, so gilt

$$\phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

und

$$\phi_{p^\nu} = \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} = \left(x^{p^{\nu-1}}\right)^{p-1} + \left(x^{p^{\nu-1}}\right)^{p-2} + \ldots + x^{p^{\nu-1}} + 1.$$

Satz 9.3. *Sei p eine Primzahl, $n = p^\nu$ und ξ eine primitive n-te Einheitswurzel. Sei weiter $\lambda = 1 - \xi$,*

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n) = p^{\nu-1}(p-1) = d$$

und $\mathcal{O}$ der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\xi)$. Dann hat die $\mathbb{Q}$-Basis $\{1, \xi, \ldots, \xi^{d-1}\}$ von $\mathbb{Q}(\xi)$ die Diskriminante

$$d(1, \xi, \ldots, \xi^{d-1}) = (-1)^{d(d-1)/2} p^m$$

mit $m = p^{\nu-1}(p\nu - \nu - 1)$, und es gilt $(p) = (\lambda)^d$ als Ideale in $\mathcal{O}$.

Beweis. Es ist

$$d(1, \xi, \ldots, \xi^{d-1}) = (-1)^{d(d-1)/2} \, \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\phi_n'(\xi)) \qquad (\star)$$

nach Satz 9.2. Differenzieren der Gleichung

$$\left(x^{p^{\nu-1}} - 1\right) \phi_n(x) = x^{p^\nu} - 1$$

nach x und anschließendes Einsetzen von ξ ergibt

$$(\xi_p - 1)\phi_n'(\xi) = p^\nu \xi^{-1},$$

wobei $\xi_p := \xi^{p^{\nu-1}}$ ist. Es folgt

$$\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\phi_n'(\xi)) = \frac{\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(p^\nu)}{\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi) \; \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi_p - 1)}. \qquad (\sharp)$$

Offensichtlich ist $\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(p^\nu) = p^{\nu d}$ wegen $[\mathbb{Q}(\xi) : \mathbb{Q}] = d$ und $p^\nu \in \mathbb{Q}$. Weiterhin gilt

$$\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi) = \prod_{i=1}^{d}(-\xi_i) = \phi_n(0) = 1.$$

Es verbleibt $\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi_p - 1)$ zu bestimmen. Dazu bemerken wir zunächst, dass gilt

$$\mathrm{N}_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(\xi_p - 1) = \prod_{i=1}^{p-1}(\xi_p^i - 1) = (-1)^{p-1}\prod_{i=1}^{p-1}(1 - \xi_p^i) = (-1)^{p-1}\phi_p(1) = (-1)^{p-1}p.$$

Außerdem ist

$$[\mathbb{Q}(\xi) : \mathbb{Q}(\xi_p)] = \frac{\varphi(n)}{\varphi(p)} = \frac{p^{\nu-1}(p-1)}{p-1} = p^{\nu-1},$$

und daher

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi_p - 1) &= \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}(\xi_p)}\left(\mathrm{N}_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(\xi_p - 1)\right)\\ &= \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}(\xi_p)}\left((-1)^{p-1}p\right) = (-1)^{(p-1)p^{\nu-1}}p^{p^{\nu-1}} = (-1)^d p^{p^{\nu-1}} = p^{p^{\nu-1}},\end{aligned}$$

da d gerade ist. Kombinieren dieser Resultate mit $(\star)$ und $(\sharp)$ ergibt

$$d(1, \xi, \ldots, \xi^{d-1}) = (-1)^{d(d-1)/2}p^{\nu d - p^{\nu-1}} = (-1)^{d(d-1)/2}p^m.$$

Damit verbleibt zu zeigen, dass $\mathcal{O}p = \mathcal{O}(1-\xi)^d$ gilt. Aus $\phi_n(1) = p$ folgt zunächst

$$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*}(1 - \xi^a) = p. \tag{$\dagger$}$$

Weiter gilt für jedes $a \in (\mathbb{Z}/n\mathbb{Z})^*$, dass $1 - \xi^a = \varepsilon_a(1-\xi)$ ist, wobei

$$\varepsilon_a = \frac{1-\xi^a}{1-\xi} = \xi^{a-1} + \xi^{a-2} + \ldots + \xi + 1 \in \mathcal{O}.$$

Wir halten ein solches a fest und wählen dazu $a' \in (\mathbb{Z}/n\mathbb{Z})^*$ mit $aa' = 1$. Dann ist

$$\frac{1-\xi}{1-\xi^a} = \frac{1-(\xi^a)^{a'}}{1-\xi^a} = (\xi^a)^{a'-1} + \ldots + \xi^a + 1 \in \mathcal{O},$$

das heißt ε_a^{-1} liegt ebenfalls in $\mathcal{O}$. Also gilt $\varepsilon_a \in \mathcal{O}^*$. Aus $(\dagger)$ folgt somit $p = \varepsilon(1-\xi)^d$ mit

$$\varepsilon = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*}\varepsilon_a \in \mathcal{O}^*.$$

Also gilt tatsächlich $\mathcal{O}p = \mathcal{O}(1-\xi)^d$. □

In der Situation des vorangegangenen Satzes gilt $\mathcal{O}p = (\lambda)^d$, wobei d der Grad der Erweiterung $\mathbb{Q}(\xi)/\mathbb{Q}$ ist. Mit der fundamentalen Identität (siehe Satz 8.4) folgt daher bereits, dass das Ideal (λ) in $\mathcal{O}$ nicht mehr weiter zerlegt werden kann, und damit prim ist. Also ist $\mathcal{O}p = (\lambda)^d$ die Primfaktorzerlegung von $\mathcal{O}p$ in $\mathcal{O}$. Der Trägheitsgrad von (λ) über p ist dementsprechend 1.

Theorem 9.4. *Sei ξ eine primitive n-te Einheitswurzel in $\overline{\mathbb{Q}}$. Dann ist der Ring der ganzen Zahlen in $\mathbb{Q}(\xi)$ gegeben durch*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\xi + \ldots + \mathbb{Z}\xi^{\varphi(n)-1} = \mathbb{Z}[\xi].$$

Beweis. Offensichtlich gilt $\mathbb{Z}[\xi] \subseteq \mathcal{O}$. Es bleibt daher die umgekehrte Inklusion zu zeigen. Setze $d := \varphi(n)$ wie zuvor. Wir betrachten zunächst den Fall $n = p^\nu$.

Nach Satz 9.3 gilt $d(1, \xi, \ldots, \xi^{d-1}) = \pm p^m$ für ein $m \in \mathbb{N}$, und nach Satz 1.16 ist somit $\mathcal{O}p^m \subseteq \mathbb{Z}[\xi]$. Setze $\lambda = 1 - \xi$. Dann ist $\mathcal{O}\lambda$ das einzige Primideal über $p\mathbb{Z}$, das heißt (λ) ist das einzige Primideal in $\mathcal{O}$ mit $(\lambda) \cap \mathbb{Z} = p\mathbb{Z}$, und es gilt $\mathcal{O}p = (\lambda)^d$. Ferner ist der Trägheitsgrad von (λ) über p gerade 1, das heißt es gilt $[\mathcal{O}/(\mathcal{O}\lambda) : \mathbb{Z}/(p\mathbb{Z})] = 1$. Also ist das Ideal $\mathbb{Z}/(p\mathbb{Z}) \cong (\mathbb{Z} + \mathcal{O}\lambda)/(\mathcal{O}\lambda)$ ein Teilkörper vom Index 1 von $\mathcal{O}/(\mathcal{O}\lambda)$, das heißt es gilt

$$\mathcal{O}/(\mathcal{O}\lambda) = (\mathbb{Z} + \mathcal{O}\lambda)/(\mathcal{O}\lambda),$$

und somit $\mathcal{O} = \mathbb{Z} + \mathcal{O}\lambda$. Dies impliziert $\mathcal{O} = \mathbb{Z}[\xi] + \mathcal{O}\lambda$ und wir bemerken

$$\mathcal{O}\lambda = \mathbb{Z}[\xi](1 - \xi) + \mathcal{O}\lambda^2 = \mathbb{Z}[\xi] + \mathcal{O}\lambda^2.$$

Es folgt $\mathcal{O} = \mathbb{Z}[\xi] + (\mathbb{Z}[\xi] + \mathcal{O}\lambda^2) = \mathbb{Z}[\xi] + \mathcal{O}\lambda^2$. Induktiv ergibt sich daher

$$\mathcal{O} = \mathbb{Z}[\xi] + \mathcal{O}\lambda^j$$

für alle $j \geq 1$. Setze $j := md$. Dann ist $\mathcal{O}\lambda^d = ((\lambda)^d)^m = (\mathcal{O}p)^m = \mathcal{O}p^m \subseteq \mathbb{Z}[\xi]$, und somit

$$\mathcal{O} = \mathbb{Z}[\xi] + \mathcal{O}\lambda^j \subseteq \mathbb{Z}[\xi] \subseteq \mathcal{O}.$$

Dies zeigt die Behauptung für den Fall $n = p^\nu$.

Sei nun $n = p_1^{\nu_1} \ldots p_t^{\nu_t}$ die Primfaktorzerlegung von $n \in \mathbb{N}$. Setze $n_i := p_i^{\nu_i}$ und $\xi_i := \xi^{n_i}$. Dann ist ξ_i eine primitive n_i-te Einheitswurzel und es gilt

$$\mathbb{Q}(\xi) = \mathbb{Q}(\xi_1, \ldots, \xi_t) = \mathbb{Q}(\xi_1) \ldots \mathbb{Q}(\xi_t). \tag{$\star$}$$

Weiterhin ist

$$\Big(\mathbb{Q}(\xi_1) \ldots \mathbb{Q}(\xi_i)\Big) \cap \mathbb{Q}(\xi_{i+1}) = \mathbb{Q} \tag{$\sharp$}$$

für alle i und wir haben bereits gezeigt, dass die Menge $\{1, \xi_i, \ldots, \xi_i^{d_i-1}\}$ mit $d_i := \varphi(n_i)$ eine ganzzahlige Basis von $\mathbb{Q}(\xi_i)/\mathbb{Q}$ mit Diskriminante

$$d(1, \xi_i, \ldots, \xi_i^{d_i-1}) = \pm p_i^{m_i}$$

bildet. Wir zeigen nun per Induktion über h, dass die Menge

$$B_h := \big\{\xi_1^{j_1} \ldots \xi_h^{j_h} : j_i = 0, \ldots, d_i - 1\big\}$$

eine ganzzahlige Basis von $K_h := \mathbb{Q}(\xi_1) \ldots \mathbb{Q}(\xi_h)$ über $\mathbb{Q}$ darstellt, deren Diskriminante durch $D_h := \pm p_1^{l_1} \ldots p_h^{l_h}$ für geeignete $l_i \in \mathbb{N}$ gegeben ist.

Der Induktionsanfang wurde bereits gezeigt. Nehme an, dass B_h eine ganzzahlige Basis von K_h mit Diskriminante D_h ist. Dann gilt $K_h \cap \mathbb{Q}(\xi_{h+1}) = \mathbb{Q}$ nach ($\sharp$), und D_h und $d(1, \xi_{h+1}, \ldots, \xi_{h+1}^{d_{h+1}-1}) = \pm p_{h+1}^{m_{h+1}}$ sind teilerfremd. Somit folgt der Induktionsschluss mit Satz 1.19. Wir haben also gezeigt, dass B_t eine ganzzahlige Basis von K_t über $\mathbb{Q}$ ist. Nach ($\star$) gilt aber gerade $K_t = \mathbb{Q}(\xi)$. Es folgt

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\xi_1 + \ldots + \mathbb{Z}\xi_1^{d_1-1} + \mathbb{Z}\xi_2 + \mathbb{Z}\xi_1\xi_2 + \mathbb{Z}\xi_1^2\xi_2 + \ldots + \mathbb{Z}\xi_1^{d_1-1}\ldots\xi_t^{d_t-1}.$$

Da jedes der Basiselemente ξ_i^j eine Potenz von ξ ist, erhalten wir hiermit $\mathcal{O} \subseteq \mathbb{Z}[\xi]$. Dies zeigt die Behauptung. □

Theorem 9.5. *Sei ξ eine primitive n-te Einheitswurzel in $\overline{\mathbb{Q}}$, $n = \prod q^{\nu_q}$ die Primfaktorzerlegung von n und $\mathcal{O}$ der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\xi)$. Sei weiter p eine Primzahl, $m \in \mathbb{Z}$ mit $n = p^{\nu_p}m$ und f_p die Ordnung von p in $(\mathbb{Z}/m\mathbb{Z})^*$. Dann ist die Primfaktorzerlegung von $\mathcal{O}p$ in $\mathcal{O}$ von der Form*

$$\mathcal{O}p = (P_1 \ldots P_r)^{\varphi(p^{\nu_p})}$$

und der Trägheitsgrad von jedem P_i über p ist f_p.

Beweis. Nach dem vorangegangenen Satz ist $\mathcal{O} = \mathbb{Z}[\xi]$, und somit

$$F = \{x \in \mathcal{O} \colon x\mathcal{O} \subseteq \mathbb{Z}[\xi]\} = \mathcal{O}.$$

Das heißt, die Ideale $p\mathbb{Z}$ und $\mathbb{Z} \cap F = \mathbb{Z}$ sind teilerfremd. Dies erlaubt uns Theorem 7.9 zu benutzen, um die Zerlegung von $\mathcal{O}p$ in $\mathcal{O}$ zu bestimmen. Nach genanntem Theorem zerfällt $\mathcal{O}p$ wie das Minimalpolynom ϕ_n von ξ mod p. Wir müssen also zeigen, dass

$$\overline{\phi_n} = (\overline{p_1} \ldots \overline{p_r})^{\varphi(p^{\nu_p})}$$

gilt, wobei $\overline{p_1}, \ldots, \overline{p_r}$ die verschiedenen irreduziblen Faktoren von $\overline{\phi_n}$ über $\mathbb{Z}/p\mathbb{Z}$ sind. Ferner müssen wir zeigen, dass diese Faktoren Grad f_p haben.

Setze $n_0 := p^{\nu_p}$. Sei $\{\varepsilon_i\}$ die Menge der primitiven m-ten Einheitswurzeln und $\{\eta_j\}$ die Menge der primitiven n_0-ten Einheitswurzeln. Dann ist durch $\{\varepsilon_i\eta_j\}$ die Menge der primitiven n-ten Einheitswurzeln gebgen, und daher gilt $\phi_n = \prod_{i,j}(1 - \varepsilon_i\eta_j)$. Wegen $x^{n_0} - 1 = (x-1)^{n_0} \bmod p$ ist $(\eta_j - 1)^{n_0} = 0 \bmod p$. Sei P ein beliebiges Primideal über p. Dann ist $(\eta_j - 1)^{n_0} \in p\mathbb{Z} \subseteq P$, also $\eta_j - 1 \in P$, da P prim ist, und somit $\eta_j = 1 \bmod P$. Es folgt

$$\phi_n = \prod_i (x - \varepsilon_i)^{\varphi(n_0)} = \phi_m^{\varphi(n_0)} \mod P.$$

Da die Koeffizienten der Kreisteilungspolynome in $\mathbb{Z}$ liegen, folgt dadurch sogar

$$\phi_n = \phi_m^{\varphi(n_0)} \mod p.$$

Nach Definition ist f_p gerade die kleinste positive ganze Zahl, für die $p^{f_p} = 1 \bmod m$ ist.

Es verbleibt dementsprechend ϕ_m zu betrachten, wobei m und p teilerfremd sind. Wir können daher nun annehmen, dass $\nu_p = 0$, $m = n$ und $n_0 = \varphi(n_0) = 1$ ist. Sei P wie

zuvor ein beliebiges Primideal über $p\mathbb{Z}$. Der Körper $\mathcal{O}/P$ ist ein Erweiterungskörper von $(\mathbb{Z}+\mathcal{O}p)/(\mathcal{O}p) \cong \mathbb{Z}/(p\mathbb{Z})$ und hat Charakteristik p. Da n von p nicht geteilt wird, hat x^n-1 nur einfache Nullstellen in $\mathcal{O}/P$. Die Abbildung

$$\mathcal{O} \to \mathcal{O}/P$$

bildet also die n-ten Einheitswurzeln in $\mathbb{Q}(\xi)$ bijektiv auf die n-ten Einheitswurzeln in $\mathcal{O}/P$ ab. Insbesondere werden primitive n-te Einheitswurzeln auf primitive n-te Einheitswurzeln abgebildet. Wir behaupten, dass gilt

$$\mathcal{O}/P \cong \mathbb{F}_{p^{f_p}}.$$

Da f_p die kleinste positive ganze Zahl ist, sodass $p^{f_p}-1$ ein Vielfaches von n ist, ist $\mathbb{F}_{p^{f_p}}$ der kleinste Erweiterungskörper von $\mathbb{F}_p$, welcher eine primitive n-te Einheitswurzel enthält. (Eine solche erzeugt eine zyklische Gruppe der Ordnung n in der Einheitengruppe des Erweiterungskörpers.) Dabei erzeugt $\overline{\xi} = \xi + P$ den Körper $\mathcal{O}/P$ über $\mathbb{F}_p$, weil ξ selbst $\mathcal{O}$ über $\mathbb{Z}$ erzeugt. Es folgt

$$\mathcal{O}/P \cong \mathbb{F}_{p^{f_p}}.$$

Die Nullstellen von $\overline{\phi_n} = \phi_n \bmod p$ sind primitive n-te Einheitswurzeln und $\overline{\phi}$ zerfällt über $\mathcal{O}/P$ in Linearfaktoren. Sei

$$\overline{\phi_n} = \overline{p_1} \dots \overline{p_r}$$

die Zerlegung von $\overline{\phi_n} \in \mathbb{F}_p[x]$ in irreduzible normierte Faktoren $\overline{p_i} \in \mathbb{F}_p[x]$. Das Polynom $\overline{\phi_n}$ hat als Teiler von x^n-1 nur einfache Nullstellen. Somit sind die $\overline{p_i}$ verschieden. Weiterhin ist jedes $\overline{p_i}$ Minimalpolynom einer primitiven n-ten Einheitswurzel. Es folgt $\operatorname{grad}(\overline{p_i}) = f_p$. □

Sei p wie zuvor eine Primzahl und P ein Primideal über p. Dann ist die Erweiterung $\mathcal{O}/P$ separabel über $\mathbb{Z}/(p\mathbb{Z})$, denn jede algebraische Erweiterung eines endlichen Körpers ist normal und separabel.

Korollar 9.6. *Sei ξ eine primitive n-te Einheitswurzel in $\overline{\mathbb{Q}}$ und p eine ungerade Primzahl. Dann gilt:*

(1) Das Ideal $p\mathbb{Z}$ ist genau dann unverzweigt in $\mathbb{Q}(\xi)$, wenn p und n teilerfremd sind.

(2) Das Ideal $p\mathbb{Z}$ ist genau dann vollständig zerlegt in $\mathbb{Q}(\xi)$, wenn $p = 1 \bmod n$ ist.

Beweis. Wir zeigen zunächst (1). Nach Definition ist $p\mathbb{Z}$ genau dann unverzweigt, wenn für den Trägheitsgrad $e = 1$ gilt, und $\mathcal{O}/P$ für jedes Primideal P über $p\mathbb{Z}$ eine separable Erweiterung über $\mathbb{Z}/(p\mathbb{Z})$ ist. Letzteres ist immer der Fall, wie wir zuvor festegestellt haben. Nach dem vorangegangenem Theorem gilt genau dann $e = 1$, wenn $\varphi(p^{\nu_p}) = 1$ ist, was äquivalent zu $\nu_p = 0$ ist. Dies ist aber genau dann der Fall, wenn p kein Teiler von n ist.

Es verbleibt (2) zu zeigen. Nach Definition ist $p\mathbb{Z}$ genau dann vollständig zerlegt, wenn $r = \varphi(n) = [\mathbb{Q}(\xi) : \mathbb{Q}]$ ist. Dies ist nach der fundamentalen Identität genau dann erfüllt, wenn $e = f = 1$ ist, was seinerseits äquivalent dazu ist, dass $\varphi(p^{\nu_p}) = 1$ ist und p Ordnung 1 in $(\mathbb{Z}/m\mathbb{Z})^*$ hat, wobei $m \in \mathbb{Z}$ mit $n = p^{\nu_p}m$. Dies ist aber genau dann der Fall, wenn $\nu_p = 0$, also $n = m$, und $p = 1 \bmod m$ ist. Zusammengefasst, ist $p\mathbb{Z}$ genau dann vollständig zerlegt, wenn $p = 1 \bmod n$ ist. □

Korollar 9.7. *Sei ξ eine primitive n-te Einheitswurzel in $\overline{\mathbb{Q}}$. Dann gilt:*

(1) Das Ideal $2\mathbb{Z}$ ist genau dann unverzweigt in $\mathbb{Q}(\xi)$, wenn 4 kein Teiler von n ist.

(2) Das Ideal $2\mathbb{Z}$ ist genau dann vollständig zerlegt in $\mathbb{Q}(\xi)$, wenn $n = 1$ oder $n = 2$ ist.

Beweis. Wir beginnen mit (1). Das Ideal $2\mathbb{Z}$ ist genau dann unverzweigt, wenn für den Trägheitsgrad $e = 1$ gilt, da die Erweiterung $\mathcal{O}/P$ über $\mathbb{Z}/(p\mathbb{Z})$ für jedes Primideal P über $p\mathbb{Z}$ separabel ist. Nach Theorem 9.5 ist $e = \varphi(2^{\nu_2})$. Also gilt genau dann $e = 1$, wenn $\nu_2 = 0$ oder $\nu_2 = 1$ ist, das heißt wenn 4 die Zahl n nicht teilt.

Es bleibt (2) zu zeigen. Das Ideal $2\mathbb{Z}$ ist genau dann vollständig zerlegt wenn r dem Grad der Erweiterung entspricht. Nach der fundamentalen Identität ist dies genau dann der Fall, wenn $e = f = 1$ ist, und nach Theorem 9.5 gilt $e = \varphi(2^{\nu_2})$ und f ist die Ordnung von 2 in $(\mathbb{Z}/m\mathbb{Z})^*$, wobei $m \in \mathbb{Z}$ mit $n = 2^{\nu_2}m$. Die Gleichung $e = 1$ ist daher genau dann erfüllt, wenn $\nu_2 = 0$ oder $\nu_2 = 1$ ist, und $f = 1$ gilt genau dann, wenn $2 = 1 \bmod m$ ist, das heißt, wenn $m = 1$ ist. Ist $\nu_2 = 0$, so gilt $m = n$, und ist $\nu_2 = 1$, so gilt $m = n/2$. Zusammengefasst ist $2\mathbb{Z}$ genau dann vollständig zerlegt, wenn entweder $n = 1$ oder $n = 2$ gilt. □

Satz 9.8. *Seien p, q ungerade Primzahlen, $q^* = (-1)^{(q-1)/2}q$ und ξ eine primitive q-te Einheitswurzel. Weiter sei $\mathcal{O}$ der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\xi)$. Dann gilt die folgende Äquivalenz:*

$$\begin{array}{c} p\mathbb{Z} \text{ ist vollständig} \\ \text{zerlegt in } \mathbb{Q}(\sqrt{q^*}) \end{array} \iff \begin{array}{c} \mathcal{O}p \text{ zerfällt in } \mathcal{O} \text{ in eine gerade} \\ \text{Anzahl von Primidealen} \end{array}$$

Beweis. Definiere

$$\tau = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a}{q}\right) \xi^a.$$

Es lässt sich zeigen, dass $\tau^2 = q^*$ ist (vergleiche [Neu99, Seite 51, 52]). Somit gilt

$$\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\xi).$$

Wir zeigen nun zunächst die Hinrichtung. Sei dazu $p\mathbb{Z}$ vollständigt zerlegt in $\mathbb{Q}(\sqrt{q^*})$. Da $\mathbb{Q}(\sqrt{q^*})$ eine Erweiterung vom Grad 2 von $\mathbb{Q}$ ist, gilt $\mathcal{O}^*p = P_1P_2$ für zwei Primideale P_1, P_2 in $\mathcal{O}^*$, wobei $\mathcal{O}^*$ den ganzen Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{q^*})$ bezeichne. Dabei ist $e = f = 1$ auf Grund der fundamentalen Identität.

Sei nun $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. Dann ist $\sigma(\mathbb{Q}(\sqrt{q^*})) = \mathbb{Q}(\sqrt{q^*})$ und die Abbildung

$$\mathrm{Gal}\left(\mathbb{Q}(\xi)/\mathbb{Q}\right) \to \mathrm{Gal}\left(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}\right), \ \sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt{q^*})}$$

ist surjektiv. Es gibt also ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ mit $\sigma(P_1) = P_2$. Sei Q_1 ein Primideal in $\mathcal{O}$ über P_1. Dann ist $\sigma(Q_1)$ ein Primideal über P_2, denn es gilt

$$P_2 = \sigma(P_1) = \sigma\left(Q_1 \cap \mathbb{Q}(\sqrt{q^*})\right) = \sigma(Q_1) \cap \sigma\left(\mathbb{Q}(\sqrt{q^*})\right) = \sigma(Q_1) \cap \mathbb{Q}(\sqrt{q^*}).$$

Also bildet σ die Primideale in $\mathcal{O}$ über P_1 bijektiv auf die Primideale in $\mathcal{O}$ über P_2 ab. Die Anzahl der Primideale in $\mathcal{O}$ über $p\mathbb{Z}$ ist daher gerade.

Es bleibt, die Rückrichtung zu zeigen. Sei $\mathcal{O}^*$ wie zuvor. Wir nehmen an, dass $\mathcal{O}p$ in $\mathcal{O}$ in eine gerade Anzahl von Primidealen zerfällt. Die fundamentale Gleichung für diese Zerlegung lautet dann $efr = n := \varphi(q)$, wobei r gerade ist. Sei P ein Primideal in $\mathcal{O}$ über $p\mathbb{Z}$. Dann ist

$$r = |G/G_P| = |G|/|G_P|,$$

also $|G_P|r = |G|$. Nach Satz 8.7 gilt außerdem

$$r = \frac{n}{ef} = \frac{[\mathbb{Q}(\xi) : \mathbb{Q}]}{[\mathbb{Q}(\xi) : T_P] \cdot [T_P : Z_P]} = [Z_P : \mathbb{Q}].$$

Es ist bekannt, das die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ zyklisch ist, und wir haben bereits bemerkt, dass $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\xi)$ gilt. Nach dem Hauptsatz der Galoistheorie ist $\mathbb{Q}(\sqrt{q^*})$ daher der Fixkörper einer Untergruppe U von $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ und es gilt

$$[\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) : U] = [\mathbb{Q}(\sqrt{q^*}) : \mathbb{Q}] = 2.$$

Entsprechend ist Z_P der Fixkörper einer Untergruppe U' von $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, deren Index wegen $[Z_P : \mathbb{Q}] = r$ gerade ist. Es folgt $U' \subseteq U$ und damit

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{q^*}) \subseteq Z_P \subseteq \mathbb{Q}(\xi).$$

Dies impliziert

$$\mathbb{Z}/(p\mathbb{Z}) \subseteq \left(\mathcal{O} \cap \mathbb{Q}(\sqrt{q^*})\right) / \left(P \cap \mathbb{Q}(\sqrt{q^*})\right) \subseteq \mathcal{O}_Z/P_Z \subseteq \mathcal{O}/P.$$

Nach Satz 8.5, Teil (3), sind der Verzweigungsindex und der Trägheitsgrad von P_Z über $p\mathbb{Z}$ beide 1. Es folgt, dass auch $P \cap \mathbb{Q}(\sqrt{q^*})$ Verzweigungsindex und Trägheitsgrad 1 über $p\mathbb{Z}$ hat. Somit zerfällt $p\mathbb{Z}$ vollständig in $\mathbb{Q}(\sqrt{q^*})$. □

Wir werden nun zeigen, dass in der Situation des vorangegangenen Satzes gilt

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

Daraus folgt dann das Reziprozitätsgesetz, das heißt Theorem 7.14.

Seien p, q, $q*$ und ξ wie zuvor, und $\mathcal{O}$ wieder der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\xi)$. Dann sind wir mit $d = q^*$ genau in der Situation von Satz 7.13, das heißt es gilt:

$$\left(\frac{q^*}{p}\right) = 1 \quad \Longleftrightarrow \quad \begin{array}{c} p\mathbb{Z} \text{ ist vollständig} \\ \text{zerlegt in } \mathbb{Q}(\sqrt{q^*}) \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} \mathcal{O}p \text{ zerfällt in } \mathcal{O} \text{ in eine gerade} \\ \text{Anzahl von Primidealen} \end{array}$$

Nach Theorem 9.5 ist die Anzahl der Primideale in der Faktorisierung von $\mathcal{O}p$ in $\mathcal{O}$ gegeben durch

$$r = \frac{\varphi(q)}{\varphi(1)f} = \frac{q-1}{f},$$

wobei f die Ordnung von p in $(\mathbb{Z}/q\mathbb{Z})^*$ ist, das heißt die kleinste positive ganze Zahl mit $p^f = 1 \bmod q$. Damit ergibt sich leicht die folgende Äquivalenz:

$$r \text{ gerade} \quad \Longleftrightarrow \quad f \,\Big|\, \frac{q-1}{2} \quad \Longleftrightarrow \quad p^{(q-1)/2} = 1 \bmod q \quad \Longleftrightarrow \quad \left(\frac{p}{q}\right) = 1$$

Die letzte Äquivalenz folgt hierbei aus $a^{(q-1)/2} = \left(\frac{a}{q}\right) \bmod q$ (vergleiche Seite 60). Fassen wir diese beiden Äquivalenzen nun zusammen, so erhalten wir

$$\left(\frac{q^*}{p}\right) = 1 \quad \Longleftrightarrow \quad \left(\frac{p}{q}\right) = 1,$$

und damit $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$.

10 Fermats letzter Satz

Fermat vermutete 1637, dass die Gleichung

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

für $n \in \mathbb{Z}$, $n \geq 3$ keine nicht-triviale ganzzahlige Lösung besitzt. Dabei reicht es, die Vermutung für $n = 4$ und ungerade Primzahlen zu beweisen, da in jedem anderen Fall ein entsprechender Exponent ausgeklammert werden kann. Fermat selbst bewies die Vermutung für $n = 4$ im Jahr 1637 mit Hilfe der Abstiegsmethode. Daraufhin folgten Beweise für spezielle Exponenten. Im Jahr 1850 gelang es Kummer, die Vermutung für alle regulären Primzahlen zu beweisen. Allgemein wurde die Vermutung 1995 durch Wiles bewiesen.

In diesem Kapitel werden wir zunächst das folgende Theorem zeigen:

Theorem 10.1. *Sei p eine ungerade Primzahl und ξ eine primitive p-te Einheitswurzel in $\overline{\mathbb{Q}}$. Teilt p nicht die Klassenzahl von $\mathbb{Q}(\xi)$, so besitzt die Gleichung*

$$x^p + y^p = z^p$$

keine nicht-triviale ganzzahlige Lösung mit $\mathrm{ggT}(xyz, p) = 1$.

Sei p eine ungerade Primzahl und ξ eine primitive p-te Einheitswurzel. Dann ist

$$X^p - 1 = \prod_{i=0}^{p-1} (X - \xi^i)$$

und mit $X = \frac{x}{-y}$ folgt

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \xi^i y). \tag{10.1}$$

Satz 10.2. *Seien $x, y, z \in \mathbb{Z}$ paarweise teilerfremd mit $x^p + y^p = z^p$ und* $\mathrm{ggT}(xyz, p) = 1$. *Dann sind die Ideale $(x + \xi^i y)$ paarweise teilerfremd in $\mathbb{Z}[\xi]$ für $i = 0, \ldots, p-1$.*

Beweis. Sei P ein Primideal in $\mathbb{Z}[\xi]$, welches die Ideale $(x + \xi^i y)$ und $(x + \xi^j y)$ teilt, wobei $i \neq j$. Dann sind die Elemente $x + \xi^i y$ und $x + \xi^j y$ in P enthalten, und es gilt

$$(1 - \xi^{j-i})y = \xi^{-i} \left[(x + \xi^i y) - (x + \xi^j y) \right] \in P.$$

Da P prim ist, folgt $1 - \xi^{j-i} \in P$ oder $y \in P$. Ersteres impliziert, dass auch $1 - \xi$ in P liegt, denn es gilt $(1 - \xi) = (1 - \xi^{j-i})$. Im vorangegangenen Kapitel haben wir aber

gesehen, dass $(1-\xi)$ ein Primideal in $\mathbb{Z}[\xi]$ ist. Somit gilt $(1-\xi) = P$ oder $(y) \subseteq P$. Weiterhin gilt wegen

$$(1-\xi^{i-j})x = (x+\xi^i y) - \xi^{i-j}(x+\xi^j y) \in P,$$

dass $(1-\xi) = P$ oder $(x) \subseteq P$ ist.

Angenommen $P \neq (1-\xi)$. Dann teilt P die Ideale (x) und (y). Dies ist aber ein Widerspruch, denn wegen $\mathrm{ggT}(x,y) = 1$ sind auch die Ideale (x) und (y) teilerfremd. Also ist $P = (1-\xi)$, das heißt $1 = \xi \mod P$, und damit

$$x + y = x + \xi^i y = 0 \mod P.$$

Weiter ist $(1-\xi)$ nach Satz 9.3 ein Primideal über $p\mathbb{Z}$, das heißt es gilt $P \cap \mathbb{Z} = p\mathbb{Z}$. Da x und y ganze Zahlen sind, folgt somit

$$x + y = 0 \mod p.$$

In $\mathbb{Z}/(p\mathbb{Z})$ ist aber $a^p = a$ für alle a. Daher gilt

$$z = z^p = x^p + y^p = x + y = 0 \mod p.$$

Dies widerspricht $\mathrm{ggT}(xyz, p) = 1$. Also gibt es kein solches Ideal P, welches $(x+\xi^i y)$ und $(x+\xi^j y)$ teilt. □

Wir erinnern kurz an Satz 6.1: Die Gruppe der Einheitswurzeln eines algebraischen Zahlkörpers K ist gegeben durch

$$\mu(K) = \{x \in K : x^m = 1 \text{ für ein } m \in \mathbb{N}\}.$$

Dies definiert eine endliche Untergruppe von $\mathcal{O}_K^*$.

Satz 10.3. *Sei p eine ungerade Primzahl und ξ eine primitive p-te Einheitswurzel. Dann gilt*

$$\mu(\mathbb{Q}(\xi)) = \{\pm\xi^j : j = 0, \ldots, p-1\}.$$

Beweis. Offensichtlich sind die Elemente $\pm\xi^j$ Einheitswurzeln in $\mathbb{Q}(\xi)$. Weiter ist die Gruppe $\mu(\mathbb{Q}(\xi))$ endlich und daher auch zyklisch. Sei $|\mu(\mathbb{Q}(\xi))| = m$ und η ein Erzeuger der Gruppe. Dann ist η eine primitive m-te Einheitswurzel. Wegen $(-1)^2 = 1$ ist $-\xi$ ein Element von $\mu(\mathbb{Q}(\xi))$, das heißt

$$\{\pm\xi^j : j = 0, \ldots, p-1\}$$

ist eine Untergruppe der Ordnung $2p$ von $\mu(\mathbb{Q}(\xi))$. Insbesondere teilt $2p$ somit die Gruppenordnung m. Schreibe $m = p^\nu 2k$ mit $\nu \in \mathbb{N}$ und p, k teilerfremd. Nach Definition ist $\mu(\mathbb{Q}(\xi)) \subseteq \mathbb{Q}(\xi)$. Also gilt $\eta \in \mathbb{Q}(\xi)$ und es folgt $\mathbb{Q} \subseteq \mathbb{Q}(\eta) \subseteq \mathbb{Q}(\xi)$. Dies impliziert

$$p^{\nu-1}(p-1)\varphi(2k) = \varphi(p^\nu)\varphi(2k) = \varphi(m) = [\mathbb{Q}(\eta) : \mathbb{Q}] \leq [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(p) = p-1.$$

Also ist $p^{\nu-1}\varphi(2k) = 1$ und somit $\nu = 1$ und $k = 1$, das heißt $m = 2p$. Es folgt die Behauptung. □

Satz 10.4. *Sei p eine ungerade Primzahl, ξ eine primitive p-te Einheitswurzel und ε eine Einheit in $\mathbb{Z}[\xi]$. Dann ist*

$$\varepsilon = \eta\xi^r$$

für ein $r \in \mathbb{Z}$ und eine reelle Einheit η in $\mathbb{Z}[\xi]$.

Beweis. Wegen $\varepsilon \in \mathbb{Z}[\xi]$ ist

$$\varepsilon = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}$$

für geeignete $a_i \in \mathbb{Z}$ (vergleiche Theorem 9.4). Dann sind

$$\overline{\varepsilon} = a_0 + a_1\xi^{-1} + \ldots + a_{p-2}\xi^{-p+2}$$

und $\varepsilon/\overline{\varepsilon}$ ebenfalls Einheiten in $\mathbb{Z}[\xi]$.

Die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ ist zyklisch und enthält die komplexe Konjugation σ auf $\mathbb{Q}(\xi)$ als ein Element. Für $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ gilt

$$|\tau(\varepsilon/\overline{\varepsilon})| = \left|\tau(\varepsilon)/\tau(\sigma(\varepsilon))\right| = \left|\tau(\varepsilon)/\sigma(\tau(\varepsilon))\right| = \left|\tau(\varepsilon)\Big/\overline{\tau(\varepsilon)}\right| = 1.$$

Somit liegt $\varepsilon/\overline{\varepsilon}$ im Kern der Abbildung λ in der Sequenz

$$1 \longrightarrow \mu(\mathbb{Q}(\xi)) \longrightarrow \mathbb{Z}[\xi]^* \xrightarrow{\lambda} \Gamma \longrightarrow 0.$$

Nach Satz 6.2 ist diese Sequenz exakt, das heißt es gilt $\ker(\lambda) = \mu(\mathbb{Q}(\xi))$. Nach Satz 10.3 ist daher $\varepsilon/\overline{\varepsilon} = \pm\xi^a$. Angenommen $\varepsilon/\overline{\varepsilon} = -\xi^a$. Dann ist

$$\varepsilon = a_0 + a_1 + \ldots + a_{p-2} = \overline{\varepsilon} \mod (1-\xi).$$

Andererseits ist $\varepsilon = -\varepsilon^a\overline{\varepsilon}$, sodass $\varepsilon = -\overline{\varepsilon} \mod (1-\xi)$ gilt. Also ist

$$2\varepsilon = \overline{\varepsilon} - \overline{\varepsilon} = 0 \mod (1-\xi)$$

und damit $2\varepsilon \in (1-\xi)$, das heißt $(2) = (2\varepsilon) \subseteq (1-\xi)$, da ε eine Einheit ist. Es folgt $2 \in (1-\xi)$ und somit $2 \in (1-\xi) \cap \mathbb{Z} = p\mathbb{Z}$. Dies ist ein Widerspruch. Also war die Annahme falsch und es gilt $\varepsilon/\overline{\varepsilon} = \xi^a$. Es lässt sich leicht einsehen, dass es ein $r \in \mathbb{Z}$ gibt, sodass $a = 2r \bmod p$ ist. Damit ist $\varepsilon = \overline{\varepsilon}\xi^{2r}$ und

$$\xi^{-r}\varepsilon = \overline{\varepsilon}\xi^r = \overline{\varepsilon\xi^{-r}}.$$

Mit $\eta := \varepsilon\xi^{-r}$ erhalten wir daher die Behauptung. □

Beweis von Theorem 10.1. Wir beweisen die Behauptung zunächst für $p = 3$. Sei $x \in \mathbb{Z}$ mit $x \neq 0 \bmod 3$. Dann ist $x^3 = \pm 1 \bmod 9$. Seien nun x, y, z ganze Zahlen mit $\mathrm{ggT}(xyz, 3) = 1$. Dann ist

$$x^3 + y^3 = -2,\ 0 \text{ oder } 2 \mod 9$$

und $z^3 = \pm 1 \bmod 9$. Insbesondere ist $x^3 + y^3 \neq z^3$, was die Behauptung für $p = 3$ zeigt.

Sei nun p eine Primzahl mit $p \geq 5$ für den Rest des Beweises. Seien weiter x, y, z ganze Zahlen mit $\mathrm{ggT}(xyz, p) = 1$ und

$$x^p + y^p = z^p.$$

Wir können ohne Beschränkung der Allgemeinheit annehmen, dass x, y, z paarweise teilerfremd sind, denn besitzten x, y, z einen gemeinsamen Teiler, so lässt sich dieser in der Gleichung kürzen, und besitzen zwei der drei Zahlen einen gemeinsamen Teiler, so ist dies auch ein Teiler der dritten Zahl, wie sich leicht nachrechnen läasst.

Sei nun ξ eine primitive p-te Einheitswurzel. Dann gilt nach Gleichung (10.1) auf Seite 78, dass

$$z^p = x^p + y^p = \prod_{i=0}^{p-1}(x + \xi^i y).$$

Im Sinne von Idealen in $\mathbb{Z}[\xi]$ heißt das

$$\prod_{i=0}^{p-1}(x + \xi^i y) = (z)^p.$$

Da nach Satz 10.2 die Ideale $(x + \xi^i y)$ paarweise teilerfremd sind, gilt

$$(x + \xi^i y) = A_i^p$$

für ein Ideal A_i, welches ein Teiler von (z) ist. Das Ideal A_i^p ist dann nach Konstruktion ein Hauptideal, das heißt es gilt $A_i^p = 1$ in der Idealklassengruppe $\mathrm{CL}_K = \mathcal{J}_K/\mathcal{P}_K$. Da aber p nach Annahme nicht die Klassenzahl $|\mathrm{CL}_K|$ teilt, muss A_i selbst bereits trivial in CL_K sein. Also ist A_i ein Hauptideal.

Sei $A_i = (\alpha_i)$ mit $\alpha_i \in \mathbb{Z}[\xi]$. Dann ist $(x + \xi^i y) = (\alpha_i)^p = (\alpha_i^p)$, sodass $x + \xi^i y = \varepsilon_i \alpha_i^p$ für eine Einheit $\varepsilon_i \in \mathbb{Z}[\xi]$ gilt. Nach Satz 10.4 gibt es $r_i \in \mathbb{Z}$ und eine Einheit $\eta_i \in \mathbb{R}$ mit $\varepsilon_i = \eta_i \xi^{r_i}$. Wir beschränken uns nun auf den Fall $i = 1$ und vernachlässigen der Übersicht halber den Index i. Es gilt also

$$x + \xi y = \eta \xi^r \alpha^p.$$

Sei

$$\alpha = b_0 + b_1\xi + \ldots + b_{p-2}\xi^{p-2}$$

für geeignete $b_i \in \mathbb{Z}$. Dann ist

$$\alpha^p = b_0^p + (b_1\xi)^p + \ldots + (b_{p-2}\xi^{p-2})^p = b_0^p + b_1^p + \ldots + b_{p-2}^p = a \mod p\mathbb{Z}[\xi]$$

für ein geeignetes $a \in \mathbb{Z}$. Es folgt

$$x + \xi y = \eta \xi^r \alpha^p = \eta \xi^r a \mod p\mathbb{Z}[\xi] \quad \text{und} \quad x + \xi^{-1} y = \overline{x + \xi y} = \eta \xi^{-r} a \mod p\mathbb{Z}[\xi],$$

sodass

$$x + \xi y - \xi^{2r} x - \xi^{2r-1} y = (x + \xi y) - \xi^{2r}(x + \xi^{-1} y) = 0 \mod p\mathbb{Z}[\xi]. \tag{10.2}$$

Wir nehmen nun an, dass die Elemente $1, \xi, \xi^{2r}, \xi^{2r-1}$ paarweise verschieden sind. Dann ist $\{1, \xi, \xi^{2r}, \xi^{2r-1}\}$ Teil einer Basis von $\mathbb{Z}[\xi]$. (Hier ist wichtig, dass $p \geq 5$ gilt, und dass wegen $1 + \xi + \ldots + \xi^{p-1} = 0$ jede $(p-1)$-elementige Teilmenge von $\{1, \xi, \ldots, \xi^{p-1}\}$ eine Basis von $\mathbb{Z}[\xi]$ ist.) Nach Gleichung (10.2) ist

$$x + \xi y - \xi^{2r} x - \xi^{2r-1} y = pt$$

für ein $t \in \mathbb{Z}[\xi]$. Schreibt man t bezüglich dieser Basis, so folgt, dass p die ganzen Zahlen x und y teilt, was $\mathrm{ggT}(xyz, p) = 1$ widerspricht. Also können die Elemente $1, \xi, \xi^{2r}, \xi^{2r-1}$ nicht paarweise verschieden sein.

Wir unterscheiden nun drei Fälle, nämlich erstens $\xi^{2r} = 1$, zweitens $\xi^{2r} = \xi$ und somit auch $\xi^{2r-1} = 1$, und drittens $\xi^{2r-1} = \xi$. Es lässt sich leicht einsehen, dass wegen $\xi \neq 1$ einer dieser Fälle eintreten muss.

(1) Sei $\xi^{2r} = 1$. Dann folgt mit Gleichung (10.2), dass gilt

$$\xi y - \xi^{-1} y = x + \xi y - x - \xi^{2r-1} y = 0 \mod p\mathbb{Z}[\xi].$$

Dies impliziert $y - \xi^{-2} y = 0 \mod p\mathbb{Z}[\xi]$. Da sich $\{1, \xi^{-2}\}$ wieder zu einer Basis von $\mathbb{Z}[\xi]$ vervollständigen lässt, folgt wie zuvor, dass p ein Teiler von y ist. Dies widerspricht der Teilerfremdheit von y und p.

(2) Sei $\xi^{2r} = \xi$ und daher auch $\xi^{2r-1} = 1$. Dann ergibt Gleichung (10.2)

$$(x - y) - \xi(x - y) = x + \xi y - \xi x - y = 0 \mod p\mathbb{Z}[\xi].$$

Also teilt p die Differenz $x - y$.

(3) Sei $\xi^{2r-1} = \xi$. Dann ist nach Gleichung (10.2)

$$x - \xi^2 x = x + \xi y - \xi^2 x - \xi y = 0 \mod p\mathbb{Z}[\xi].$$

Wir in (1) folgt, dass p ein Teiler von x ist, was deren Teilerfremdheit widerspricht.

Somit tritt Fall (2) ein, das heißt $\xi^{2r-1} = 1$ und p teilt $x - y$. Wir haben also gezeigt, dass für paarweise teilerfremde ganze Zahlen x, y, z mit $\mathrm{ggT}(xyz, p) = 1$ und $x^p + y^p = z^p$ folgt, dass $x = y \mod p$ ist.

Wir betrachten nun die Gleichung

$$x^p + (-z)^p = (-y)^p,$$

welche sich wegen $(-1)^p = -1$ ergibt. Offensichtlich sind die drei ganzen Zahlen wieder paarweise teilerfremd und jeweils teilerfremd zu p. Es folgt daher, dass auch $x = -z \mod p$ ist. Weiterhin ist $a^p = a \mod p$ für beliebige ganze Zahlen a und damit

$$x + y = x^p + y^p = z^p = z \mod p.$$

Es folgt

$$0 = z - (x + y) = z - (x + x) = z - (-z - z) = 3z \mod p.$$

Also ist p ein Teiler von $3z$, und da $p \geq 5$ gilt, teilt p somit z selbst. Dies widerspricht aber der Annahme $\mathrm{ggT}(xyz, p) = 1$. Das Theorem ist damit bewiesen. □

Sei p eine ungerade Primzahl in $\mathbb{Z}$. Wir nennen p **regulär**, wenn p die Klassenzahl $h_{\mathbb{Q}(\xi)}$ nicht teilt, wobei ξ eine beliebige primitive p-te Einheitswurzel ist.

Im Folgenden werden wir die Fermatsche Vermutung nun noch für beliebige reguläre Primzahlen beweisen. Dazu benötigen wir zunächst die folgenden beiden Lemma, von welchen wir nur das Erste beweisen.

Lemma 10.5. *Sei p eine ungerade Primzahl und ξ eine primitive p-te Einheitswurzel. Dann gilt*

$$\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(1+\xi) = 1 \quad \textit{und} \quad \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(1-\xi) = p.$$

Beweis. Seien $\tau_1, \ldots, \tau_{p-1}$ die verschiedenen $\mathbb{Q}$-Homomorphismen $\mathbb{Q}(\xi) \to \overline{\mathbb{Q}}$. Dann ist bis auf Umnummerierung $\tau_i(1+\xi) = 1+\xi^i$. Es folgt

$$\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(1+\xi) = \prod_{i=1}^{p-1} \tau_i(1+\xi) = \prod_{i=1}^{p-1}(1+\xi^i) = (-1)^{p-1}\prod_{i=1}^{p-1}(-1-\xi^i) = \phi_p(-1) = 1.$$

Die zweite Identität ergibt sich analog. □

Lemma 10.6 (Kummersches Lemma)**.** *Sei p eine reguläre Primzahl, ξ eine primitive p-te Einheitswurzel und $\mathcal{O}$ der Ring der ganzen Zahlen in $\mathbb{Q}(\xi)$. Weiter sei $\varepsilon \in \mathcal{O}^*$ mit*

$$\varepsilon = a \mod \mathcal{O}p$$

für ein $a \in \mathbb{Z}$. Dann gibt es ein $\eta \in \mathcal{O}^*$ mit

$$\varepsilon = \eta^p.$$

Der Beweis dieses Lemmas ist deutlich aufwendiger als sich zunächst vermuten lässt. Wir verweisen auf [BS66]. Das Lemma ist dort als Theorem 3 in Kapitel 5, Abschnitt 6.4 auf Seite 377 gegeben.

Theorem 10.7 (Kummer)**.** *Sei p eine reguläre Primzahl. Dann hat die Gleichung*

$$x^p + y^p = z^p$$

keine nicht-triviale Lösung in $\mathbb{Z}$.

Beweis. Angenommen es gibt eine nicht-triviale Lösung der Gleichung in $\mathbb{Z}$, das heißt $x, y, z \in \mathbb{Z}$ mit

$$x^p + y^p = z^p.$$

Wir können wieder ohne Einschränkung der Allgemeinheit annehmen, dass x, y, z paarweise teilerfremd sind. Nach Theorem 10.1 wissen wir bereits, dass es keine solche Lösung geben kann, wenn $\mathrm{ggT}(xyz, p) = 1$ ist. Das heißt p teilt eine der drei Zahlen x, y, z. Wegen $(-1)^p = -1$ können wir die Gleichung beliebig umstellen, und daher ohne Beschränkung der Allgemeinheit annehmen, dass p ein Teiler von z und $\mathrm{ggT}(xy, p) = 1$ ist. Das heißt, es ist $z = p^k z_0$ mit $k \in \mathbb{N}$ und $\mathrm{ggT}(z_0, p) = 1$. Insbesondere ist $\mathrm{ggT}(xyz_0, p) = 1$.

Sei ξ eine primitive p-te Einheitswurzel und $\mathcal{O} = \mathbb{Z}[\xi]$ der Ring der ganzen Zahlen in $\mathbb{Q}(\xi)$. Nach Satz 9.3 gilt

$$(p) = \mathcal{O}p = (1-\xi)^{p-1} = \big((1-\xi)^{p-1}\big)$$

als Ideale in $\mathcal{O}$. Es folgt $p = \varepsilon(1-\xi)^{p-1}$ für ein $\varepsilon \in \mathcal{O}^*$ und daher

$$x^p + y^p = \varepsilon^{pk}(1-\xi)^{pm} z_0^p$$

mit $m := k(p-1) > 0$. Wir werden im Folgenden zeigen, dass die Gleichung

$$x^p + y^p = \varepsilon(1-\xi)^{pm} z^p \tag{10.3}$$

keine Lösung $x, y, z \in \mathcal{O}$ mit (xyz), $(1-\xi)$ teilerfremd in $\mathcal{O}$, $\varepsilon \in \mathcal{O}^*$, und $m \in \mathbb{N}$ besitzt.

Wir nehmen an es gibt eine solche Lösung. Dann können wir ohne Beschränkung der Allgemeinheit annehmen, dass x, y, z teilerfremd sind und m minimal ist. Setze $P := (1-\xi)$ und $A := (z)$. Nach Satz 9.3 ist P prim. Aus (10.1) und (10.3) folgt nun

$$\prod_{k=0}^{p-1}(x + \xi^k y) = (x^p + y^p) = P^{pm} A^p. \tag{10.4}$$

Nach Annahme sind P und A teilerfremd als Ideale in $\mathcal{O}$. Weiter gibt es ein i, sodass P ein Teiler von $(x + \xi^i y)$ ist. Wegen $(1-\xi^j) = 0 \mod P$ für alle j folgt für alle k, dass

$$(x + \xi^k y) = (x + \xi^i y) - (\xi^i)(1-\xi^{k-i})y = 0 \mod P.$$

Das heißt P teilt jedes $(x + \xi^k y)$. Man bemerke, dass dies nicht Satz 10.2 widerspricht, da nicht $x^p + y^p = z^p$ gilt.

Als nächstes werden wir nun zeigen, dass für $i \neq j$ gilt

$$\frac{x + \xi^i y}{1-\xi} \neq \frac{x + \xi^j y}{1-\xi} \mod P. \tag{10.5}$$

Angenommen es gäbe i, j, sodass in (10.5) Gleichheit gilt. Dann ist

$$\xi^i(1-\xi^{j-i})y = (x + \xi^i y) - (x + \xi^j y) = 0 \mod P^2$$

und mit $(1-\xi^{j-i}) = P$ folgt $\xi^i y = 0 \mod P$. Da ξ^i eine Einheit ist, ergibt sich somit $y = 0 \mod P$. Dies widerspricht der Annahme, dass die Ideale (xyz) und P teilerfremd sind. Also gilt für $i \neq j$ die Ungleichung in (10.5).

Weiter gilt nach Lemma 10.5, dass

$$|\mathcal{O}/P| = \mathfrak{N}(P) = \mathfrak{N}((1-\xi)) = \big|\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(1-\xi)\big| = p.$$

Die p voneinander verschiedenen Quotienten $(x + \xi^i y)/(1-\xi)$ bilden daher bereits ein vollständiges Restklassensystem modulo P. Das heißt, es gibt genau ein k, sodass gilt

$$\frac{x + \xi^k y}{1-\xi} \in P.$$

Also teilt P^2 genau einen Repräsentanten $(x+\xi^k y)$. Da wir $\xi^k y$ durch y ersetzen können, können wir annehmen, dass $k = 0$ ist, und damit P^2 ein Teiler von $(x + y)$ ist. Weiter haben wir gesehen, dass P alle Ideale $(x + \xi^i y)$ teilt, aber P^2 keines der Ideale $(x + \xi^i y)$ für $i \neq 0$. Die linke Seite von Gleichung (10.4) ist daher durch $P^2 P^{p-1} = P^{p+1}$ teilbar. Damit folgt nun einerseits, dass $m > 1$ gelten muss, und andererseits, dass $(x + y)$ sogar von $P^{pm-(p-1)}$ geteilt wird, da die anderen Faktoren nur P selbst als Teiler enthalten, aber nicht P^2.

Sei nun M der größte gemeinsame Teiler der Ideale (x) und (y). Dann ist P kein Teiler von M, da (x) und P bzw. (y) und P nach Annahme teilerfremd sind. Es folgt

$$P^{pm-(p-1)} M \,\Big|\, (x + y) \quad \text{und} \quad PM \,\Big|\, (x + \xi^i y) \text{ für } i = 1, \ldots, p - 1.$$

Wir wählen Ideale $C_0, \ldots, C_{p-1}$ in $\mathcal{O}$, sodass gilt

$$(x + y) = P^{pm-(p-1)} M C_0 \quad \text{und} \quad (x + \xi^i y) = PMC_i \text{ für } i = 1, \ldots, p - 1.$$

Wir behaupten, dass die so gewählten Ideale paarweise teilerfremd sind. Um dies einzusehen nehmen wir an, dass es $i \neq j$ und ein Primideal Q in $\mathcal{O}$ gibt, welches C_i und C_j teilt. Dann werden $(x + \xi^i y)$ und $(x + \xi^j y)$ von PMQ geteilt. Wie zuvor folgt wegen

$$\xi^i (1 - \xi^{j-i}) y = (x + \xi^i y) - (x + \xi^j y) = 0 \mod PMQ,$$

und weil $(1 - \xi^{j-i}) = P$ und ξ^i eine Einheit ist, dass MQ ein Teiler von (y) ist. Analog lässt sich folgern, dass MQ auch (x) teilt. Dies widerspricht aber der Definition von M. Somit haben wir gezeigt, dass die Ideale $C_0, \ldots, C_{p-1}$ teilerfremd sind.

Gleichung (10.4) können wir jetzt schreiben als

$$P^{pm} A^p = (P^{pm-(p-1)} M C_0)(PMC_1) \ldots (PMC_{p-1}) = P^{pm} M^p C_0 \ldots C^{p-1}.$$

Da die C_i paarweise teilerfremd sind, gibt es zu jedem i einen Teiler A_i von A, sodass $C_i = A_i^p$. Dementsprechend gilt dann

$$(x + y) = P^{pm-(p-1)} M A_0^p \quad \text{und} \quad (x + \xi^i y) = PMA_i^p \text{ für } i = 1, \ldots, p - 1.$$

Wir erinnern daran, dass die gebrochenen Ideale in $\mathbb{Q}(\xi)$ eine Gruppe bezüglich der Multiplikation bilden, das heißt wir können Ideale invertieren. Daher gilt einerseits

$$(x + \xi^i y) P^{p(m-1)} = (x + y)(A_i A_0^{-1})^p, \tag{10.6}$$

und wegen $P = (1 - \xi)$ andererseits

$$(x + \xi^i y) \left(\frac{(1 - \xi)^{p(m-1)}}{x + y} \right) = (A_i A_0^{-1})^p.$$

Aus letzterem folgt, dass $(A_i A_0^{-1})^p$ ein gebrochenes Hauptideal in $\mathbb{Q}(\xi)$ ist. Da p als reguläre Primzahl die Klassenzahl $h_{\mathbb{Q}(\xi)}$ nicht teilt, folgt, dass auch $A_i A_0^{-1}$ selbst ein gebrochenes Hauptideal ist. Sei

$$A_i A_0^{-1} = \left(\frac{\alpha_i}{\beta_i} \right)$$

für geeignete $\alpha_i, \beta_i \in \mathcal{O}$. (Diese existieren nach Satz 2.10.) Da P und A teilerfremd sind, teilt P keines der Ideale A_i, denn diese sind selbst Teiler von A. Somit können wir α_i und β_i so wählen, dass P weder (α_i) noch (β_i) teilt.

Aus Gleichung (10.6) folgt nun

$$(x + \xi^i y)(1 - \xi)^{p(m-1)} = (x + y) \left(\frac{\alpha_i}{\beta_i}\right)^p \varepsilon_i \tag{10.7}$$

für ein $\varepsilon_i \in \mathcal{O}^*$. Dabei verstehen wir die Gleichung nun wieder im Sinne von Elementen in $\mathcal{O}$ und nicht als Gleichheit von Idealen. Bemerke, dass

$$(x + \xi y)(1 + \xi) - (x + \xi^2 y) = \xi(x + y).$$

Multipikation mit $(1 - \xi)^{p(m-1)}$ liefert

$$(x + \xi y)(1 + \xi)(1 - \xi)^{p(m-1)} - (x + \xi^2 y)(1 - \xi)^{p(m-1)} = \xi(x + y)(1 - \xi)^{p(m-1)}.$$

Setzen wir in diese Gleichung nun zweimal (10.7) ein, einmal für $i = 1$ und einmal für $i = 2$, so erhalten wir

$$(x + y) \left(\frac{\alpha_1}{\beta_1}\right)^p \varepsilon_1(1 + \xi) - (x + y) \left(\frac{\alpha_2}{\beta_2}\right)^p \varepsilon_2 = \xi(x + y)(1 - \xi)^{p(m-1)}.$$

Umformen ergibt

$$(\alpha_1\beta_2)^p - \frac{\varepsilon_2}{\varepsilon_1(1 + \xi)}(\alpha_2\beta_1)^p = \frac{\xi}{\varepsilon_1(1 + \xi)}(1 - \xi)^{p(m-1)}(\beta_1\beta_2)^p.$$

Da $1 + \xi$ nach Lemma 10.5 und Satz 2.1 eine Einheit in $\mathcal{O}$ ist, erhalten wir dadurch eine Gleichung der Form

$$\alpha^p + \varepsilon_0\beta^p = \varepsilon'(1 - \xi)^{p(m-1)}\gamma^p, \tag{10.8}$$

wobei $\alpha, \beta, \gamma \in \mathcal{O}$ mit $\mathrm{ggT}(\alpha\beta\gamma, 1 - \xi) = 1$ und $\varepsilon_0, \varepsilon' \in \mathcal{O}^*$.

Schließlich möchten wir das Kummersche Lemma (Lemma 10.6) benutzen, um zu zeigen, dass es ein $\eta \in \mathcal{O}^*$ mit $\varepsilon_0 = \eta^p$ gibt. Aus $m \geq 1$ folgt zunächst $p(m - 1) \geq p$, das heißt es gilt

$$\alpha^p + \varepsilon_0\beta^p = 0 \mod P^p, \tag{10.9}$$

und (β) und P^p sind teilerfremd, das heißt es ist $(\beta) + P^p = \mathcal{O}$. Es gibt also ein $\beta' \in \mathcal{O}$ mit

$$\beta\beta' = 1 \mod P^p.$$

Multiplikation von Gleichung (10.9) mit $(\beta')^p$ liefert

$$(\alpha\beta')^p + \varepsilon_0 = 0 \mod P^p,$$

sodass

$$\varepsilon_0 = -(\alpha\beta')^p = (-\alpha\beta')^p = \omega^p \mod P^p$$

für $\omega := -\alpha\beta' \in \mathcal{O}$. Schreibe $\omega = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}$ für geeignete $a_i \in \mathbb{Z}$. Dann ist

$$\omega = a_0 + a_1 + \ldots + a_{p-2} = a \mod (1-\xi)$$

für ein $a \in \mathbb{Z}$, und daher $\omega^p = a^p \bmod p(1-\xi)$. Mit

$$P(1-\xi)\mathcal{O} = (1-\xi)^{p-1}(1-\xi) = (1-\xi)^p = P^p$$

folgt weiter $\omega^p = a^p \bmod P^p$. Also ist $\varepsilon_0 = a^p \bmod P^p$. Nach dem Kummerschen Lemma gibt es damit $\eta \in \mathcal{O}^*$, sodass $\varepsilon_0 = \eta^p$ ist.

Gleichung (10.8) lässt sich dadurch schreiben als

$$\alpha^p + (\eta\beta)^p = \varepsilon'(1-\xi)^{p(m-1)}\gamma^p.$$

Damit haben wir eine Lösung von (10.3) gefunden, welche der Minimalität des dort gewählten m's widerspricht. Dies zeigt die Behauptung des Theorems. □

Zum Abschluss bemerken wir, dass es genau drei ungerade irreguläre Primzahlen zwischen 0 und 100 gibt, nämlich 37, 59 und 67. Alle übrigen ungeraden Primzahlen zwischen 0 und 100 sind regulär. Es ist unbekannt, ob es unendlich viele reguläre Primzahlen gibt. Umgekehrt gilt aber:

Theorem 10.8. *Es gibt unendlich viele irreguläre Primzahlen.*

Für einen Beweis verweisen wir erneut auf [BS66]. Das Theorem ist dort als Theorem 2 in Kapitel 5, Abschnitt 7.2 auf Seite 381 gegeben.

Literaturverzeichnis

[BS66] Z. I. Borevich and I. R. Shafarevich. *Number Theory*. Academic Press, New York, 1966.

[Lan02] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer-Verlag, New York, 3rd edition, 2002.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, Berlin ; New York, 1999.