Zahlentheorie, WS 12/13

(Prof. Dr. O. Bogopolski)

1 Vorlesung
Endliche und algebraische Erweiterungen

Definition 1.1. Seien K, E zwei Körper

1) Der Körper E heißt *Erweiterung* des Körpers K, falls $K \subseteq E$ ist. In dem Fall kann man E als Vektorraum über K betrachten. Die Dimension dieses Vektorraums wird mit $[E : K]$ bezeichnet.

2) Die Erweiterung E heißt *endlich* über K, falls $[E : K]$ endlich ist.

3) Ein Element $\alpha \in E$ heißt *algebraisch* über K, falls ein nichtnullsches Polynom $p(x) \in K[x]$ existiert, so dass $p(\alpha) = 0$ ist. Beispiel dazu: $\alpha = 5\sqrt{2} + \sqrt{3} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$.

4) Die Erweiterung E heißt *algebraisch* über K, falls jedes Element von E algebraisch über K ist.

Satz 1.2. Sei $\alpha \in E$ algebraisch über K. Wir betrachten die Menge von Polynomen über K, die α annulieren:

$$\mathrm{Ann}_K(\alpha) = \{f(x) \in K[x] \mid f(\alpha) = 0\}.$$

Es gelten:

1) Die Menge $\mathrm{Ann}_K(\alpha)$ enthält genau ein Polynom $p(x) \neq 0$ des minimalen Grades und mit dem Hauptkoeffizient gleich 1. Dieses Polynom heißt *minimales Polynom* für α.

2) $p(x)$ ist ein Teiler jedes Polynoms $f(x)$ aus $\mathrm{Ann}_K(\alpha)$.

3) $p(x)$ ist irreduzibel über K.

Wir bezeichnen das minimale Polynom für α durch $m_\alpha(x)$.

Folgerung 1.3. Das minimale Polynom $m_\alpha(x)$ für α gleich dem Polynom $q(x) \in K[x]$ mit folgenden Eigenschaften ist:
1) $q(x)$ ist irreduzibel über K,
2) $q(\alpha) = 0$,
3) $q(x)$ ist *monisch*, d.h. der Hauptkoeffizient von $q(x)$ gleich 1 ist.

Beispiel. Das Polynom $x^4 - 10x^2 + 1$ ist das minimale Polynom für $\alpha = \sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$.

Satz 1.4. Jede endliche Erweiterung E über K ist algebraisch über K.

Wir werden sehen, dass algebraische Erweiterungen E über K existieren, die unendlich über K sind.

Satz 1.5. Seien $k \subseteq K \subseteq E$ Erweiterungen. Dann gilt $[E : k] = [E : K][K : k]$. Ist $\{u_i\}_{i \in I}$ eine Basis von K über k und ist $\{v_j\}_{j \in J}$ eine Basis von E über K, dann ist $\{u_i v_j\}_{(i,j) \in I \times J}$ eine Basis von E über k.

Definition 1.6. Sei $K \subset E$ eine Erweiterung. Für $\alpha \in E$ bezeichnen wir mit $K(\alpha)$ den kleinsten Körper in E, der K und α enthält. Es ist leicht zu sehen:

$$K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \,|\, f(x), g(x) \in K[x] \text{ und } g(\alpha) \neq 0\}.$$

Wir bezeichnen

$$K[\alpha] = \{f(\alpha) \,|\, f(x) \in K[x]\}.$$

Analog definiert man $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ und $K[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

Satz 1.7. Sei α algebraisch über K. Dann ist $K(\alpha) = K[\alpha]$. Außerdem gilt:

$$[K(\alpha) : K] = \mathrm{Grad}(m_\alpha(x)).$$

Beispiel. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ ist eine algebraische Erweiterung von $\mathbb{Q}$, die unendlich über $\mathbb{Q}$ ist. Um das zu beweisen, benutzt man die Sätze 1.5, 1.7 und 1.8.

Satz 1.8. (Eisenstein-Kriterium.) Sei $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ und sei p eine Primzahl. Nehmen wir an, dass das folgende gilt:

1) $p \nmid a_n$,

2) $p | a_i$ für $0 \leqslant i < n$,

3) $p^2 \nmid a_0$.

Dann ist $p(x)$ irreduzibel über $\mathbb{Z}$ und über $\mathbb{Q}$.

Satz 1.9. Sei $E = K(\alpha_1, \ldots, \alpha_n)$ und alle α_i algebraisch über K. Dann ist E endlich über K und folglich algebraisch über K.

2 Vorlesung Norm und Spur

Definition 2.1. Sei E eine endliche Erweiterung von K. Sei $\alpha \in K$. Wir betrachten die Abblidung

$$\varphi_\alpha : \begin{array}{l} E \to E, \\ x \to \alpha x. \end{array}$$

Diese Abbildung ist linear über K. Sei $\omega = \{\omega_1, \ldots, \omega_n\}$ eine Basis von E über K. Wir multiplizieren die Elemente von ω mit α und schreiben diese Produkte als lineare Kombinationen der Basiselementen mit Koeffizienten aus K:

$$\begin{aligned}\alpha\omega_1 &= a_{11}\omega_1 + \cdots + a_{1n}\omega_n \\ &\vdots \\ \alpha\omega_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n\end{aligned}$$

Daraus entsteht die Darstellungsmatrix der linearen Abbildung φ_α in der Basis ω :

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

Das Polynom $\chi_\alpha(x) = \det(xE_n - A)$ heißt das *charakteristische Polynom* von α.
Die Zahl $\det(A)$ heißt die *Norm* von α und wird min $N_{E/K}(\alpha)$ bezeichnet.
Die Zahl $\mathrm{Spur}(A) = a_{11} + \cdots + a_{nn}$ heißt *Spur* von α und wird mit $\mathrm{Sp}_{E/K}(\alpha)$ bezeichnet.

Bemerkung.

1) Das Polynom $\chi_\alpha(x)$ und die Zahlen $N_{E/K}(\alpha)$, $\mathrm{Sp}_{E/K}(\alpha)$ hängen nicht von der Wahl der Basis ω ab.
2) $\chi_\alpha(\mathbf{x}) = \mathbf{x}^n - \mathrm{Sp}_{E/K}(\alpha)\mathbf{x}^{n-1} + \cdots + (-1)^n N_{E/K}(\alpha)$.

Beispiel. Betrachten $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dann ist $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine Basis von E über $\mathbb{Q}$. Es gelten:

1) $N_{E/\mathbb{Q}}(\sqrt{6}) = 36$,
2) $\mathrm{Sp}_{E/\mathbb{Q}}(\sqrt{6}) = 0$,
3) $\chi_{\sqrt{6}}(x) = (x^2 - 6)^2$,
4) $m_{\sqrt{6}}(x) = x^2 - 6$.

Satz 2.2. Seien E^* und K^* die multiplikative Gruppen des Körpers E und K entsprechend und sei $n = [E : K]$ endlich. Dann gilt:

1) $N_{E/K} : E^* \to K^*$ ist ein Homomorphismus.
2) $\mathrm{Sp}_{E/K} : E \to K$ ist eine K-lineare Abbildung.
3) $N_{E/K}(k\alpha) = k^n \cdot N_{E/K}(\alpha)$ für alle $k \in K$.
4) $\mathrm{Sp}_{E/K}(k\alpha) = k \cdot \mathrm{Sp}_{E/K}(\alpha)$ für alle $k \in K$.

Satz 2.3. Seien $L \subseteq K \subseteq E$ endliche Körpererweiterungen. Dann gelten:

$$N_{E/L} = N_{K/L} \circ N_{E/K},$$

$$\mathrm{Sp}_{E/L} = \mathrm{Sp}_{K/L} \circ \mathrm{Sp}_{E/K},$$

Satz 2.4. Sei $K \subseteq E$ eine endlich Körpererweiterung und sei $\alpha \in E$. Dann ist das charakteristische Polynim von α eine Potenz des minimalen Polynoms von α:

$$\chi_\alpha(x) = (m_\alpha(x))^k.$$

Definition 2.5. Sei $K \subseteq E$ eine Körpererweiterung mit $[E : K] = n < \infty$. Sei $(\alpha_1, \ldots, \alpha_n)$ ein Tupel von Elementen von E. Die folgende Zahl aus K heißt *Diskriminante* dieses Tupels:

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \mathrm{Sp}(\alpha_1\alpha_1) & \ldots & \mathrm{Sp}(\alpha_1\alpha_n) \\ \vdots & & \vdots \\ \mathrm{Sp}(\alpha_n\alpha_1) & \ldots & \mathrm{Sp}(\alpha_n\alpha_n) \end{pmatrix}.$$

Satz 2.6. Sei $K \subseteq E$ eine Körpererweiterung mit $[E : K] = n < \infty$. Sei $(\alpha_1, \ldots, \alpha_n)$ ein Tupel von Elementen von E. Dann gelten:
1) Wenn $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ ist, dann ist $(\alpha_1, \ldots, \alpha_n)$ eine Basis von E über K.
2) Wenn $\mathrm{char}(L) = 0$ ist und $(\alpha_1, \ldots, \alpha_n)$ eine Basis von E über K, dann ist $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

Satz 2.7. Seien $(\alpha_1, \ldots, \alpha_n)$ und $(\beta_1, \ldots, \beta_n)$ zwei Basen von E über K. Sei $\alpha_i = \sum_{j=1}^n c_{ij}\beta_j$, wobei $c_{ij} \in K$ ist. Dann gilt $\Delta(\alpha_1, \ldots, \alpha_n) = (\det(c_{ij}))^2 \Delta(\beta_1, \ldots, \beta_n)$.

3 Einige wichtige Definitionen und Sätze

3.1 Legendre-Symbol

Definition 3.1.1. Sei p eine Primzahl und sei $a \in \mathbb{Z}$ mit $ggT(a, p) = 1$. Das Legendre-Symbol $\left(\frac{a}{p}\right)$ ist durch die folgende Formel definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } \exists x \in \mathbb{Z} : \ x^2 \equiv a \mod p, \\ -1 & \text{falls } \nexists x \in \mathbb{Z} : \ x^2 \equiv a \mod p. \end{cases}$$

Bemerkung 3.1.2. Sei p eine ungerade Primzahl. Die folgenden Formeln sind bekannt (Gauß, Euler):

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \mod 8, \\ -1 & \text{falls } p \equiv \pm 3 \mod 8. \end{cases}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 4, \\ -1 & \text{falls } p \equiv 3 \mod 4. \end{cases}$$

Daraus folgt

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 8, \\ 1 & \text{falls } p \equiv 3 \mod 8, \\ -1 & \text{falls } p \equiv 5 \mod 8, \\ -1 & \text{falls } p \equiv 7 \mod 8. \end{cases}$$

Satz 3.1.3. (Reziprozitätssatz von Gauß) Seien p, q zwei verschiedene Primzahlen, $p, q \geqslant 3$. Dann gilt

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

Satz 3.1.4. Das Polynom $x^4 + 1$ ist irreduzibel über $\mathbb{Z}$, aber es ist reduzibel über $\mathbb{Z}_p$ für jede Primzahl p.

Beweis. Das Polynom $f(x) = x^4+1$ ist irreduzibel über $\mathbb{Z}$, da das Polynom $f(x+1) = x^4+4x^3+6x^2+4x+2$ irreduzibel über $\mathbb{Z}$ nach dem Eisenstein-Kriterium ist. Jetzt beweisen wir, dass $f(x)$ reduzibel über $\mathbb{Z}_p$ für jede Primzahl p ist.

Wir haben $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (2 - a^2)x^2 + 1$, falls $a^2 \equiv 2 \mod p$ ist. Eine solche a existiert für $p \equiv \pm 1 \mod 8$.

Wir haben $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1) = x^4 + (-2 - a^2)x^2 + 1$, falls $a^2 \equiv -2 \mod p$ ist. Eine solche a existiert für $p \equiv 3 \mod 8$.

Wir haben $x^4 + 1 = (x^2 + a)(x^2 - a) = x^4 - a^2$, falls $a^2 \equiv -1 \mod p$ ist. Eine solche a existiert für $p \equiv 1 \mod 4$, insbesondere für $p \equiv 5 \mod 8$. □

Weiter sind einige wichtige Definitionen und Sätze gegeben, die wir wegen Zeitmangels nicht ausführlich besprechen (beweisen) können. Den Stoff kann man in dem Buch von S. Lang "Algebra" (Kapitel: "Algebraic extensions") finden.

3.2 AlgebraischerAbschluss

Definition 3.2.1. Ein Körper L heißt *algebraisch abgeschlossen*, falls jedes Polynom in $L[X]$ des Grades $\geqslant 1$ eine Nullstelle in L hat.

Definition 3.2.2. Sei $k \subseteq L$ eine Körpererweiterung. Der Körper L heißt *algebraischer Abschluss* von k, falls das Folgende gilt:
1) L ist algebraisch abgeschlossen,
2) L ist algebraisch über k.

Satz 3.2.3. Für jeden Körper k existiert ein algebraischer Abschluss von k. Seien L_1, L_2 zwei algebraische Abschlüsse von k, dann existiert ein Isomorphismus $\varphi : L_1 \to L_2$ mit $\varphi_{|k} = id$.

Einen algebraischen Abschluss von k bezeichnen wir mit k^{a}.

Bemerkung. Es gibt algebraisch abgeschlossene, aber nicht algebraische Erweiterungen von k. Ein Beispiel dazu: $k(t)^{\mathrm{a}}$, wobei $k(t)$ der Körper aller rationalen Funktionen von t über k ist:

$$k(t) := \{\frac{f(t)}{g(t)} \mid f(t), g(t) \in k[t], g(t) \neq 0\}.$$

Ein anderes Beispiel: $\mathbb{C}$ ist eine algebraisch abgeschlossene, aber nicht algebraische Erweiterung von $\mathbb{Q}$.

3.3 Erweiterungen von Einbettungen

Sei $k \subseteq K$ eine Körpererweiterung und sei L ein Körper.

Seien $\sigma : k \to L$ und $\tau : K \to L$ zwei Einbettungen (d.h. injektive Homomorphismen). Man sagt, dass τ eine *Erweiterung* von σ ist, falls $\tau_{|k} = \sigma$ ist.

Satz 3.3.1. Sei $K = k(\alpha)$, wobei α algebraisch über k ist. Jede Einbettung $\sigma : k \to L$ von k in einen algebraisch abgeschlossenen Körper L hat genau n Erweiterungen $\tau : K \to L$, wobei n die Anzahl der verschiedenen Nullstellen von $m_\alpha(x)$ in k^{a} ist.

Beweis. Sei $m_\alpha(x) = x^n + a_{n-1}x^n + \cdots + a_0$ das minimale Polynom von α über k, $a_i \in k$. Wir betrachten das Polynom $\sigma(m_\alpha(x)) = x^n + \sigma(a_{n-1})x^n + \cdots + \sigma(a_0)$ und sei β eine beliebige Nullstelle von $\sigma(m_\alpha(x))$ in L. Eine solche Nullstelle existiert, weil L algebraisch abgeschlossen ist. Merken wir an, dass $\sigma(m_\alpha(x))$ das *minimale* Polynom für β über $\sigma(k)$ ist. In der Tat, wenn $\sigma(m_\alpha(x))$ zerlegbar über $\sigma(k)$ wäre, dann wäre $m_\alpha(x)$ über k zerlegbar, was unmöglich ist.

Wir definieren eine Abbildung $\tau : k(\alpha) \to L$ mit Hilfe $\tau(\alpha) = \beta$ und $\tau_{|k} = \sigma$. Etwas ausführlicher: Sei $\omega \in k(\alpha)$. Nach Satz 1.7 ist $\omega = f(\alpha)$ für ein Polynom $f(x) \in k[x]$. Dann setzen wir $\tau(\omega) := \sigma(f(x))(\beta)$. (Das Letztgenannte versteht man so: wende σ an die Koeffizienten von $f(x)$ und setze β statt x.)

Wir sollen das Folgende zeigen:

1) $\tau(\omega)$ ist wohldefiniert, d.h. $\tau(\omega)$ hängt nicht von der Wahl von $f(x)$ ab.

   In der Tat, wenn $\omega = f(\alpha) = g(\alpha)$ mit $f(x), g(x) \in k[x]$ ist, dann ist $m_\alpha(x)$ ein Teiler von $f(x) - g(x)$. Dann ist $\sigma(m_\alpha(x))$ ein Teiler von $\sigma(f(x)) - \sigma(g(x))$. Da $\sigma(m_\alpha(x))(\beta) = 0$ ist, haben wir $\sigma(f(x))(\beta) = \sigma(g(x))(\beta)$.

2) $\tau : k(\alpha) \to L$ ist ein Homomorphismus.

   In der Tat, seien $\omega_1 = f_1(\alpha)$ und $\omega_2 = f_2(\alpha)$ für einige $f(x), g(x) \in k[x]$. Dann gilt:

$$\tau(\omega_1\omega_2) = \sigma(f_1(x)f_2(x))(\beta) = \sigma(f_1(x))(\beta) \cdot \sigma(f_2(x))(\beta) = \tau(\omega_1)\tau(\omega_2).$$

3) τ ist injektiv.

   In der Tat, sei ω ein Element von $k(\alpha)$ mit $\tau(\omega) = 0$. Wir haben $\omega = f(\alpha)$ für einen $f(x) \in k[x]$ und es gilt $0 = \tau(\omega) = \sigma(f(x))(\beta)$. Da $\sigma(m_\alpha(x))$ ein minimales Polynom für β über $\sigma(k)$ ist, ist $\sigma(m_\alpha(x))$ ein Teiler von $\sigma(f(x))$. Daraus folgt, dass $m_\alpha(x)$ ein Teiler von $f(x)$ ist und so $\omega = 0$ ist.

Schließlich zeigen wir, dass die Anzahl von Fortsetzungen τ gleich der Anzahl von verschiedenen Nullstellen von $m_\alpha(x)$ in L ist. Wir haben $0 = m_\alpha(\alpha)$. Sei τ eine der gewünschten Fortsetzungen. Nach der Anwendung von τ bekommen wir $0 = \sigma(m_\alpha)(\tau(\alpha))$. Dann ist $\tau(\alpha)$ eine der Nullstellen von $\sigma(m_\alpha)$. Oben haben wir schon gezeigt, dass jede Nullstelle des Polynoms $\sigma(m_\alpha)(x)$ in L eine Fortsetzung τ definiert. □

4 Separable Erweiterungen

Der folgende Satz ist eine Verallgemeinerung des Satzes 3.3.1.

Satz und Definition 4.1. Sei $k \subseteq K$ eine algebraische Erweiterung von k. Jede Einbettung $\sigma : k \to L$ von k in einen algebraisch abgeschlossenen Körper L kann bis zu einer Einbettung $\tau : K \to L$ erweitert werden.

Die Kardinalität der Menge der Erweiterungen hängt nur von k und K ab (also nicht von L und σ). Diese Kardinalität heißt *Separabilitätsgrad* von K über k und wird als $[K : k]_s$ bezeichnet. Es gilt $[K : k]_s \leqslant [K : k]$.

Definition 4.2.

1) Eine endliche Erweiterung $k \subseteq K$ heißt *separabel*, falls $[K : k]_s = [K : k]$ gilt.

2) Ein algebraisches Element α über k heißt *separabel*, falls $m_\alpha(x)$ keine vielfachen Nullstellen hat.

Satz 4.3.

1) Eine endliche Erweiterung $k \subseteq k(\alpha)$ ist separabel genau dann, wenn α separabel ist.

2) Seien $k \subseteq k_1 \subseteq K$ endliche Erweiterungen. Dann gilt: Die Erweiterung $k \subseteq K$ ist separabel genau dann, wenn beide Erweiterungen $k \subseteq k_1$ und $k_1 \subseteq K$ separabel sind.

3) Seien $k \subseteq k_1 \subseteq K$ endliche Erweiterungen. Dann gilt: $[K : k]_s = [K : k_1]_s[k_1 : k]_s$

Satz 4.4. Eine endliche Erweiterung $k \subseteq K$ ist separabel genau dann, wenn jedes $\alpha \in K$ separabel über k ist.

Satz 4.5. Sei $k \subseteq K$ eine separable Erweiterung mit endlichem Grad $[K : k] = n$ und seien $\tau_1, \tau_2, \ldots, \tau_n$ alle Einbettungen von K in k^{a} (über k). Dann gilt für jedes $\alpha \in K$:

$$\chi_\alpha(x) = (x - \tau_1(\alpha))(x - \tau_2(\alpha)) \ldots (x - \tau_n(\alpha)).$$

Folgerung 4.6. Sei $k \subseteq K$ eine separable Erweiterung mit endlichem Grad $[K : k] = n$ und seien $\tau_1, \tau_2, \ldots, \tau_n$ alle Einbettungen von K in k^{a} (über k). Dann gilt für jedes $\alpha \in K$:

$$\mathrm{Sp}_{K/k}(\alpha) = \tau_1(\alpha) + \tau_2(\alpha) + \ldots + \tau_n(\alpha),$$

$$N_{K/k}(\alpha) = \tau_1(\alpha) \cdot \tau_2(\alpha) \cdot \ldots \cdot \tau_n(\alpha).$$

Satz 4.7. Sei $k \subseteq K$ eine separable Erweiterung mit $[K : k] = n < \infty$ und seien $\tau_1, \ldots, \tau_n$ alle Einbettungen von K in k^{a} über k. Seien $\alpha_1, \ldots, \alpha_n \in K$. Dann gilt:

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(\tau_j(\alpha_i)))^2 = \begin{vmatrix} \tau_1(\alpha_1) & \ldots & \tau_n(\alpha_1) \\ \vdots & & \vdots \\ \tau_1(\alpha_n) & \ldots & \tau_n(\alpha_n) \end{vmatrix}^2.$$

5 Algebraische Zahlkörper K und ganze Zahlen in K

Definition 5.1. Ein Körper K heißt *Zahlkörper*, falls $\mathbb{Q} \subseteq K \subset \mathbb{C}$ ist und $[K : \mathbb{Q}]$ endlich ist.

Definition 5.2. Ein $\alpha \in \mathbb{C}$ heißt *ganze algebraische Zahl*, falls ein Polynom $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ mit $c_0, \ldots, c_{n-1} \in \mathbb{Z}$ und dem Hauptkoeffizient 1 existiert, so dass $f(\alpha) = 0$ ist.

Äquivalente Definition ist:

Definition 5.2′. Ein $\alpha \in \mathbb{C}$ heißt *ganze algebraische Zahl*, falls die Koeffizienten des minimalen Polynoms $m_\alpha(x, \mathbb{Q})$ in $\mathbb{Z}$ liegen.

Satz 5.3. Die Menge $\mathcal{O}$ der ganzen algebraischen Zahlen in $\mathbb{C}$ bildet einen Ring.

Definition 5.4. Sei K ein Zahlkörper. Der Ring $\mathcal{O}_K = \mathcal{O}_\mathbb{C} \cap K$ heißt *Ring der algebraischen Zahlen in K* oder *Ganzheitsring* von K.

Satz 5.5. Es gilt $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

Satz 5.6. Sei $m \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei (d.h. m ein Produkt von verschiedenen Primzahlen ist) und sei $K = \mathbb{Q}(\sqrt{m})$.

(a) Die Zahl $\alpha = a + b\sqrt{m} \in K$ mit $a, b \in \mathbb{Q}$ ist ganz genau dann, wenn die folgenden Zahlen ganz sind:

$$\begin{array}{rcl} N(\alpha) & = & a^2 - b^2 m, \\ \mathrm{Sp}(\alpha) & = & 2a. \end{array}$$

(b) Es ist:

$$\begin{array}{rcccl} \mathcal{O}_K & = & \mathbb{Z}[\sqrt{m}] & = & \mathbb{Z} \oplus \mathbb{Z}\sqrt{m}, \quad \text{falls} \quad m = 2 \text{ oder } 3 \mod 4, \\ \mathcal{O}_K & = & \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & = & \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{m}}{2}, \quad \text{falls} \quad m = 1 \mod 4. \end{array}$$

6 Einheiten, Primelemente und irreduzible Elemente

Definition 6.1. Sei R ein kommutativer Ring mit 1.

1) Seien $x, y \in R$. Man sagt, dass y ein *Teiler* von x ist, falls ein $z \in R$ mit $x = yz$ existiert. In dem Fall schreibt man $y|x$.

2) Ein Element $x \in R$ heißt *Einheit* in R, falls ein $y \in R$ mit $xy = 1$ existiert.
Die Menge der Einheiten in R ist eine multiplikative Gruppe. Diese Gruppe heißt *Einheitsgruppe* von R und wird mit R^* bezeichnet.

3) Ein Element $0 \neq x \in R$ heißt *Primelement* in R, falls das Folgende gilt:
(a) x ist keine Einheit;
(b) für alle $a, b \in R$ gilt:
Teilt x das Produkt ab, dann teilt x das Element a oder das Element b.

4) Ein Element $0 \neq x \in R$ heißt *irreduzibel* in R, falls das Folgende gilt:
(a) x ist keine Einheit;
(b) aus $x = yz$ mit $y, z \in R$ folgt, dass y oder z eine Einheit in R ist.

Satz 6.2. Sei $m \in \mathbb{Z}$ und $K = \mathbb{Q}(\sqrt{m})$. Dann ist

$$(\mathcal{O}_K)^* = \{x \in \mathcal{O}_K \mid N(x) = \pm 1\}.$$

$\boxed{\textbf{Aufgabe.}}$ Sei $K = \mathbb{Q}(\sqrt{-5})$. Beweisen Sie, dass die Zahl $3n$ (wobei $n \in \mathbb{N}$ ist) nicht in Primzahlen in $\mathcal{O}_K$ zerlegt werden kann.

Beweis. Wir schreiben $3n = 3^\alpha m$ mit $\alpha, m \in \mathbb{N}$ und $3 \nmid m$. Nehmen wir an, dass

$$3^\alpha m = \prod_{i=1}^{k} p_i$$

ist, wobei $p_i \in \mathrm{Prim}(\mathcal{O}_K)$ ist. Dann gilt $p_i | 3$ oder $p_i | m$ in $\mathcal{O}_K$.

Fall 1. Nehmen wir an, dass $p_i | 3$ in $\mathcal{O}_K$ für ein i ist.

Sei $3 = p_i q_i$ für ein $q_i \in \mathcal{O}_K$. Dann gilt $N(p_i)N(q_i) = N(3) = 9$.

Da p_i keine Einheit ist, ist $N(p_i) \neq 1$. Auch ist $N(p_i) \neq 3$. Dann ist $N(p_i) = 9$ und $N(q_i) = 1$, also ist $q_i = \pm 1$ und $p_i = \pm 3$.

Dann gilt $3 \in \mathrm{Prim}(\mathcal{O}_K)$. Wir betrachten

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

Dann teilt 3 eine der Zahlen $(1 + \sqrt{-5}), (1 - \sqrt{-5})$ in $\mathcal{O}_K$, was unmöglich ist.

Fall 2. Nehmen wir an, dass $p_i | m$ in $\mathcal{O}_K$ für alle i ist.

Dann ist $m = p_i q_i$ für einige $q_i \in \mathcal{O}_K$. Dann gilt:

$$3^\alpha \cdot m \prod_{i=1}^{k} q_i = \prod_{i=1}^{k} (p_i q_i) = m^k$$

Dann ist $\prod_{i=1}^{k} q_i = m^{k-1}/3$. Diese Zahl liegt nicht in $\mathcal{O}_K$, ein Widerspruch.

Satz 6.3. Sei $K = \mathbb{Q}(\sqrt{-5})$ und sei p eine Primzahl in $\mathbb{Z}$. Dann gilt

$$p \in \mathrm{Prim}(\mathcal{O}_K) \Leftrightarrow \left(\frac{-5}{p}\right) = -1.$$

Beweis. Der Fall $p = 5$ ist trivial: $5 \notin \mathrm{Prim}(\mathcal{O}_K)$ weil $5 | \sqrt{-5} \cdot \sqrt{-5}$, aber $\frac{\sqrt{-5}}{5} \notin \mathcal{O}_K$ ist.

Jetzt betrachten wir den Fall $p \neq 5$.
Nach dem Satz 5.6 b) gilt: $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$.

1) Sei $\left(\frac{-5}{p}\right) = 1$. Dann existiert $a \in \mathbb{Z}$ mit $a^2 \equiv -5 \pmod p$. Dann gilt

$$p|(a^2+5) = (a+\sqrt{-5})(a-\sqrt{-5}).$$

Es ist klar, dass $(a \pm \sqrt{-5}) \in \mathcal{O}_K$, aber $p \nmid (a \pm \sqrt{-5})$ ist. Daraus folgt $p \notin \mathrm{Prim}(\mathcal{O}_K)$.

2) Sei $\left(\frac{-5}{p}\right) = -1$. Wir zeigen, dass $p \in \mathrm{Prim}(\mathcal{O}_K)$ gilt. Dafür müssen wir zeigen: wenn

$$p|(a+b\sqrt{-5})(a_1+b_1\sqrt{-5}) \tag{1}$$

in $\mathcal{O}_K$ gilt, dann teilt p einen dieser Faktoren in $\mathcal{O}_K$. Aus (1) folgt

$$N(p)|\ N(a+b\sqrt{-5}) \cdot N(a_1+b_1\sqrt{-5}), \tag{2}$$

$$p^2|(a^2+5b^2)(a_1^2+5b_1^2).$$

O.B.d.A. gilt

$$p|(a^2+5b^2). \tag{3}$$

Wenn $p|b$ ist, dann ist $p|a$ und $p|(a+b\sqrt{-5})$ in $\mathcal{O}_K$.

Wenn $p \nmid b$ ist, dann folgt aus $a^2 \equiv -5b^2 \pmod p$ die Kongruenz $(a/b)^2 \equiv -5 \pmod p$, wobei wir a durch b in $\mathbb{Z}_p$ teilen. Dann haben wir $\left(\frac{-5}{p}\right) = 1$; ein Widerspruch.

Korollar 6.4.

1) Es existieren unendlich viel $p \in \mathrm{Prim}(\mathbb{Z})$, die nicht prim in $\mathcal{O}_K$ sind. Z.B. sind so die Primzahlen der Form $1+20n$ mit $n \in \mathbb{N}$.
2) Es existieren unendlich viel $p \in \mathrm{Prim}(\mathbb{Z})$, die prim in $\mathcal{O}_K$ sind. Z.B. sind so die Primzahlen der Form $11+20n$ mit $n \in \mathbb{N}$.

Satz 6.5. Sei $K = \mathbb{Q}(\sqrt{-5})$ und sei $\alpha = a + b\sqrt{-5} \in \mathcal{O}_K$ mit $a, b \in \mathbb{Z}$, $b \neq 0$. Dann gilt

$$\alpha \in \mathrm{Prim}(\mathcal{O}_K) \Leftrightarrow N(\alpha) = a^2 + 5b^2 \in \mathrm{Prim}(\mathbb{Z}).$$

Beweis. Für $a = 0$ ist die Aussage leicht. Deswegen nehmen wir an, dass $a \neq 0$ ist. Der Teil 1) ist nicht schwer und wir empfehlen, ihn zu lesen. Der Teil 2) ist schwer und kann beim ersten Lesen vernachlässigt werden. Wir bezeichnen $\overline{\alpha} := a - b\sqrt{-5}$. Dann gilt

$$\alpha\overline{\alpha} = N(\alpha).$$

Da $a, b \neq 0$ ist, ist $N(\alpha) = a^2 + 5b^2 \geqslant 6$.

Teil 1) Sei $\alpha \in \mathrm{Prim}(\mathcal{O}_K)$. Wir beweisen, dass $N(\alpha) \in \mathrm{Prim}(\mathbb{Z})$ ist.

Da $N(\alpha) > 1$ ist, können wir $N(\alpha)$ in der folgenden Form schreiben:

$$N(\alpha) = q^k r,$$

wobei q der minimale Primteiler von $N(\alpha)$ in $\mathbb{Z}$ ist und $r \in \mathbb{Z}$ teilerfremd zu q ist.

Fall 1. Sei $r \neq 1$.

Dann gilt $r > q$. Wir haben $\alpha | N(\alpha)$ in $\mathcal{O}_K$, deshalb gilt $\alpha | q$ oder $\alpha | r$. Dann gilt $N(\alpha) | N(q)$ oder $N(\alpha) | N(r)$. Dann gilt $q^k r | q^2$ oder $q^k r | r^2$, was unmöglich ist.

Fall 2. Sei $r = 1$ und $k \geqslant 2$, also sei $N(\alpha) = q^k$ mit $k \geqslant 2$.

Wir haben $\alpha | N(\alpha)$ in $\mathcal{O}_K$, deshalb gilt $\alpha | q$, und so gilt

$$\begin{aligned} q &= \alpha \cdot \beta \text{ für einen } \beta \in \mathcal{O}_K, \\ N(q) &= N(\alpha) \cdot N(\beta), \\ q^2 &= q^k \cdot N(\beta). \end{aligned}$$

Daraus und aus $k \geqslant 2$ folgt $k = 2$ und $N(\beta) = 1$. Wir schreiben β in der Form $\beta = a_1 + b_1\sqrt{-5}$ mit $a_1, b_1 \in \mathbb{Z}$. Dann gilt $N(\beta) = a_1^2 + 5b_1^2 = 1$. Daraus folgt $b_1 = 0$, $a_1 = \pm 1$, und so ist $\beta = \pm 1$. Wir haben $q = \pm\alpha = \pm(a + b\sqrt{-5})$, was unmöglich ist, da $b \neq 0$ ist.

Fall 3. Sei $r = 1$ und $k = 1$, also sei $N(\alpha) = q$.

Dann gilt $N(\alpha) \in \mathrm{Prim}(\mathbb{Z})$.

Teil 2) Sei $N(\alpha) = q \in \mathrm{Prim}(\mathbb{Z})$. Wir beweisen, dass $\alpha \in \mathrm{Prim}(\mathcal{O}_K)$ ist.
Wir müssen beweisen, dass aus

$$\alpha \,|\, (a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}) \tag{4}$$

mit $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ folgt:

$$\alpha \,|\, (a_1 + b_1\sqrt{-5}) \quad \text{oder} \quad \alpha \,|\, (a_2 + b_2\sqrt{-5}). \tag{5}$$

Zuerst bemerken wir, dass aus (4) folgt:

$$q \,|\, (a_1^2 + 5b_1^2) \cdot (a_2^2 + 5b_2^2).$$

O.B.d.A. gilt

$$q \,|\, (a_1^2 + 5b_1^2). \tag{6}$$

Äquivalent gilt

$$a_1^2 \equiv -5b_1^2 \pmod{q}. \tag{7}$$

Außerdem gilt

$$a^2 \equiv -5b^2 \pmod{q}, \qquad 0 < |b| < q, \tag{8}$$

da $q = N(\alpha) = a^2 + 5b^2$ ist.

Fall 1. Sei $q | b_1$.

Dann ist $q | a_1$ und $q | (a_1 + b_1\sqrt{-5})$. Also gilt $N(\alpha) | (a_1 + b_1\sqrt{-5})$. Jetzt merken wir an, dass $\alpha | N(\alpha)$ gilt. Daraus folgt $\alpha \,|\, (a_1 + b_1\sqrt{-5})$, was in (5) gewünscht wurde.

Fall 2. Sei $q \nmid b_1$.

Dann ist b_1 in $\mathbb{Z}_q$ invertibel und (7) und (8) implizieren

$$(\widetilde{a}_1/\widetilde{b}_1)^2 = -5 = (\widetilde{a}/\widetilde{b})^2,$$

wobei $\widetilde{n}$ das Bild von n in $\mathbb{Z}_q$ bedeutet. In dem Körper $\mathbb{Z}_q$ existieren nicht mehr als zwei Lösungen der Gleichung $x^2 = -5$, deswegen gilt:

$$(\widetilde{a}_1/\widetilde{b}_1) = \pm(\widetilde{a}/\widetilde{b}).$$

So existiert ein $\widetilde{s} \in \mathbb{Z}_q$ mit

$$(\widetilde{a}_1, \widetilde{b}_1) = \widetilde{s}(\widetilde{a}, \pm\widetilde{b}).$$

Daraus folgt:

$$a_1 = sa + qn \quad \text{und} \quad b_1 = \pm sb + qm \tag{9}$$

für einige $n, m \in \mathbb{Z}$. Dabei kann man s so wählen, dass $0 \leqslant s < q$ gilt.

Fall 2.1. Sei $s = 0$.

Dann gilt

$$\begin{aligned} a_1 + b_1\sqrt{-5} &= q(n + m\sqrt{-5}) \\ &= N(\alpha)(n + m\sqrt{-5}). \end{aligned}$$

Mit Hilfe von $\alpha | N(\alpha)$ leiten wir daraus ab:

$$\alpha | (a_1 + b_1\sqrt{-5}), \tag{10}$$

was in (5) gewünscht wurde.

Fall 2.2. Sei $0 < s < q$.

Fall 2.2.a) Wenn das Vorzeichen in (9) "+" ist, dann ist

$$\begin{aligned} (a_1 + b_1\sqrt{-5}) &= (sa + qn) + (sb + qm)\sqrt{-5} \\ &= s(a + b\sqrt{-5}\,) + q(n + m\sqrt{-5}\,) \\ &= s\alpha + N(\alpha)(n + m\sqrt{-5}\,). \end{aligned}$$

Mit Hilfe von $\alpha | N(\alpha)$ leiten wir daraus ab:

$$\alpha | (a_1 + b_1\sqrt{-5}), \tag{11}$$

was in (5) gewünscht wurde.

Fall 2.2.b) Wenn das Vorzeichen in (9) "−" ist, dann ist

$$\begin{aligned} (a_1 + b_1\sqrt{-5}) &= (sa + qn) + (-sb + qm)\sqrt{-5} \\ &= s(a - b\sqrt{-5}) + q(n + m\sqrt{-5}) \\ &= s\overline{\alpha} + N(\alpha)(n + m\sqrt{-5}). \end{aligned} \tag{12}$$

Mit Hilfe von $\alpha|N(\alpha)$ leiten wir daraus und aus (4) ab:

$$\alpha|\, s\overline{\alpha} \cdot (a_2 + b_2\sqrt{-5}). \tag{13}$$

Dann ist

$$\alpha|\, s(\overline{\alpha} + \alpha) \cdot (a_2 + b_2\sqrt{-5}),$$

also ist

$$\alpha|s(2a)(a_2 + b_2\sqrt{-5}). \tag{14}$$

Daraus folgt:

$$q|s^2(2a)^2 \cdot N(a_2 + b_2\sqrt{-5}).$$

Man kann leicht verstehen, dass $q \nmid s^2(2a)^2$ ist. (Dafür benutzt man die Fakten, dass $q \in \mathrm{Prim}(\mathbb{Z})$, $q = a^2 + 5b^2 \geqslant 6$, $0 < s < q$ und $a \neq 0$ ist.) Dann gilt $q|N(a_2 + b_2\sqrt{-5})$, also gilt

$$q|(a_2^2 + 5b_2^2). \tag{15}$$

Vergleichen Sie das mit der Formel (6).
Das Weitere kann man entwickeln wie nach der Formel (6), und das folgende analog der Formel (12) erhalten:

$$(a_2 + b_2\sqrt{-5}) = t\overline{\alpha} + N(\alpha)(r + k\sqrt{-5}), \tag{16}$$

wobei $0 < t < q$ ist. Durch Einsetzen von (12) und (16) in (4) erhalten wir wegen $\alpha|N(\alpha)$:

$$\alpha|st\overline{\alpha}^2.$$

Dann ist

$$\frac{st\overline{\alpha}^2}{\alpha} \in \mathcal{O}_K.$$

Wir haben

$$\frac{st\overline{\alpha}^2}{\alpha} = \frac{st\overline{\alpha}^3}{q} = \frac{st(a - b\sqrt{-5}\,)^3}{q} = \frac{sta(a^2 - 15b^2) + st(-3a^2b + 5b^3)\sqrt{-5}}{q}.$$

Da $0 < s, t, |a| < q = a^2 + 5b^2$ ist, ist $q|(a^2 - 15b^2)$ und so ist $q|20b^2$, was unmöglich ist, da $q \geqslant 6$ und $0 \neq |b| < q$ ist. □

7 Faktorringe, maximale Ideale und Primideale

Wichtige Beobachtung. Sei $K = \mathbb{Q}(\sqrt{-5})$.
1) Es ist leicht zu sehen, dass 2 und 3 keine Primzahlen in $\mathcal{O}_K$ sind: Betrachte

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

2) Die Zahlen 2, 3, 6 können nicht in Primzahlen in dem Ring $\mathcal{O}_K$ zerlegt werden.

Unser großes Ziel ist zu zeigen, dass jedes Ideal in $\mathcal{O}_K$ eindeutig in das Produkt von Primidealen zerlegt werden kann. Dafür benötigen wir einige Definitionen:

- Primideal
- Integritätsbereich
- Noetherscher Ring
- Ganzabgeschlossener Ring
- Dedekindscher Ring.

7.1. Zuerst erinnern wir uns an folgende grundlegende Definitionen und Sätze.
Sei R ein kommutativer Ring mit 1.

- Eine nichtleere Teilmenge $A \subseteq R$ heißt *Ideal* in R, falls:
  1) aus $x, y \in A$ folgt $x - y \in A$,
  2) aus $x \in A$ und $r \in R$ folgt $xr \in A$.

  Es ist klar, dass ein Ideal in R ein Unterring von R ist. Nicht jeder Unterring von R ist ein Ideal in R: Sei $R = \mathbb{Z}[x]$ und sei $A := \mathbb{Z}[x^2]$. Dann ist A ein Unterring in R, aber kein Ideal.

- Seien $a_1, \ldots, a_k$ Elemente von R. Das *Ideal erzeugte von* $a_1, \ldots, a_k$ ist:
  $$(a_1, \ldots, a_k) := a_1R + \cdots + a_kR := \{a_1r_1 + \cdots + a_kr_k \,|\, r_1, \ldots, r_k \in R\}.$$
  Ein Ideal A in R heißt *endlich erzeugt*, falls in A endlich viel Elemente $a_1, \ldots, a_k$ existieren, so dass $A = (a_1, \ldots, a_k)$ gilt.

- Ein Ideal A in R heißt *Hauptideal*, falls A von einem Element erzeugt ist.

- Die Summe und das Produkt von zwei Idealen A und B von R wird so definiert:
  $$\begin{aligned} A + B: &= \{a + b \,|\, a \in A,\, b \in B\}, \\ AB: &= \{a_1b_1 + \cdots + a_kb_k \,|\, k \in \mathbb{N},\, a_i \in A,\, b_i \in B,\, i = 1, \ldots, k\} \end{aligned}$$
  Es ist klar, dass $A + B$ und AB wieder Ideale in R sind. Es gilt $AB \subseteq A \cap B$.

- Sei A ein Ideal in R. Für ein Element $x \in R$ heißt die Menge
  $$[x] := x + A := \{x + a \,|\, a \in A\}$$
  Nebenklasse von A in R mit dem Repräsentant x. Die Menge aller Nebenklassen von A in R
  $$\{[x] \,|\, x \in R\}$$
  mit der Addition $[x] + [y] := [x + y]$ und $[x] \cdot [y] := [xy]$ ist ein Ring. Der Ring heißt *Faktorring* von R modulo A und wird mit R/A bezeichnet.

Das folgende Beispiel zeigt, wie wichtig die Faktorringe sind.

Beispiel: Sei $n \in \mathbb{N}$.
1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ (der Restklassenring modulo n),
2) $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ (der Körper von komplexen Zahlen).
3) Sei p eine Primzahl und sei $f(x)$ ein irreduzibles Polynom in $\mathbb{Z}_p[x]$ des Grades k. Dann ist $\mathbb{Z}_p[x]/(f(x))$ ein Körper der Ordnung p^k.

- Ein Ideal A in R heißt *maximal*, falls A ein *echtes* Ideal ist (d.h. $A \neq R$ ist) und kein Ideal B in R mit
$$A \subsetneqq B \subsetneqq R$$
existiert.

Satz 7.1.1. Sei R ein kommutativer Ring mit 1. Dann liegt jedes echte Ideal von R in einem maximalen Ideal.

Beweis erfolgt mit Hilfe des Zornschen Lemmas aus Logik.

Satz 7.1.2. Sei R ein kommutativer Ring mit 1 und sei A ein echtes Ideal in R. Der Faktorring R/A ist genau dann ein Körper, wenn A maximal ist.

Beweis. 1) Sei A ein maximales Ideal in R. Wir beweisen, dass für jedes nichtnullsche Element in R/A ein Inverses existiert. Sei also $x + A \neq 0 + A$ ein Element von R/A. Dann ist $x \notin A$. Wir betrachten das Ideal $xR + A$ in R. Da $1 \in R$ ist, ist $x \in xR + A$. Dann ist das Ideal $xR + A$ größer als A. Dann ist $xR + A = R$ und somit existieren ein $r \in R$ und ein $a \in A$ mit $xr + a = 1$. Daraus folgt $(x + A)(r + A) = (1 + A)$.

2) Sei A kein maximales Ideal in R. Dann existiert ein Ideal B in R mit $A \subset B \subset R$. Wir nehmen $b \in B \setminus A$ und zeigen, dass kein Inverses zu $b + A$ in R/A existiert. Wenn ein solches Inverses $(c + A)$ existiert, dann gilt $(b + A)(c + A) = (1 + A)$. Dann ist $bc = 1 + a$. Dann ist $1 = bc - a \in BR + A \subseteq BR + B = B$. Daraus folgt $R = B$. Ein Widerspruch. □

7.2. Jetzt definieren wir ein Primideal und stellen einen Zusammenhang her zwischen Primidealen und maximalen Idealen.

Definition 7.2.1. Sei R ein kommutativer Ring. Ein Ideal A in R heißt *prim*, falls

1) A echt ist, d.h. $A \neq R$ ist, und
2) für je zwei Ideale B und C in R gilt:

$$\text{aus } BC \subseteq A \text{ folgt } B \subseteq A \text{ oder } C \subseteq A.$$

Behauptung 7.2.2. Sei R ein kommutativer Ring mit 1. Ein $x \in R \setminus \{0\}$ ist genau dann prim, wenn das von x erzeugte Hauptideal $(x) := xR$ prim ist.

Satz 7.2.3. Sei R ein kommutativer Ring mit 1. Ein Ideal A in R ist prim genau dann, wenn $A \neq R$ und R/A nullteilerfrei ist.

Beweis. 1) Sei R/A nicht nullteilerfrei. Dann existieren $x + A \neq 0 + A$ und $y + A \neq 0 + A$ mit $(x + A)(y + A) = 0 + A$. Daraus folgt $x \notin A$, $y \notin A$ und $xy \in A$. Wir betrachten die Ideale $B := xR + A$ und $C := yR + A$. Dann ist $B \supsetneqq A$, $C \supsetneqq A$ und $BC \subseteq A$. Deswegen ist A nicht prim.

2) Sei A nicht prim. Dann existieren Ideale B und C in R mit $B \subsetneqq A$, $C \subsetneqq A$ und $BC \subseteq A$. Wir wählen $x \in B \setminus A$, $y \in C \setminus A$. Dann ist $x \notin A$, $y \notin A$ und $xy \in A$. Daraus folgt $x + A \neq 0 + A$, $y + A \neq 0 + A$ und $(x + A)(y + A) = 0 + A$. Also ist R/A nicht nullteilerfrei. □

Satz 7.2.4. Sei R ein kommutativer Ring mit 1. Dann gilt:
1) Wenn A ein maximales Ideal in R ist, dann ist A prim.
2) Wenn A prim ist und R/A endlich ist, dann ist A maximal.

Beweis. 1) Sei A ein maximales Ideal in R. Dann ist R/A ein Körper, also ist R/A nullteilerfrei. Nach Satz 7.2.3 ist A prim.

2) R/A ist ein endlicher kommutativer nullteilerfreier Ring mit 1. Man kann leicht zeigen, dass R/A ein Körper ist. Dann ist A maximal nach Satz 7.1.2. □

8 Diskriminante. Noethersche Ringe

In diesem Abschnitt definieren wir noethersche Ringe und beweisen, dass der Ring $\mathcal{O}_K$ noethersch ist. Auch wird die Diskriminante des Zahlkörpers K definiert. Wir erinnern uns, dass ein Zahlkörper eine endliche Erweiterung von $\mathbb{Q}$ in $\mathbb{C}$ ist.

Definition 8.1. Sei R ein nullteilerfreier kommutativer Ring mit 1. Für $a, b \in R$ mit $b \neq 0$ betrachten wir einen formalen Ausdruck $\frac{a}{b}$ und die Klasse

$$\left[\frac{a}{b}\right] := \left\{\frac{x}{y} \mid x, y \in R, y \neq 0, ay = bx\right\}.$$

Der *Quotientenkörper* von R ist die Menge aller solcher Klassen

$$\left\{\left[\frac{a}{b}\right] \mid a, b \in R, b \neq 0\right\}$$

zusammen mit zwei Verknüpfungen $+$ und $\cdot$, die folgendermaßen definiert sind:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right], \qquad \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

Der Quotientenkörper von R wird mit $\mathrm{Quot}(R)$ bezeichnet.

Satz 8.2. Sei K ein Zahlkörper. Für jedes $\alpha \in K$ existiert ein $m \in \mathbb{N}$ mit $m\alpha \in \mathcal{O}_K$.

Folgerung 8.3. Sei K ein Zahlkörper. Dann ist $\mathrm{Quot}(\mathcal{O}_K) \cong K$.

Satz 8.4. Sei K ein Zahlkörper. Jedes nichtnullsche Ideal A in $\mathcal{O}_K$ enthält eine Basis $\alpha_1, \ldots, \alpha_n$ von K über $\mathbb{Q}$.

Satz 8.5. Sei K ein Zahlkörper und sei A ein nichtnullsches Ideal in $\mathcal{O}_K$. Dann gilt:

1) Das Ideal A enthält Zahlen $\alpha_1, \ldots, \alpha_n$, für die das Folgende gilt:
   a) $\alpha_1, \ldots, \alpha_n$ ist eine Basis von K über $\mathbb{Q}$;
   b) $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.
2) Die Zahl $\Delta(\alpha_1, \ldots, \alpha_n)$ liegt in $\mathbb{Z} \setminus \{0\}$ und hängt nicht von der Wahl der Zahlen in 1) ab.

Definition 8.6. Sei K ein Zahlkörper und sei A ein nichtnullsches Ideal in $\mathcal{O}_K$.

i) Die Zahlen $\alpha_1, \dots, \alpha_n$ in A aus dem Satz 8.5.1) heißen *Ganzheitsbasis von A*.

ii) Die Zahl $\Delta(\alpha_1, \dots, \alpha_n)$ im Satz 8.5.2) heißt *Diskriminante von A* und wird mit $\delta(A)$ bezeichnet.

iii) Die Diskriminante von $\mathcal{O}_K$ ist besonders wichtig und heißt *Diskriminante des Körpers K über $\mathbb{Q}$* und wird mit $\delta(K)$ bezeichnet.

Satz 8.7. Sei $K = \mathbb{Q}(\sqrt{m})$, wobei $m \in \mathbb{Z} \setminus \{0\}$ quadratfrei ist. Dann gilt

$$\delta(K) = \begin{cases} 4m & \text{falls } m \equiv 2, 3 \pmod 4, \\ m & \text{falls } m \equiv 1 \pmod 4). \end{cases}$$

Beweis. Im Satz 5.6 ist eine ganzzahlige Basis von $\mathcal{O}_K$ gegeben. Die Diskriminante $\delta(\mathcal{O}_K)$ wird dann nach Definition berechnet. □

Definition 8.8. Sei R ein kommutativer Ring mit 1. Der Ring heißt *noethersch*, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

1) jede unendliche aufsteigende Kette $A_1 \subseteq A_2 \subseteq A_3 \subset \dots$ von Idealen in R stabilisiert sich, d.h. es existiert ein $n \in \mathbb{N}$ mit $A_n = A_{n+1} = A_{n+2} \dots$.
2) jedes Ideal A in R ist endlich erzeugt, d.h. es existieren endlich viel $a_1, \dots, a_k \in A$ mit $A = a_1R + a_2R + \dots + a_kR$.

Beispiel.
a) Der Ring $\mathbb{Z}$ und jeder Körper sind noethersch.
b) Der Ring $\mathbb{Q}[X_1, X_2, \dots]$ in unendlich vielen Unbestimmten ist nicht noethersch, da das Ideal, das von allen Unbestimmten erzeugt wird, nicht endlich erzeugt ist.

Satz 8.9. (Hilbertscher Basissatz) Ist R ein nötherscher Ring, so ist auch der Polynomring $R[x]$ nöthersch. Insbesondere sind die Ringe $\mathbb{Z}[X_1, \dots, X_n]$ und $K[X_1, \dots, X_n]$ noethersch, wobei K ein Körper ist.

Satz 8.10. Sei K ein Zahlkörper. Dann ist der Ganzheitsring $\mathcal{O}_K$ noethersch.

Beweis. Der Beweis folgt aus dem Satz 8.5.

9 Der Ganzheitsring $\mathcal{O}_K$ ist dedekindsch

Lemma 9.1. In jedem nichtnullschen Ideal A des Ganzheitsringes $\mathcal{O}_K$ liegt eine natürliche Zahl.

Satz 9.2. Sei A ein nichtnullsches Ideal in $\mathcal{O}_K$. Dann ist der Faktorring $\mathcal{O}_K/A$ endlich.

Satz 9.3. Jedes nichtnullsche Primideal in $\mathcal{O}_K$ ist maximal.

Definition 9.4. Ein *Integritätsbereich* ist ein nichtnullscher Ring R mit folgenden Eigenschaften:

1) R ist kommutativ und mit 1.
2) R ist nullteilerfrei (d.h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$).

Definition 9.5. Ein Integritätsbereich R heißt *ganzabgeschlossen*, falls gilt:
Ist $\alpha \in \operatorname{Quot}(R)$ eine Nullstelle eines monischen Polynoms $f(x) \in R[x]$, so ist $\alpha \in R$.

Satz 9.6. Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K$ ganzabgeschlossen.

Beweis. Nach Folgerung 8.3 ist $K = \operatorname{Quot}(\mathcal{O}_K)$. So müssen wir das Folgende beweisen: Ist $\alpha \in K$ eine Nullstelle eines monischen Polynoms $f(x) \in \mathcal{O}_K[x]$, dann ist $\alpha \in \mathcal{O}_K$. Das Letzte kann man mit einem Standardargument zeigen.

Definition 9.7. Ein Ring R heißt *dedekindscher* Ring falls das Folgende gilt:

1) R ist ein Integritätsbereich;
2) R ist noethersch;
3) R ist ganzabgeschlossen;
4) jedes nichtnullsche Primideal in R ist maximal.

Folgerung 9.8. Für jeden Zahlkörper K ist der Ring $\mathcal{O}_K$ dedekindsch.

Definition 9.9. Sei R ein Integritätsbereich. Zwei nichtnullsche Ideale A, B in R heißen *äquivalent*, falls zwei nichtnullsche Elemente α, β in R mit

$$(\alpha)A = (\beta)B$$

existieren. In dem Fall schreibt man $A \sim B$. (Man kann nachprüfen, dass $\sim$ eine Äquivalenzrelation auf der Menge aller nichtnullschen Ideale von R ist.) Sei $[A]$ die Äquivalenzklasse, die das Ideal A enthält:

$$[A] := \{B \mid B \sim A\}.$$

Die Anzahl von Äquivalenzklassen aller nichtnullschen Ideale von R heißt *Idealklassenzahl* und wird mit h_R bezeichnet.

Aufgabe 9.10. Sei R ein Integritätsbereich. Dann ist $h_R = 1$ genau dann, wenn jedes Ideal in R ein Hauptideal ist.

Lemma 9.11. Sei K ein Zahlkörper. Dann existiert ein $M \in \mathbb{N}$ mit der folgenden Eigenschaft:

Für jedes $\gamma \in K$ existieren eine natürliche Zahl $1 \leqslant n \leqslant M$ und ein Element $\omega \in \mathcal{O}_K$, so dass gilt:

$$|N(n\gamma - \omega)| < 1.$$

Satz 9.12. Sei K ein Zahlkörper. Dann ist die Idealklassenzahl von $\mathcal{O}_K$ endlich.

10 Zerlegung von Idealen in $\mathcal{O}_K$ in Primideale

Lemma 10.1. Sei $A \neq \{0\}$ ein Ideal in $\mathcal{O}_K$ und sei $\beta \in K$, so dass $\beta A \subseteq A$ ist. Dann ist $\beta \in \mathcal{O}_K$.

Lemma 10.2. Seien $A, B \neq \{0\}$ Ideale in $\mathcal{O}_K$, so dass $A = AB$ ist. Dann ist $B = \mathcal{O}_K$.

Lemma 10.3. Seien $A, B \neq \{0\}$ zwei Ideale in $\mathcal{O}_K$ und sei $\omega \in \mathcal{O}_K \setminus \{0\}$, so dass $A \cdot (\omega) = AB$ gilt. Dann ist $(\omega) = B$.

Satz 10.4. Für jedes Ideal $A \neq \{0\}$ in $\mathcal{O}_K$ existiert ein $k \in \mathbb{N}$ mit $1 \leqslant k \leqslant h_k$, so dass A^k ein Hauptideal ist. Hier ist h_K die Idealklassenzahl von K.

Satz 10.5. Die Menge

$$\{[A] \,|\, A \text{ ist ein Ideal in } \mathcal{O}_K,\ \ A \neq \{0\}\}$$

mit der Multiplikation $[A] \cdot [B] := [AB]$ bildet eine Gruppe. Sie ist kommutativ und endlich.

Definition 10.6. Die Gruppe aus dem Satz 10.5 heißt *Idealklassengruppe* von K und wird mit $Cl(K)$ bezeichnet.

Satz 10.7. Seien $A, B \neq \{0\}$ Ideale in $\mathcal{O}_K$, so dass $A \subseteq B$ gilt. Dann existiert ein Ideal C in $\mathcal{O}_K$ mit $A = BC$.

Satz 10.8. Seien $A, B, C \neq \{0\}$ Ideale in $\mathcal{O}_K$, so dass $AB = AC$ gilt. Dann gilt $B = C$.

Satz 10.9. Sei $B \neq \{0\}$ ein Ideal in $\mathcal{O}_K$. Wenn $B \neq \mathcal{O}_K$ ist, dann existieren ein Primideal P und ein Ideal C in $\mathcal{O}_K$, so dass $B = PC$ gilt. Außerdem gilt $B \subsetneqq C$.

Satz 10.10. Sei A ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$. Dann ist $A = P_1 P_2 \dots P_k$ für einige (nicht unbedingt verschiedene) Primideale $P_1, P_2, \dots, P_k$ in $\mathcal{O}_K$.

Satz 10.11. Sei $\{0\} \neq A \neq \mathcal{O}_K$ ein Ideal in $\mathcal{O}_K$. Dann gilt

$$A \supsetneqq A^2 \supsetneqq A^3 \supsetneqq \dots \quad \text{und} \quad \bigcap_{i=1}^{\infty} A^i = \{0\}.$$

Definition 10.12. Sei P ein Primideal und sei A ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$. Wir setzen $P^0 := \mathcal{O}_K$ und definieren die *Ordnung* von A bezüglich P durch

$$\mathrm{ord}_P(A) := \max\{k \geqslant 0 \,|\, A \subseteq P^k\}.$$

Bemerkung. Dieses maximum existiert nach Satz 10.11. Man kann die Definition folgendermaßen umformulieren:

$$\mathrm{ord}_P(A) = k \iff A \subseteq P^k \text{ und } A \not\subseteq P^{k+1}.$$

Satz 10.13. Sei P ein Primideal und seien A, B Ideale in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$ und $\{0\} \neq B \neq \mathcal{O}_K$. Dann gilt:

1) $\mathrm{ord}_P(P) = 1$;

2) $\mathrm{ord}_P(P') = 0$ falls $P' \neq P$ ein Primideal ist;

3) $\mathrm{ord}_P(AB) = \mathrm{ord}_P(A) + \mathrm{ord}_P(B)$.

Satz 10.14. Sei A ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$. Dann kann A in der Form

$$A = P_1^{n_1} P_2^{n_2} \dots P_k^{n_k}$$

geschrieben werden, wobei $P_1, \dots, P_k$ verschiedene Primideale in $\mathcal{O}_K$ sind und $n_1, \dots, n_k \in \mathbb{N}$ ist. Diese Zerlegung ist eindeutig bis zu einer Permutation von $P_1, \dots, P_k$. Außerdem gilt $n_i = \mathrm{ord}_{P_i}(A)$ für alle i.

Beweis. Die Existenz der Zerlegung wurde im Satz 10.10 formuliert. Die Eindeutigkeit folgt (mit Hilfe des Satzes 10.13) aus der Formel

$$\mathrm{ord}_{P_i}(A) = \sum_{j=1}^{k} \big(n_j \cdot \mathrm{ord}_{P_i}(P_j)\big) = n_i.$$

Aufgabe. Sei $K = \mathbb{Q}(\sqrt[3]{5})$. Zerlegen Sie das Hauptideal (3) in $\mathcal{O}_K$ in Primideale.

Lösung. Sei $\alpha = \sqrt[3]{5}$. Wir prüfen nach, dass das Folgende gilt:
1) $(3) = (3, 1+\alpha)^3$;
2) $(3, 1+\alpha)$ ist ein Primideal in $\mathcal{O}_K$.

Zu 1): Es gilt $(3, 1+\alpha)^2 = (9, 3+3\alpha, 1+2\alpha+\alpha^2)$. Daraus folgt

$$\begin{aligned}
(3, 1+\alpha)^3 &= (27, 9+9\alpha, 3+6\alpha+3\alpha^2, 1+3\alpha+3\alpha^2+\alpha^3)\\
&= (27, 9+9\alpha, 3+6\alpha+3\alpha^2, 6+3\alpha+3\alpha^2)\\
&= (27, 9+9\alpha, 3+6\alpha+3\alpha^2, 3-3\alpha)\\
&= (27, 9+9\alpha+3[3-3\alpha], 3+6\alpha+3\alpha^2, 3-3\alpha)\\
&= (27, 18, 3+6\alpha+3\alpha^2, 3-3\alpha)\\
&= (9, 3+6\alpha+3\alpha^2, 3-3\alpha)\\
&= (9, 3+6\alpha+3\alpha^2+[\alpha+3][3-3\alpha], 3-3\alpha)\\
&= (9, 12, 3-3\alpha)\\
&= (3, 3-3\alpha)\\
&= (3).
\end{aligned}$$

Zu 2): Wir zeigen, dass der Faktorring $\mathcal{O}_K/(3, 1+\alpha)$ genau 3 Elemente enthält. Dann wird das Ideal $(3, 1+\alpha)$ maximal und somit prim in $\mathcal{O}_K$.

Wir wissen aus dem Übungsblatt 8, dass das Folgende gilt:

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2.$$

Jedes Element $\gamma \in \mathcal{O}_K$ mit Hilfe von $1+\alpha$ kann bis zu einer Zahl $n \in \mathbb{Z}$ "vereinfacht" werden. Die weitere Vereinfachung bis zu einer der Zahlen 0,1,2 erfolgt mit Hilfe von 3. Die Zahlen $0, 1, 2$ liegen in verschiedenen Nebenklassen modulo $(3, 1+\alpha)$, sonst liegt 1 in $(3, 1+\alpha)$, dann wäre $(3, 1+\alpha) = \mathcal{O}_K$, was aber unmöglich ist wegen 1).

11 Verzweigungsindex und Grad eines Primideals

Sei K ein Zahlkörper und sei $\mathcal{O}_K$ der Ganzheitsring von K.

Definition 11.1. Sei A ein Ideal in $\mathcal{O}_K$. Dann heißt die Zahl

$$N(A) := |\mathcal{O}_K/A|$$

Norm des Ideals A.

Lemma 11.2. Sei $\mathbb{P}$ ein Primideal in $\mathcal{O}_K$. Dann ist $\mathbb{P}\cap\mathbb{Z} = p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{N}$.

In dem Fall sagt man, dass $\mathbb{P}$ *über p liegt.*

Lemma 11.3. Sei $\mathbb{P}$ ein Primideal, das über einer Primzahl $p \in \mathbb{N}$ liegt. Dann ist

$$N(\mathbb{P}) = p^f$$

für eine Zahl $f \in \mathbb{N}$. Diese f heißt *Grad von* $\mathbb{P}$.

Lemma 11.4. Sei $p \in \mathbb{Z}$ eine Primzahl und sei $(p) = \mathbb{P}_1^{e_1}\mathbb{P}_2^{e_2}\dots\mathbb{P}_k^{e_k}$ die Zerlegung des Ideals (p) von $\mathcal{O}_K$ in Primideale. Dann sind $\mathbb{P}_i$ genau die Primideale von $\mathcal{O}_K$, die über p liegen.

Die Zahl e_i heißt *Verzweigungsindex von* $\mathbb{P}_i$ *über* p.

Satz 11.5. (Fundamentalsatz) Sei K ein Zahlkörper mit $n = [K : \mathbb{Q}]$. Sei $p \in \mathbb{N}$ eine Primzahl und sei $(p) = \mathbb{P}_1^{e_1}\mathbb{P}_2^{e_2}\dots\mathbb{P}_k^{e_k}$ die Zerlegung des Ideals (p) von $\mathcal{O}_K$ in Primideale. Dann gilt

$$n = e_1f_1 + \cdots + e_kf_k.$$

Dieser Satz wird mit Hilfe der folgenden Aussagen bewiesen.

Lemma 11.6. (Chinesischer Restklassensatz) Sei R ein kommutativer Ring mit 1. Seien $A_1, A_2, \dots, A_k$ Ideale in R, so dass $A_i + A_j = R$ für alle $i \neq j$ ist. Dann gilt

$$R/A_1A_2\dots A_k \cong R/A_1 \oplus \cdots \oplus R/A_k.$$

Folgerung 11.7. Seien $\mathbb{P}_1, \mathbb{P}_2, \dots, \mathbb{P}_k$ verschiedene Primideale in $\mathcal{O}_K$ und seien $e_1, e_2, \dots, e_k$ natürliche Zahlen. Dann gilt

$$N(\mathbb{P}_1^{e_1}\mathbb{P}_2^{e_2}\dots\mathbb{P}_k^{e_k}) = N(\mathbb{P}_1^{e_1})N(\mathbb{P}_2^{e_2})\dots N(\mathbb{P}_k^{e_k}).$$

Lemma 11.8. Sei $\mathbb{P}$ ein Primideal in $\mathcal{O}_K$ und sei $e \in \mathbb{N}$. Dann gilt

$$N(\mathbb{P}^e) = (N(\mathbb{P}))^e.$$

Lemma 11.9. Sei K ein Zahlkörper mit $n = [K : \mathbb{Q}]$. Sei $p \in \mathbb{N}$ und sei (p) das Ideal in $\mathcal{O}_K$, das von p erzeugt ist. Dann gilt

$$N((p)) = p^n.$$

12 Eine Anwendung der Idealklassengruppe

Satz 12.1. Die Gleichung $y^2 = x^3 - 5$ hat keine ganzzahligen Lösungen.

13 Einheitsgruppe $\mathcal{O}_K^*$

Die Definition der Einheitsgruppe R^* eines kommutativen Ringes R mit 1 wurde in Definition 6.1.2) gegeben.

Satz 13.1. (Dirichletscher Einheitssatz) Sei K ein Zahlkörper. Dann existieren Zahlen $\alpha, \beta_1, \dots, \beta_n$ in der Einheitsgruppe $\mathcal{O}_K^*$, so dass das Folgende gilt:

1) α hat eine endliche Ordnung m;
2) $\beta_1, \dots, \beta_n$ haben unendliche Ordnungen;
3) jede Zahl $\gamma \in \mathcal{O}_K^*$ kann eindeutig in der Form $\gamma = \alpha^i \beta_1^{j_1} \dots \beta_n^{j_n}$ mit $i, j_1, \dots, j_n \in \mathbb{Z}$ und $0 \leqslant i < m$ geschrieben werden.

Mit anderen Worten ist $\mathcal{O}_K^* \cong \mathbb{Z}_m \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n}$. Außerdem gilt:

(a) m ist die maximale natürliche Zahl, für die $e^{\frac{2\pi i}{m}} \in K$ gilt.

(b) $n = r + s - 1$, wobei

(b1) r die Anzahl von reellen Einbettungen $K \to \mathbb{R}$ ist,

(b2) s die Anzahl der Paare von zueinander konjugierten nicht reellen Einbettungen $K \to \mathbb{C}$ ist.

Satz 13.2. Für jede irrationale Zahl α existieren unendlich viele Paare $(x, y) \in \mathbb{Z}^2$ mit

$$\left| \frac{x}{y} - \alpha \right| < \frac{1}{y^2}.$$

Satz 13.3. Sei $d > 1$ eine quadratenfreie natürliche Zahl. Dann hat die Gleichung

$$x^2 - dy^2 = 1$$

unendlich viele Lösungen $(x, y) \in \mathbb{Z}^2$. Außerdem existiert eine solche ganzzahlige Lösung (x_1, y_1) mit $x_1 > 0$, $y_1 > 0$, so dass jede ganzzahlige Lösung die Form $\pm(x_n, y_n)$ hat, wobei $x_n + \sqrt{d} y_n = (x_1 + \sqrt{d} y_1)^n$ mit $n \in \mathbb{Z}$ ist.

Folgerung 13.4. Sei $K = \mathbb{Q}(\sqrt{d})$, wobei d eine quadratenfreie natürliche Zahl ist.

1) Wenn $d > 1$ ist, dann gilt $\mathcal{O}_K^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}$.
2) Wenn $d \leqslant -1$ ist, dann ist $\mathcal{O}_K^*$ eine endliche zyklische Gruppe. Genauer:

2.1) Für $d = -1$ ist $\mathcal{O}_K^* = \{\pm 1, \pm i\}$;

2.2) Für $d = -3$ ist $\mathcal{O}_K^* = \{\pm 1, \pm \omega, \pm \omega^2\}$, wobei $\omega = \frac{-1+i\sqrt{3}}{2}$ ist;

2.3) Für $d = -2$ und für $d < -3$ ist $\mathcal{O}_K^* = \{\pm 1\}$;