Skriptum zur Vorlesung
Algebra II
Sommersemester 2004

Prof. Dr. Helmut Maier

Inhaltsverzeichnis

4. Endliche Körper und Kreisteilungskörper

4.1. Einheitswurzeln und Kreisteilungskörper

DEFINITION 4.1.1
Sei K ein Körper und $n \in \mathbb{N}$. Ein Zerfällungskörper des Polynoms $X^n - 1$ über K wird mit $K^{(n)}$ bezeichnet und n-ter Kreisteilungskörper über K genannt. Die Nullstellen von $X^n - 1$ heißen die n-ten Einheitswurzeln von K, und ihre Menge wird mit $E^{(n)}$ bezeichnet. Wenn $K = K^{(n)}$ ist sagt man, dass K alle n-ten Einheitswurzeln enthält.

BEISPIEL 4.1.1
Zu jedem $n \in \mathbb{N}$ enthält $\mathbb{C}$ die n-ten Einheitswurzeln. Durch sie wird die Peripherie des Einheitskreises in n Stücke gleicher Länge geteilt, daher der Name „Kreisteilungskörper".

BEISPIEL 4.1.2
Ein beliebiger Körper K enthält stets die zweiten Einheitswurzeln, nämlich 1 und -1.

Für das Weitere denken wir uns zu K und n einen Kreisteilungskörper $K^{(n)}$ stets fest gewählt. Ist $m|n$, so sind offenbar alle m-ten Einheitswurzeln auch n-te Einheitswurzeln und damit in $K^{(n)}$ enthalten. Um auch den Fall $\mathrm{char}(K) = p$ mit p Primzahl behandeln zu können, betrachten wir einen speziellen Monomorphismus in solchen Körpern. Im Hinblick auf spätere Anwendungen dehnen wir den Begriff der Charakteristik auf beliebige Ringe aus:

DEFINITION 4.1.2
Die Charakteristik $\mathrm{char}(R)$ eines Rings R ist die kleinste natürliche Zahl n, so dass für $1 \in R$ die n-fache Summe $1 + \cdots + 1$ im Ring R die Null ergibt. Falls es kein solches n gibt setzt man $\mathrm{char}(R) = 0$.

BEMERKUNG 4.1.1
Man sieht leicht, dass Definition 4.1.2 die Definition 3.1.3 (R ist ein Körper) als Spezialfall enthält.

SATZ 4.1.1
Es sei R ein Integritätsring, dann gilt:

(a) *Die Charakteristik von R ist 0 oder eine Primzahl p.*
(b) *Ist $\mathrm{char}(R) = p \neq 0$, so ist die Abbildung*

$$\phi = \begin{cases} R & \to & R \\ a & \mapsto & a^p \end{cases}$$

ein Ringmonomorphismus. Ist R ein Körper, so ist $\phi(R)$ ein Unterkörper von R.

BEWEIS
Teil a) wird bewiesen wie die entsprechende Aussage für Körper in Satz 3.1.1. Zu b): Für $j \in \mathbb{Z}$ und $a \in R$ sei $j \cdot a$ das Element $\Phi(j) \cdot a$ mit dem Ringhomomorphismus $\Phi : \mathbb{Z} \to R$ aus Satz 3.1.1. In jedem kommutativen Ring R lässt sich durch vollständige Induktion der binomische Lehrsatz beweisen:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \text{ mit } a, b \in R,\ n \in \mathbb{N}\,.$$

Insbesondere gilt für $a, b \in R$ mit $n = p$:

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p\,.$$

Für $1 \leq k \leq p-1$ ist jedoch

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

durch p teilbar, also Null in R. Es folgt $(a+b)^p = a^p + b^p$. Zusammen mit $(ab)^p = a^p b^p$ folgt die Relationstreue von ϕ. Wegen der Integrität von R gilt $a^p = 0 \Leftrightarrow a = 0$, d. h. es ist $\mathrm{Ker}(\phi) = \{0\}$, und ϕ ist ein Monomorphismus. Ist R ein Körper, so folgt ebenso, dass $\phi(R)$ ein Unterkörper von K ist. □

Satz 4.1.2
Es sei $p = \mathrm{char}(K)$ und $n \in \mathbb{N}$ beliebig:

(1) *Gilt $p|n$, also $n = mp^l$ mit $m, l \in \mathbb{N}$ und $p \nmid m$, so ist jede n-te Einheitswurzel in K eine m-te.*
(2) *Gilt $p \nmid n$, so ist $E^{(n)}$ mit der Multiplikation in $K^{(n)}$ eine zyklische Gruppe der Ordnung n.*

Beweis
Zu 1): Es ist p eine Primzahl. Nach Satz 4.1.1 ist die Abbildung $\psi : K \to K,\ a \mapsto a^{p^l}$ als l-te Potenz von $\phi :\ a \mapsto a^p$ ein Ringmonomorphismus, d. h. injektiv. Für $\zeta \in E^{(n)}$ gilt $\psi(\zeta^m) = (\zeta^m)^{p^l} = 1_K = \psi(1)$, was nur für $\zeta^m = 1_K$ möglich ist. Zu 2): $X^n - 1$ und seine formale Ableitung nX^{n-1} sind wegen $p \nmid n$ teilerfremd. Nach Satz 3.5.1 ist $X^n - 1$ separabel und besitzt im zugehörigen Zerfällungskörper $K^{(n)}$ genau n verschiedene Nullstellen, d. h. $|E^{(n)}| = n$. Mit $\zeta, \eta \in E^{(n)}$ folgt stets $(\zeta\eta^{-1})^n = \zeta^n \cdot (\eta^n)^{-1} = 1_K$ und damit $\zeta\eta^{-1} \in E^{(n)}$. Da K ein Körper ist hat für $d \in \mathbb{N}$ die Gleichung $x^d = 1_K$ höchstens d Lösungen $x \in E^{(n)}$. Nach Satz 2.5.9 ist $E^{(n)}$ zyklisch. □

Definition 4.1.3
Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Ein erzeugendes Element der zyklischen Gruppe $E^{(n)}$ heißt eine primitive n-te Einheitswurzel über K.

Satz 4.1.3
Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann gibt es genau $\varphi(n)$ verschiedene primitive n-te Einheitswurzeln. Ist ζ_n eine von ihnen, so sind die anderen gegeben durch ζ_n^k mit $1 \le k \le n$ und $\mathrm{ggT}(n,k) = 1$.

Beweis
Das folgt aus den Sätzen 4.1.2 und 2.5.8. □

Definition 4.1.4
Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $\zeta_n \in K^{(n)}$ eine n-te primitive Einheitswurzel über K. Das Polynom

$$\Phi_n(X) \ = \prod_{\substack{j=1 \\ \mathrm{ggT}(j,n)=1}}^{n} (X - \zeta_n^j) \ \in \ K^{(n)}[X]$$

heißt das n-te Kreisteilungspolynom über K.

Satz 4.1.4
Es sei P der Primkörper von K und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Dann ist $\Phi_n(X) \in P[X]$. Ist $P = \mathbb{Q}$, so gilt sogar $\Phi_n(X) \in \mathbb{Z}[X]$.

Beweis
Es bezeichne $E_d^{(n)}$ die Menge aller Elemente von $E^{(n)}$ der Ordnung d. Dann ist

$$E^{(n)} \ = \bigcup_{d|n} E_d^{(n)}$$

eine Partition von $E^{(n)}$. Wegen $d|n$ enthält $E^{(n)}$ alle d-ten Einheitswurzeln, folglich ist $E_d^{(n)}$ die Menge der d-ten primitiven Einheitswurzeln aus $E^{(n)}$. Daher gilt

$$(*)\ X^n - 1 \ = \prod_{\omega \in E^{(n)}} (X - \omega) \ = \prod_{d|n} \prod_{\omega \in E_d^{(n)}} (X - \omega) \ = \prod_{d|n} \Phi_d(X)\,.$$

Wir beweisen nun die Behauptung des Satzes durch Induktion nach n. Für $n = 1$ ist $\Phi_1(X) = X - 1$. Es sei $n > 1$ und die Behauptung für alle $d < n$ bewiesen. Dann folgt $(*)$ aus

$$\Phi_n(X) \cdot f(X) \;=\; X^n - 1 \quad , \quad f(X) \;=\; \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$

mit $f(X) \in P[X]$ nach Induktionsvoraussetzung (für $P = \mathbb{Q}$ sogar $f(X) \in \mathbb{Z}[X]$). Das Polynom $\Phi_n(X)$ kann aus $X^n - 1$ und $f(X)$ mittels „langer Division“gewonnen werden. Da der Divisor $f(X)$ normiert ist und seine Koeffizienten in P (für $P = \mathbb{Q}$ sogar in $\mathbb{Z}$) liegen, sieht man, dass dies auch für alle in der Division auftretenden Koeffizienten der Fall ist. □

Beispiel 4.1.3
Es sei $K = \mathbb{Q}$ und p eine Primzahl. Dann ist

$$\Phi_p(X) \;=\; \frac{X^p - 1}{X - 1} \;=\; 1 + X + X^2 + \cdots + X^{p-1} \,.$$

Für $n = 6$ ist dagegen

$$\Phi_6(X) \;=\; \frac{X^6 - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} \;=\; \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} \;=\; X^2 - X + 1 \,.$$

Lemma 4.1.5
Es sei R ein faktorieller Ring mit Quotientenkörper Q. Es seien $f, h \in R[X]$ und f primitiv. Gilt $f|h$ in $Q[X]$, dann auch $f|h$ in $R[X]$.

Beweis
Es sei $h(X) = f(X)g(X)$ mit $f \in R[X]$ und $g \in Q[X]$. Dann gibt es ein $\gamma \in Q$, so dass $\gamma \cdot g(X) \in R[X]$ und primitiv ist. Also $\gamma \cdot h(X) = f(X) \cdot (\gamma g(X))$. Damit ist $\gamma \cdot h(X) \in R[X]$ und nach Satz 2.4.6 (Gauß) ist $\gamma \cdot h(X)$ primitiv, woraus $\gamma \in R^*$ folgt. Damit gilt $h(X) = f(X) \cdot (\gamma^{-1} g(X))$ mit $\gamma^{-1} g(X) \in R[X]$, d. h. $f|h$ in $R[X]$. □

Satz 4.1.6
Für alle $n \in \mathbb{N}$ ist das n-te Kreisteilungspolynom $\Phi_n(X)$ über dem Körper $\mathbb{Q}$ irreduzibel in $\mathbb{Q}[X]$.

Beweis
Nach Lemma 2.4.7 genügt es, die Irreduzibilität von $\Phi_n(X)$ in $\mathbb{Z}[X]$ zu zeigen. Wir nehmen das Gegenteil an: Es sei

$$(1) \quad \Phi_n(X) \;=\; f(X) \cdot g(X)$$

mit einem irreduziblen (und damit primitiven) $f(X) \in \mathbb{Z}[X]$ und irgend einem $g(X) \in \mathbb{Z}[X]$. Es sei ζ_n eine Nullstelle von $f(X)$ in $\mathbb{Q}^{(n)}$ und p eine Primzahl mit $p \nmid n$. Behauptung:

$$(2) \quad \zeta_n^p \text{ ist ebenfalls Nullstelle von } f(X) \,.$$

Wir nehmen wieder das Gegenteil an und setzen

$$X^n - 1 \;=\; f(X) \cdot c(X)$$

mit einem normierten $c(X) \in \mathbb{Z}[X]$. Dann ist ζ_n^p Nullstelle von $c(X)$, damit ζ_n Nullstelle des Polynoms $c(X^p)$. Nach Satz 3.2.2(b) gilt $f(X)|c(X^p)$ in $\mathbb{Q}[X]$, und wegen der Primitivität von $f(X)$ nach Lemma 4.1.5 sogar $f(X)|c(X^p)$ in $\mathbb{Z}[X]$, also

$$(3) \quad c(X^p) \;=\; f(X) \cdot h(X)$$

für ein $h(X) \in \mathbb{Z}[X]$. Es sei Y eine Unbestimmte über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Nach Definition 2.3.1 für den Polynomring und Satz 2.3.1 lässt sich der Homomorphismus

$$\psi \;=\; \begin{cases} \mathbb{Z} & \to & \mathbb{F}_p \\ a & \mapsto & a \bmod p \end{cases}$$

fortsetzen zu einem Homomorphismus

$$\Psi \;=\; \begin{cases} \mathbb{Z}[X] & \to & \mathbb{F}_p[X] \\ \sum a_j X^j & \mapsto & \sum (a_j \bmod p) Y^j \end{cases} .$$

Wir schreiben kurz $\bar{a}$ für $a \bmod p$ sowie $\bar{f}$ für $\Psi(f)$. Indem wir Ψ auf (1) und (3) anwenden, erhalten wir

$$\bar{\Phi}_n(Y) \;=\; \bar{f}(Y) \cdot \bar{g}(Y) \quad , \quad \bar{c}(Y^p) \;=\; \bar{f}(Y) \cdot \bar{h}(Y) \, .$$

Nach Satz 4.1.1(b) ist die Abbildung

$$\mathbb{F}_p[Y] \;\to \mathbb{F}_p[Y] \quad , \quad \bar{a}(Y) \;\mapsto \bar{a}(Y)^p$$

ein Monomorphismus. Nach Satz 2.5.7(b) („kleiner Fermat“) gilt außerdem $\bar{a}^p = \bar{a}$ für alle $\bar{a} \in \mathbb{F}_p$, somit $\bar{c}(Y)^p = \bar{c}(Y^p)$, womit in Verbindung mit (3) folgt:

$$(4) \quad (\bar{c}(Y))^p \;=\; \bar{f}(Y) \cdot \bar{h}(Y) \, .$$

Es sei nun $\bar{b}(Y)$ irgend ein irreduzibler Faktor von $\bar{f}(Y)$ in $\mathbb{F}_p[Y]$. Aus (4) folgt $\bar{b}(Y) | \bar{c}(Y)$ in $\mathbb{F}_p[Y]$, und aus (1) und $p \geq 2$ folgt

$$\bar{b}(Y)^2 | \bar{\Phi}_n(Y) \, .$$

Wegen $\bar{\Phi}_n(Y) | (Y^n - \bar{1})$ folgt

$$(5) \quad \bar{b}(Y)^2 | (Y^n - \bar{1}) \, .$$

Die formale Ableitung von $Y^n - \bar{1}$ ist jedoch $\bar{n} Y^{n-1}$, wegen $p \nmid n$ ist $\bar{n} \neq \bar{0}$, d. h. $Y^n - \bar{1}$ und $\bar{n} Y^{n-1}$ sind in $\mathbb{F}_p[Y]$ teilerfremd. Damit ist $Y^n - \bar{1}$ nach Satz 3.5.1 separabel und besitzt keine mehrfachen Nullstellen im Kreisteilungskörper über $\mathbb{F}_p$ im Widerspruch zu (5). Damit ist Behauptung (2) bewiesen: ζ_n^p ist Nullstelle von $f(X)$. Es sei nun $\eta = \zeta_n^m$ mit $\mathrm{ggT}(m, n) = 1$ eine beliebige Nullstelle von $\Phi_n(X)$ in $\mathbb{Q}^{(n)}$. Es ist $m = p_1 \cdots p_r$ mit Primzahlen $p_j \nmid n$. Damit ist nach (2) auch $\zeta_n^{p_1}$ Nullstelle von $f(X)$. Sukzessive folgt, dass auch $(\zeta_n^{p_1})^{p_2}$ Nullstelle ist, usw.. Schließlich ist $\eta = \zeta_n^{p_1 \cdots p_r}$ Nullstelle von $f(X)$. Da η eine beliebige primitive n-te Einheitswurzel ist folgt $f(X) = \Phi_n(X)$ und damit, dass $\Phi_n(X)$ irreduzibel ist. □

Definition 4.1.5
Für $n \in \mathbb{N}$ und $\alpha \in K$ bezeichne $\sqrt[n]{\alpha}$ irgend eine (jeweils fest gewählte) Nullstelle von $X^n - \alpha$ in einem Zerfällungskörper über K. Man nennt $\sqrt[n]{\alpha}$ eine n-te Wurzel von α über K, oder ein Radikal vom Exponenten n über K. Ist $X^n - \alpha$ irreduzibel in $K[X]$, so heißt $\sqrt[n]{\alpha}$ irreduzibles Radikal über K.

Das Symbol $\sqrt[n]{\alpha}$ ist im allgemeinen mehrdeutig und muss daher bei der jeweiligen Anwendung fixiert werden. Der nächste Satz gibt eine Aussage über das Ausmaß der Mehrdeutigkeit:

Satz 4.1.7
Es sei $p = \mathrm{char}(K)$ und $\alpha \in K^* = K - \{0\}$. Für ein $n \in \mathbb{N}$ sei $n = k \cdot p^e$ mit $p \nmid k$ falls $p \neq 0$ ist oder $n = k$ für $p = 0$. Ferner sei L ein Zerfällungskörper von $X^n - \alpha$ über K und $\sqrt[n]{\alpha} \in L$ fest gewählt. Dann enthält L alle k-ten Einheitswurzeln, und sämtliche verschiedenen n-ten Wurzeln von α über K liegen in L und sind gegeben durch $\sqrt[n]{\alpha} \cdot \zeta^j$ für $j = 0 \ldots k-1$, wobei ζ eine primitive k-te Einheitswurzel in L bezeichnet. Insbesondere ist $L = K(\sqrt[n]{\alpha}, \zeta)$.

Beweis
Es sei $\beta = \sqrt[n]{\alpha}$. Da das Polynom $f(X) = X^n - \alpha \in K[X]$ in $L[X]$ linear zerfällt, tut es auch

$$\alpha^{-1} \cdot f(\beta X) \;=\; X^n - 1 \, .$$

Nach Satz 4.1.2 sind die verschiedenen Nullstellen von $X^n - 1$ gegeben durch ζ^j mit $j = 0 \ldots k-1$ (für eine primitive k-te Einheitswurzel $\zeta \in L$), die damit sämtlich in L liegen. Folglich sind die Nullstellen von $f(X)$ die Elemente $\beta \cdot \zeta^j$. □

4.2. Endliche Körper

Satz 4.2.1
Es sei K ein endlicher Körper mit $|K| = q$ Elementen, dann gilt:

(a) *Es ist q eine Primzahlpotenz: $q = p^n$ mit $p, n \in \mathbb{N}$ und p Primzahl.*
(b) *Sei $q = p^n$ eine beliebige Primzahlpotenz, dann gibt es bis auf Isomorphie genau einen Körper mit q Elementen.*

Wir beweisen Satz 4.2.1 zusammen mit dem nächsten Satz. Vorher geben wir folgende

Definition 4.2.1
Es sei $q = p^n$ eine Primzahlpotenz. Der nach Satz 4.2.1(b) bis auf Isomorphie eindeutig bestimmte endliche Körper mit q Elementen wird mit $\mathbb{F}_q$ bezeichnet.

Satz 4.2.2
Es sei $q = p^n$ eine Primzahlpotenz. Der Körper $\mathbb{F}_q$ hat die folgenden Eigenschaften:

(a) *Für den Primkörper P von $\mathbb{F}_q$ gilt: $P \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, und es ist* $\mathrm{char}(\mathbb{F}_q) = p$.
(b) *$\mathbb{F}_q$ ist Zerfällungskörper des Polynoms $X^q - X$ über P und dessen Nullstellenmenge.*
(c) *Die Einheitengruppe $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ ist eine zyklische Gruppe der Ordnung $q-1$. Insbesondere ist $\mathbb{F}_q$ ein $(q-1)$-ter Kreisteilungskörper über seinem Primkörper $\mathbb{F}_p$.*

Beweis
Zu a): Es sei $|K| = p^n$. Nach Satz 3.1.1 muss $\mathrm{char}(K) \neq 0$ sein, da der Primkörper sonst isomorph zu $\mathbb{Q}$ und damit $|K| = \infty$ wäre. Also ist $\mathrm{char}(K) = p$, und die Aussage a) ist in Satz 3.1.1(a) enthalten. Wegen $|K| < \infty$ muss $[K : P] = n < \infty$ sein. Sei $B = \{x_1, \ldots, x_n\}$ eine Basis von K als P-Vektorraum, so ist

$$K \;=\; \left\{ \sum_{j=1}^{n} a_j x_j \mid a_j \in P \right\}$$

die eindeutige Darstellung aller Elemente von K bzgl. B, daraus folgt $|K| = p^n$. Zu b): Nach Satz 1.7.3(c) ist $X^{q-1} = 1_K$ für alle $x \in K^*$ da K^* bzgl. der Multiplikation eine Gruppe der Ordnung $q-1$ bildet. Es sei $f(X) = X^q - X \in P[X]$. Dann ist $f(x) = 0$ für alle $x \in K$, also

$$f(X) \;=\; \prod_{x \in K} (X - x)\,.$$

Insbesondere ist K die Nullstellenmenge und ein Zerfällungskörper von $f(X)$ über P. Da ein solcher Zerfällungskörper nach Satz 3.4.3 bis auf Isomorphie eindeutig bestimmt ist, ist auch K bereits durch die Elementanzahl $q = p^n$ bis auf Isomorphie festgelegt. K ist auch der Zerfällungskörper von $X^{q-1} - 1$ über P und somit ein $(q-1)$-ter Kreisteilungskörper. Der Rest von c) folgt aus Satz 4.1.2(b). □

5. Galoistheorie

5.1. Der Satz vom primitiven Element

Wir geben in diesem Kapitel zunächst eine ausführliche Behandlung der Galoistheorie, die in der Vorlesung Algebra I nur angeschnitten werden konnte. Danach werden wir einige Anwendungen aufzeigen. Als Voraussetzung brauchen wir den Satz vom primitiven Element.

Definition 5.1.1
Es sei L/K eine Körpererweiterung. Ein $\alpha \in L$ heißt primitives Element von L/K, falls $L = K(\alpha)$ ist.

Satz 5.1.1 (Satz vom primitiven Element)
Es sei L/K eine endliche Körpererweiterung mit $L = K(\alpha_1, \ldots, \alpha_n)$. Sind $\alpha_2, \ldots, \alpha_n$ jeweils separabel über K, so ist L/K einfach. Speziell sind alle endlichen separablen Erweiterungen einfach.

Beweis
Ist K endlich, so ist L nach Satz 4.2.2(c) ein Kreisteilungskörper, nach Satz 4.1.2 ist L/K dann einfach. Wir können also im Folgenden voraussetzen, dass L unendlich viele Elemente enthält. Weiter genügt es, den Fall $n = 2$ zu behandeln, da der allgemeine Fall daraus durch Induktion nach n folgt. Es genügt also zu zeigen: Ist $L = K(\alpha, \beta)$ algebraisch über K und ist β separabel über K, so ist L/K einfach. Es sei $f(X)$ das Minimalpolynom von α über K sowie $g(X)$ das Minimalpolynom von β. In einem Zerfällungskörper Z von $f(X) \cdot g(X)$ über K liege der Zerfall

$$f(X) \;=\; \prod_{i=1}^{r}(X - \alpha_i) \quad , \quad g(X) \;=\; \prod_{i=1}^{s}(X - \beta_i)$$

mit den Konjugierten α_i bzw. β_i und $\alpha = \alpha_1$ bzw. $\beta = \beta_1$ vor. Nach Voraussetzung ist $\beta_j \neq \beta_1$ für $2 \leq j \leq s$. Die Gleichung

$$\alpha_i + \beta_j x \;=\; \alpha_1 + \beta_1 x$$

hat für $1 \leq i \leq r$ und $2 \leq j \leq s$ höchstens eine Lösung $x \in K$. Weil K unendlich viele Elemente enthält, gibt es ein $c \in K$ mit

$$\alpha_i + \beta_j c \;\neq\; \alpha_1 + \beta_1 c$$

für alle $1 \leq i \leq r$ und $2 \leq j \leq s$. Wir setzen $\gamma = \alpha + c\beta \in L$. Wegen $g(\beta) = 0$ und $f(\gamma - c\beta) = 0$ ist β eine gemeinsame Nullstelle von $g(X)$ und $f(\gamma - cX) \in (K(\gamma))[X]$. Nach Wahl von c ist β die einzige gemeinsame Nullstelle dieser Polynome im Zerfällungskörper Z. Weil β nach Voraussetzung eine einfache Nullstelle von $g(X)$ ist, gilt

$$X - \beta \;=\; \mathrm{ggT}_{Z[X]}(g(X), f(\gamma - cX)) \,.$$

Wegen $g(X), f(\gamma - cX) \in K(\gamma)[X]$ liegt auch der ggT in $K(\gamma)[X]$. Somit ist $\beta \in K(\gamma)$ und damit auch $\alpha = \gamma - c\beta$. Folglich ist $K(\gamma) \supseteq L = K(\alpha, \beta)$, woraus $L = K(\gamma)$ und damit die Einfachheit von L/K mit dem primitiven Element $\gamma \in L$ folgt. □

Lemma 5.1.2
Es sei L/K eine separable Körpererweiterung, so dass $\deg(\alpha) = [K(\alpha) : K] \leq n$ ist für ein $n \in \mathbb{N}$ und alle $\alpha \in L$. Dann ist $[L : K] \leq n$.

Beweis
Sei $\alpha \in L$ beliebig mit $\deg(\alpha) \leq n$ maximal. Angenommen $L \neq K(\alpha)$, dann gibt es ein $\beta \in L - K(\alpha)$ mit $[K(\alpha, \beta) : K] > [K(\alpha) : K]$. Da L aber separabel über K ist, gibt es ein primitives Element $\gamma \in L$, das $K(\alpha, \beta)$ erzeugt. Wegen $[K(\alpha, \beta) : K] > [K(\alpha) : K]$ ist dann $\deg(\gamma) > \deg(\alpha)$ im Widerspruch zur Wahl von α. □

5.2. Der Hauptsatz der Galoistheorie

Wir erinnern an die Definition der galoisschen Körpererweiterungen (Definition 3.3.5):

Definition 5.2.1
Eine Körpererweiterung L/K heißt galoissch, wenn $L^G = K$ ist für eine endliche Untergruppe $G \leq G(L/K)$.

Wir erinnern an die Charakterisierung der galoisschen Erweiterungen (Satz 3.6.1) und geben jetzt einen Beweis für diese Aussage.

Satz 5.2.1
Eine Erweiterung L/K ist genau dann galoissch, wenn sie endlich, normal und separabel ist.

Beweis
Hinrichtung: Es sei L/K endlich, normal und separabel sowie $Z = L^{G(L/K)}$ der zur vollen Automorphismengruppe gehörende Fixkörper. Nach den Sätzen 3.2.1, 3.4.6 und 3.5.3 ist auch L/Z eine Erweiterung, die endlich, normal und separabel ist. Nach Satz 3.5.5 gilt

$$[L : K] \;=\; |G(L/K)| \;=\; |G(L/Z)| \;=\; [L : Z]\,.$$

Also ist $Z = L^{G(L/K)} = K$ und L/K galoissch. Rückrichtung: Es sei $K = L^G$ für eine endliche Untergruppe $G \leq G(L/K)$. Für $\alpha \in L$ seien $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ die verschiedenen Elemente der Menge $G \circ \alpha = \{\sigma(\alpha) \mid \sigma \in G\}$. Wir betrachten das Polynom

$$(1) \quad f(X) \;=\; \prod_{j=1}^{n}(X - \sigma_j(\alpha)) \;=\; X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \;\in\; L[X]\,.$$

Mit jedem $\sigma \in G$ ist auch $G \circ \alpha = \{(\sigma \circ \sigma_1)(\alpha), \ldots, (\sigma \circ \sigma_n)(\alpha)\}$, da mit σ_i auch $\sigma \circ \sigma_i$ alle Elemente von G durchläuft. Also ist

$$f^{(\sigma)}(X) = X^n + \sigma(a_{n-1})X^{n-1} + \cdots + \sigma(a_1)X + \sigma(a_0) = \prod_{j=1}^{n}(X - \sigma(\sigma_j(\alpha))) = \prod_{j=1}^{n}(X - \sigma_j(\alpha)) = f(X).$$

Daraus folgt $\sigma(a_i) = a_i$ für alle $\sigma \in G$ und die Koeffizienten von $f(X)$, also $a_i \in L^G$. Somit ist $f(X) \in K[X]$, zudem ist $f(X)$ ein separables Polynom mit $f(\alpha) = 0$. Damit gilt $m_\alpha(X) | f(X)$ für das Minimalpolynom $m_\alpha(X)$ von α über K, d. h. auch das Minimalpolynom von α ist separabel. Da $\alpha \in L$ beliebig war, ist L separabel über L. Weiterhin gilt

$$[K(\alpha) : K] \;=\; \deg(m_\alpha(X)) \;\leq\; \deg(f) \;\leq\; |G|\,.$$

Nach Lemma 5.1.2 ist $[L : K] \leq |G|$ und L/K eine endliche Erweiterung. Es sei $g(X) \in K[X]$ irreduzibel und $\alpha \in L$ sei eine Nullstelle von $g(X)$ in L. Nach Satz 3.2.2 ist $g(X) = c \cdot m_\alpha(X)$ für ein $c \in K$ und das Minimalpolynom $m_\alpha(X)$ von α über K. Wie oben gezeigt, zerfällt $m_\alpha(X)$ und damit $g(X)$ vollständig in Linearfaktoren aus $L[X]$. Somit ist L/K nach Definition 3.4.3 eine normale Erweiterung. Damit ist Satz 5.2.1 bewiesen. □

Satz 5.2.2
Es sei L/K endlich und normal sowie Z ein Zwischenkörper $(L/Z/K)$. Dazu sei M/L eine Erweiterung von L und $\sigma : Z \to M$ ein K-Isomorphismus von Z. Dann lässt sich σ zu einem Automorphismus von L fortsetzen. Insbesondere gilt $\sigma(Z) \subseteq L$.

Beweis
Wir zeigen $\sigma(Z) \subseteq L$. Dazu wählen wir ein beliebiges $\alpha \in M$ und setzen $g(X) = m_\alpha(X)$. Dann ist auch $\sigma(\alpha)$ eine Nullstelle von $g(X)$. Wegen der Normalität von L/K zerfällt $g(X)$ in $L[X]$ linear. Folglich ist $\sigma(\alpha) \in L$. Nach Satz 3.4.5 ist L Zerfällungskörper eines Polynoms $f(X) \in K[X]$ über K, folglich auch Zerfällungskörper von $f(X)$ über M sowie von $f(X)$ über $\sigma(M)$. Daher gibt es nach Satz 3.4.4 einen Automorphismus von L, der σ fortsetzt. □

Satz 5.2.3 (Charakterisierung normaler Körpererweiterungen)
Es sei L/K endlich und M/L eine Erweiterung von L, die über K normal ist. Dann gilt: L ist normal über K genau dann, wenn jeder K-Isomorphismus von L in M ein Automorphismus ist.

Beweis
Hinrichtung: Es sei L normal über K. Nach Satz 5.2.2 (für den Spezialfall $M = L$) ist jeder K-Isomorphismus von L in M ein Automorphismus von L. Rückrichtung: Es sei $g(X)$ ein normiertes und irreduzibles Polynom in $K[X]$ mit einer Nullstelle α in L. Nach Satz 3.2.3(iii) gibt es endlich viele Elemente $\gamma_1, \ldots, \gamma_r$ mit $L = K(\gamma_1, \ldots, \gamma_r)$. Da M über K normal ist, enthält M einen Zerfällungskörper M_0 von $g(X) \cdot m_{\gamma_1}(X) \cdots m_{\gamma_r}(X)$ über K. Sei β eine beliebige Nullstelle von $g(X)$ in M_0. Nach Satz 3.3.1 existiert ein surjektiver K-Isomorphismus $\sigma : K(\alpha) \to K(\beta)$ definiert durch $\sigma(\alpha) = \beta$. Nach Satz 5.2.2 lässt sich σ zu einem Automorphismus $\hat{\sigma}$ von M_0 fortsetzen. Die Restriktion $\hat{\sigma}|_L$ ist ein K-Isomorphismus von L in M, folglich (wegen der besonderen Eigenschaft von L) ein Automorphismus von L. Insbesondere ist $\beta = \hat{\sigma}(\alpha) \in L$. Also zerfällt das beliebig gewählte $g(X)$ schon linear in L, und L ist normal über K. □

Satz 5.2.4 (Hauptsatz der Galoistheorie)
Es sei L/K eine galoissche Erweiterung, dann gilt:

(a) *Es ist $G = G(L/K)$ und $|G(L/K)| = [L : K]$. L/K ist eine endliche Erweiterung.*
(b) *Die Abbildungen*

$$\begin{array}{ccc} \{L/Z/K \text{ Zwischenk.}\} & \longleftrightarrow & \{U \leq G \text{ Untergruppe}\} \\ Z & \to & G(L/Z) \\ L^U & \leftarrow & U \end{array}$$

sind bijektiv und invers zueinander.
(c) *Für jeden Zwischenkörper $L/Z/K$ gilt:*
  (i) *L/Z ist galoissch,*
  (ii) *Z/K galoissch $\Leftrightarrow$ $\sigma(Z) = Z$ für alle $\sigma \in G(L/K)$ $\Leftrightarrow$ $G(L/Z) \leq G(L/K)$ normal.*
(d) *Ist für einen Zwischenkörper $L/Z/K$ die Erweiterung Z/K galoissch, so gilt*

$$G(Z/K) \cong G(L/K) \,/\, G(L/Z) \ .$$

(e) *Es sei $L = K(\alpha)$ einfach und $H \leq G(L/K)$ so dass*

$$\prod_{\sigma \in H} (X - \sigma(\alpha)) = \sum_{i=0}^{m} \beta_i X^i$$

gilt. Dann ist $L^H = K(\beta_0, \ldots, \beta_m)$.

Lemma 5.2.5
Es sei L/K galoissch und $L/Z/K$ ein Zwischenkörper, dann ist $G(L/\sigma(Z)) = \sigma \circ G(L/Z) \circ \sigma^{-1}$ für alle $\sigma \in G(L/K)$.

Beweis
Für $\tau \in G(L/K)$ gilt:

$$\tau \in G(L/\sigma(Z)) \Leftrightarrow \tau(\sigma(Z)) = \sigma(Z) \Leftrightarrow (\sigma^{-1}\tau\sigma)(Z) = Z \Leftrightarrow \sigma^{-1}\tau\sigma \in G(L/Z) \Leftrightarrow \tau \in \sigma G(L/Z)\sigma^{-1}.$$

□

Beweis des Hauptsatzes der Galoistheorie
Zunächst c), Teil i): Nach den Sätzen 3.2.1, 3.4.6 und 3.5.3 ist L/Z endlich, normal und separabel, nach Satz 5.2.1 ist L/Z galoissch. Teil ii): Es gilt

$$Z/K \text{ galoissch} \quad \Leftrightarrow \quad Z/K \text{ endlich, normal, separabel}$$

nach Satz 5.2.1. Nach Satz 3.2.1 ist auch Z/K endlich. Aus Definition 3.5.4 folgt, dass mit L/K auch Z/K separabel ist. Nach Satz 5.2.3 ist Z/K normal genau dann, wenn $\sigma(Z) = Z$ ist für alle $\sigma \in G(L/K)$. Es folgt

$$\begin{array}{rcl} \forall \sigma \in G(L/K) : \sigma(Z) = Z & \Leftrightarrow & \forall \sigma \in G(L/K) : G(L/\sigma(Z)) = G(L/Z) \quad \Leftrightarrow_{5.2.5} \\ \forall \sigma \in G(L/K) : G(L/Z) = \sigma \circ G(L/Z) \circ \sigma^{-1} & \Leftrightarrow & G(L/Z) \trianglelefteq G(L/K) \, . \end{array}$$

Zu a): Nach Satz 3.5.5 ist

$$(1) \quad [L : K] \; = \; |G(L/K)| \, ,$$

und nach dem Beweis von Satz 3.6.1 (Rückrichtung) ist $L^{G(L/K)} = K$. Nach dem Satz vom primitiven Element gibt es $\alpha \in L$ mit $L = K(\alpha)$. Es sei $L^G = K$ für eine Untergruppe $G \leq G(L/K)$. Dann gilt $[K(\alpha) : K] = |G|$ nach dem Beweis von Satz 5.2.1. Mit (1) folgt $G = G(L/K)$. Zu b): Es sei $L/Z/K$ ein Zwischenkörper, dann gilt:

$$\alpha \in Z \;\Rightarrow\; \forall \sigma \in G(L/Z) : \sigma(\alpha) = \alpha \;\Rightarrow\; \alpha \in L^{G(L/Z)} \;\Rightarrow\; Z \subseteq L^{G(L/Z)} \, .$$

Es sei nun $G \leq G(L/K)$ irgend eine Untergruppe, dann gilt

$$\sigma \in G \;\Rightarrow\; \forall \alpha \in L^G : \sigma(\alpha) = \alpha \;\Rightarrow\; \sigma \in G(L/L^G) \;\Rightarrow\; G \leq G(L/L^G) \, .$$

Nach a) folgt

$$(2) \quad [L : Z] \; = \; |G(L/Z)| \; \leq \; |G(L/L^{G(L/Z)})| \; = \; [L : L^{G(L/Z)}] \, ,$$

mit (1) also $L^{G(L/Z)} = Z$. Nach a) folgt

$$[L : L^G] \; = \; |G(L/L^G)| \; = \geq \; |G| \; = \; [L : L^G]$$

und damit $G(L/L^G) \; = \; G$. Insgesamt folgt Teil b). Zu d): Wir definieren einen Homomorphismus durch Restriktion:

$$\psi \; = \; \begin{cases} G(L/K) & \to & G(Z/K) \\ \sigma & \mapsto & \sigma|_Z \end{cases} \, .$$

Dann ist $\mathrm{Ker}(\psi) = \{\sigma \in G(L/K) \mid \sigma|_Z = \mathrm{id}_Z\} = G(L/Z)$. Nach dem Homomorphiesatz für Gruppen ist $G(Z/K) \cong G(L/K)/G(L/Z)$. Teil e) ist eine leichte Übungsaufgabe. □

Satz 5.2.6
Es sei L/K eine galoissche Erweiterung. Für Zwischenkörper Z_1 und Z_2 und ihre zugehörigen Gruppen $U_i = G(L/Z_i)$ gelten die Aussagen

(a) $Z_1 \subseteq Z_2 \Leftrightarrow U_1 \supseteq U_2$ *(man sagt: $U \mapsto L^U$ ist ein Antiisomorphismus bzgl. $\subseteq$).*
(b) $G(L/(Z_1 \cap Z_2)) = \langle U_1 \cup U_2 \rangle$.
(c) $G(L/Z_1 Z_2) = U_1 \cap U_2$.

Dabei ist $Z_1 Z_2 = Z_1(Z_2) = Z_2(Z_1)$ das Kompositum der Zwischenkörper in L.

Beweis
Teil a) ist trivial. Zu b): Aus $U_i \leq \langle Z_1 \cup Z_2 \rangle$ für $i = 1, 2$ folgt, dass $Z_i \supseteq L^{\langle U_1 \cup U_2 \rangle}$ gilt, also

$$Z_1 \cap Z_2 \supseteq L^{\langle U_1 \cup U_2 \rangle} \;\Rightarrow\; G(L/(Z_1 \cap Z_2)) \subseteq U_1 \cup U_2 \, .$$

Andererseits ist trivialerweise $G(L/(Z_1 \cap Z_2)) \;\supseteq\; \langle U_1 \cup U_2 \rangle$. Teil c): Analog zur vorigen Rechnung folgt aus $U_1 \cap U_2 \subseteq U_i$, dass $L^{U_1 \cap U_2} \supseteq Z_i$ für $i = 1, 2$ gilt. Also folgt

$$L^{U_1 \cap U_2} \;\supseteq\; Z_1 Z_2 \;\Rightarrow\; U_1 \cap U_2 \subseteq G(L/Z_1 Z_2) \, .$$

Andererseits ist $U_1 \cap U_2 \supseteq G(L/Z_1 Z_2)$ trivial. □

5.3. Auflösbarkeit durch Radikale

Aus der Schule kennt man die Lösungsformel für die quadratische Gleichung. Das Polynom

$$f(X) \;=\; a_2X^2 + a_1X + a_0 \;\in \mathbb{R}[X]$$

hat die Nullstellen

$$\alpha_{1,2} \;=\; \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}\,.$$

Die Nullstellen liegen also in der Radikalerweiterung $\mathbb{R}(\sqrt{D})$ von $\mathbb{R}$, wobei D die Diskriminante $D = a_1^2 - 4a_0a_2$ ist. Der Körper $\mathbb{R}(\sqrt{D})$ ist der Zerfällungskörper von $f(X)$ über $\mathbb{R}$. Dies motiviert die folgende

Definition 5.3.1
Eine Erweiterung L/K mit $L = K(\sqrt[m]{\beta})$ für $m \in \mathbb{N}$ und ein $\beta \in K$ heißt Radikalerweiterung. Es sei $f(X)$ ein nicht konstantes Polynom aus $K[X]$ und L ein Zerfällungskörper von $f(X)$ über K. Man nennt $f(X)$ auflösbar über K, wenn es eine Erweiterung M/L mit folgenden Eigenschaften gibt: Es existiert eine endliche aufsteigende Folge $K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$ von Unterkörpern $M_j \subseteq M$, so dass

$$M_{j+1} \;=\; M_j(\sqrt[m_j]{\beta_j})$$

ist für $m_j \in \mathbb{N}$ und jeweils $\beta_j \in M_j$. Ist zudem für jedes j das Radikal $\sqrt[m_j]{\beta_j}$ irreduzibel über M_j, so heißt $f(X)$ durch irreduzible Radikale auflösbar.

Satz 5.3.1
Es sei $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ mit einem Körper K, der die n-ten Einheitswurzeln enthält. Dann gilt:

(a) *Ist $L = K(\sqrt[n]{\beta})$ für ein $\beta \in K$, so ist L/K galoissch und $G(L/K)$ zyklisch, sowie $|G(L/K)| = m$ mit $m|n$. Dabei ist*

$$m = n \;\Leftrightarrow\; \sqrt[n]{\beta} \text{ irreduzibel (bzgl. } K)\,.$$

(b) *Ist umgekehrt L/K galoissch mit zyklischer Galoisgruppe $G(L/K)$ der Ordnung n, so gibt es $\beta \in K$ mit $L = K(\sqrt[n]{\beta})$.*

Zum Beweis dieses Satzes benötigen wir

Satz 5.3.2 (Unabhängigkeitssatz)
Es seien M, K Körper und $n \in \mathbb{N}$, sowie $\sigma_1, \ldots, \sigma_n : M \to K$ paarweise verschiedene Monomorphismen von Ringen. Dann gibt es zu jedem n-Tupel $\vec{a} = (a_1, \ldots, a_n) \in K^n - \{\vec{0}\}$ ein $\alpha \in M$ mit

$$\sum_{j=1}^{n} a_j \cdot \sigma_j(\alpha) \;\neq\; 0_K\,.$$

Anders formuliert: aus verschiedenen Monomorphismen $\sigma_1, \ldots, \sigma_n$ lässt sich nicht die Nullabbildung kombinieren, sie sind linear Unabhängig über K.

Beweis
Wir nehmen an, dass die Behauptung falsch ist, etwa mit einem nichttrivialen $\vec{a} \in K^n$ und (nach geeigneter Umnummerierung) einem $r \leq n$ so dass

$$(1) \quad \sum_{j=1}^{r} a_j\sigma_j(\alpha) \;=\; 0 \quad \forall \alpha \in M$$

gilt, d. h. die a_j kombinieren aus den σ_j die Nullabbildung. Es sei $r \leq n$ minimal mit dieser Eigenschaft. Zunächst ist $r \geq 2$, denn ansonsten wäre $a_1\sigma_1(\alpha) = 0 \Leftrightarrow \alpha = 0$. Es ist $\sigma_1 \neq \sigma_r$, es gibt also ein $\beta \in M$ mit $\sigma_1(\beta) \neq \sigma_r(\beta)$. Ersetzen wir α in (1) durch $\beta\alpha$, so folgt

$$(2) \quad a_1\sigma_1(\beta)\sigma_1(\alpha) \;+ \cdots +\; a_r\sigma_r(\beta)\sigma_r(\alpha) \;=\; 0\,.$$

Wir multiplizieren (1) mit $\sigma_r(\beta)$ und subtrahieren das Ergebnis von (2):

$$(3)\quad a_1(\sigma_1(\beta)-\sigma_r(\beta))\sigma_1(\alpha) + \cdots + a_{r-1}(\sigma_{r-1}(\beta)-\sigma_r(\beta))\sigma_{r-1}(\alpha) + \underbrace{a_r(\sigma_r(\beta)-\sigma_r(\beta))\sigma_r(\alpha)}_{=0} = 0\,,$$

für alle $\alpha \in M$. Wegen $a_1(\sigma_1(\beta)-\sigma_r(\beta)) \neq 0$ widerspricht dies der Minimalität von r. □

Beweis von Satz 5.3.1
Es sei ζ_n eine primitive Einheitswurzel in K. Zu a): Ohne Einschränkung sei $\beta \neq 0$. In $L[X]$ haben wir die Zerlegung

$$X^n - \beta = (X - \sqrt[n]{\beta}\zeta_n^0)(X - \sqrt[n]{\beta}\zeta_n^1)\cdots(X - \sqrt[n]{\beta}\zeta_n^{n-1})\,.$$

Dann ist L ein Zerfällungskörper des separablen Polynoms $X^n - \beta$ über K, also ist L/K galoissch. Da die Konjugierten von $\sqrt[n]{\beta}$ über K Nullstellen von $X^n - \beta$ sind folgt $G(L/K) = \{\sigma_1, \ldots, \sigma_m\}$ mit

$$\sigma_j(\sqrt[n]{\beta}) = \sqrt[n]{\beta}\cdot\eta_j$$

mit m verschiedenen n-ten Einheitswurzeln $\eta_j \in K$. Wir betrachten den Monomorphismus

$$\Phi = \begin{cases} G(L/K) & \to & E^{(n)} \\ \sigma_j & \mapsto & \eta_j \end{cases}\,.$$

Die Injektivität von Φ ist klar. Die Relationstreue folgt aus

$$(\sigma_j\circ\sigma_k)(\sqrt[n]{\beta}) = \sigma_j(\sqrt[n]{\beta}\cdot\eta_k) = \sigma_j(\sqrt[n]{\beta})\cdot\eta_k = \sqrt[n]{\beta}\cdot\eta_j\cdot\eta_k$$

und damit

$$\Phi(\sigma_j\circ\sigma_k) = \eta_j\eta_k = \Phi(\sigma_j)\Phi(\sigma_k)\,.$$

Somit ist $G(L/K)$ isomorph zu einer Untergruppe der zyklischen Gruppe $E^{(n)}$. Nach Satz 1.7.4 ist $G(L/K)$ damit zyklisch mit Ordnung $m|n$. Es gilt ferner:

$$\sqrt[n]{\beta}\text{ irreduzibel} \;\Leftrightarrow\; X^n-\beta \in K[X]\text{ irreduzibel} \;\Leftrightarrow\; X^n-\beta = m_{\sqrt[n]{\beta}}(X)$$

mit $\deg(X^n-\beta) = n$ und $\deg(m_{\sqrt[n]{\beta}}(X)) = [L:K] = |G(L/K)| = m$. Das Minimalpolynom ist separabel, also ist $\sqrt[n]{\beta}$ irreduzibel genau dann, wenn $m = n$ gilt. Zu b): es sei L/K galoissch und $G(L/K) = \langle\sigma\rangle$ zyklisch vom Grad n. Für $\alpha \in L$ betrachten wir die Lagrangesche Resolvente

$$\vartheta = \vartheta(\alpha) = \alpha + \zeta_n\sigma(\alpha) + \zeta_n^2\sigma^2(\alpha) + \cdots + \zeta_n^{n-1}\sigma^{n-1}(\alpha)\,.$$

Nach dem Unabhängigkeitssatz gibt es $\alpha_0 \in L$ mit $\vartheta(\alpha_0) \neq 0$. Wir setzen $\vartheta_0 = \vartheta(\alpha_0)$. Dann ist

$$\begin{aligned} \vartheta_0 &= \alpha_0 + \zeta_n\sigma(\alpha_0) + \cdots + \zeta_n^{n-1}\sigma^{n-1}(\alpha_0) \\ \sigma(\vartheta_0) &= \sigma(\alpha_0) + \zeta_n\sigma^2(\alpha_0) + \cdots + \zeta_n^{n-1}\sigma^n(\alpha_0) \\ &= \zeta_n^{-1}\vartheta_0 \end{aligned}$$

wegen $\sigma^n(\alpha_0) = \alpha_0$ und $\zeta_n^n = 1$. Es folgt induktiv $\sigma^k(\vartheta_0) = \zeta_n^{-k}\vartheta_0$. Also gilt

$$\sigma^k(\vartheta_0) = \vartheta_0 \;\Leftrightarrow\; n|k \;\Leftrightarrow\; \sigma^k = \mathrm{id}$$

und damit $K(\vartheta_0) = L^{\langle\sigma^n\rangle} = L^{\{\mathrm{id}\}} = L$. Für $\beta = \vartheta_0^n$ gilt

$$\sigma^k(\beta) = \sigma^k(\vartheta_0)^n = (\zeta_n^{-k}\vartheta_0)^n = \vartheta_0^n = \beta$$

für $k = 0\ldots n$. Also $\beta \in L^{G(L/K)} = K$, und $L = K(\sqrt[n]{\beta})$. □

Zum Verständnis der folgenden Definition machen wir folgende Vorbemerkungen: Es sei $f(X) \in K[X]$ ein separables Polynom und L ein Zerfällungskörper von $f(X)$ über K mit dem Zerfall

$$f(X) = (X-\alpha_1)\cdots(X-\alpha_n) \in L[X]$$

und der Nullstellenmenge $\mathcal{N} = \{\alpha_1, \ldots, \alpha_n\}$. Für ein $\sigma \in G(L/K)$ ist die Restriktion $\sigma|_{\mathcal{N}}$ offenbar eine Permutation von $\mathcal{N}$, d. h. bis auf Isomorphie von $\mathfrak{S}_n$. Die Abbildung

$$\Phi \;=\; \begin{cases} G(L/K) & \to & \mathfrak{S}(\mathcal{N}) \\ \sigma & \mapsto & \sigma|_{\mathcal{N}} \end{cases}$$

ist ein Automorphismus von Gruppen. Das Bild $\Phi(G(L/K)) =: G'(L/K)$ ist eine Untergruppe der vollen Permutationsgruppe $\mathfrak{S}(\mathcal{N}) \cong \mathfrak{S}_n$. Die Gruppen $G'(L/K)$ (bzw. $G(L/K)$) operieren von links auf $\mathcal{N}$ im Sinne von Definition 1.2.1. Damit ist $\mathcal{N}$ disjunkte Vereinigung seiner Bahnen nach Definition 1.2.3(b).

Definition 5.3.2
Es sei $f(X) \in K[X]$ separabel sowie L ein Zerfällungskörper von $f(X)$ über K. Unter der Galoisgruppe von $f(X)$ über K (Schreibweise $G(f, K)$) versteht man die Gruppe $G(L/K)$ oder die ihr zugeordnete Permutationsgruppe $G'(L/K)$ der Nullstellenmenge von $f(X)$ in L.

Der nächste Satz enthüllt einige Eigenschaften von $G'(L/K)$:

Satz 5.3.3
Es sei $f(X) \in K[X]$ normiert und separabel mit $\deg(f) = n > 0$ und Nullstellenmenge $\mathcal{N} \subset L$ in einem Zerfällungskörper L von $f(X)$ über K. Dann gilt:

(a) *$|G(L/K)|$ ist ein Teiler von $n!$.*
(b) *$G'(L/K)$ ist die Menge aller Permutationen $\sigma \in \mathfrak{S}(\mathcal{N})$ mit folgender Eigenschaft: Für ein beliebiges Polynom $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ gilt*

$$h(\alpha_1, \ldots, \alpha_n) \;=\; 0 \quad \Rightarrow \quad h(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) \;=\; 0\,.$$

(c) *Ist $\mathcal{N} = \{\beta_1, \ldots, \beta_r\} \dot\cup \{\gamma_1, \ldots, \gamma_s\} \dot\cup \cdots$ die Zerlegung von $\mathcal{N}$ in Bahnen unter $G'(L/K)$, so ist $f(X) = g_1(X)g_2(X)\cdots$ mit*

$$g_1(X) \;=\; (X - \beta_1)\cdots(X - \beta_r) \;\;,\;\; g_2(X) \;=\; (X - \gamma_1)\cdots(X - \gamma_s) \;\;,\;\; \cdots$$

die Zerlegung von $f(X)$ in irreduzible normierte Faktoren in $K[X]$. Insbesondere ist $f(X)$ irreduzibel in $K[X]$ genau dann, wenn $\mathcal{N}$ nur genau eine Bahn enthält. Man sagt dann, dass $G(L/K)$ bzw. $G'(L/K)$ transitiv auf $\mathcal{N}$ operiert.

Beweis
Teil a) ist klar, da $G'(L/K) \leq \mathfrak{S}_n$ ist mit $|\mathfrak{S}_n| = n!$. Zu Teil b): Jedes $\sigma \in G(L/K)$ hat die genannte Eigenschaft wegen der Relationstreue bzgl. Addition und Multiplikation. Es sei nun umgekehrt $\sigma \in \mathfrak{S}(\mathcal{N})$ beliebig, so dass die Nullstelleneigenschaft unter Anwendung von σ in jedem n-stelligen Polynom $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ erhalten bleibt. Es ist zu zeigen: es gibt einen K-Automorphismus $\tau \in G(L/K)$ mit $\tau|_{\mathcal{N}} = \sigma$. Da der Zerfällungskörper L von den Nullstellen $\alpha_1, \ldots, \alpha_n$ erzeugt wird gibt es für jedes $\beta \in L$ ein Polynom $h_\beta(X_1, \ldots, X_n)$ über K mit $h(\alpha_1, \ldots, \alpha_n) = \beta$. Das gesuchte τ definieren wir wie folgt:

$$\tau(\beta) \;:=\; \tau(h_\beta(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)))\,.$$

Dadurch wird die Wirkung der Permutation σ auf den Erzeugern auf L fortgesetzt. Es ist allerdings zu zeigen, dass die Definition unabhängig von der Wahl des Polynoms h_β zu β ist. Seien also h_β und h'_β n-stellig über K mit $\beta = h_\beta(\alpha_1, \ldots, \alpha_n) = h'_\beta(\alpha_1, \ldots, \alpha_n)$. Dann ist die Differenz $d = h_\beta - h'_\beta$ ein n-stelliges Polynom mit $d(\alpha_1, \ldots, \alpha_n) = 0$. Nach Wahl von σ ist auch $d(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0$, also $\tau(\beta) = h_\beta(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = h'_\beta(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$, d. h. die Definition ist gerechtfertigt. Die Relationstreue von τ folgt aus der Relationstreue der Zuordnung $K[X_1, \ldots, X_n] \to L$, $h \mapsto h(\alpha_1, \ldots, \alpha_n)$ bzgl. Addition und Multiplikation. Es sei $|\langle\sigma\rangle| = m$. Dann ist $\tau^m(\alpha) = h_\alpha(\sigma^m(\alpha_1), \ldots, \sigma^m(\alpha_n)) = h_\alpha(\alpha_1, \ldots, \alpha_n) = \alpha$, also $\tau^m = \mathrm{id}$, d. h. die Abbildung τ^{m-1} ist das Inverse zu τ bzgl. der Operation $\circ$. Jedes $\alpha \in K$ wird durch das konstante Polynom $h_\alpha(X_1, \ldots, X_n) = \alpha$ dargestellt, woraus die K-Linearität von τ folgt. Ebenso wird jedes α_j dargestellt durch $h_j(X_1, \ldots, X_n) = X_j$, woraus $\tau|_{\mathcal{N}} = \sigma$ folgt. Insgesamt ist τ ein K-Automorphismus von L. Zu Teil c): Es ist zu zeigen, dass $g_1(X)$,

$g_2(X)$ usw. irreduzible Polynome in $K[X]$ sind. Wir dürfen uns auf $g_1(X)$ beschränken: durch jedes $\tau \in G(L/K)$ werden die Nullstellen $\beta_1, \ldots, \beta_r$ permutiert, also $g_1(X) \in L^{G(L/K)}[X] = K[X]$. Angenommen $g_1(X) = g(X)g'(X)$ ist eine Zerlegung in $K[X]$ mit $\deg(g(X)) \geq 1$, dann ist $g(\beta_j) = 0$ für mindestens eine Nullstelle β_j von $g_1(X)$. Wegen $g^{(\sigma)}(X) = g(X)$ sind dann aber auch alle anderen Elemente der Bahn $\{\beta_1, \ldots, \beta_r\}$ Nullstellen von $g(X)$, woraus $\deg(g'(X)) = 0$ folgt, d. h. $g_1(X)$ ist irreduzibel. □

Satz 5.3.4
Es sei $m \in \mathbb{N}$, $\mathrm{char}(K) \nmid m$ und L/K eine galoissche Erweiterung mit $L^{(m)} \subseteq L$. Ferner sei $\beta \in L$ und $\beta_1, \ldots, \beta_r$ ein volles System von Konjugierten zu β über K in L. Dann ist

$$M \;=\; L(\sqrt[m]{\beta_1}, \ldots, \sqrt[m]{\beta_r})$$

eine Galoiserweiterung von K.

Beweis
Ohne Einschränkung sei $\beta \neq 0$. M ist Zerfällungskörper des Polynoms

$$h(X) \;=\; (X^m - \beta_1) \cdots (X^m - \beta_r) \;\in\; L[X]$$

über L. Zunächst ist $h(X)$ separabel, da seine Nullstellen die paarweise verschiedenen Elemente $\zeta_m^k \sqrt[m]{\beta_j}$ $(1 \leq j \leq r,\ 1 \leq k \leq m)$ mit einer primitiven m-ten Einheitswurzel $\zeta_m \in L$ sind. Wir zeigen zunächst $h(X) \in K[X]$, dazu sei $L' = K(\beta_1, \ldots, \beta_r)$, dann ist L' Zerfällungskörper des separablen Polynoms $m_\beta(X) \in K[X]$, und damit nach Satz 5.2.1 galoissch über K. Es sei $\sigma \in G(L'/K)$ und

$$h(X) \;=\; \sum_{j=0}^{r} a_j X^{jm} \quad , \quad a_j \in L' \,,$$

dann ist

$$h^{(\sigma)}(X) \;=\; \sum_{j=0}^{r} \sigma(a_j) X^{jm} \;=\; (X^m - \sigma(\beta_1)) \cdots (X^m - \sigma(\beta_r)) \;=\; (X^m - \beta_1) \cdots (X^m - \beta_r) \;=\; h(X)$$

da σ das Konjugiertensystem der β_j lediglich permutiert. Es folgt $\sigma(a_j) = a_j$, damit $a_j \in L'^{G(L'/K)} = K$. Also ist M Zerfällungskörper des separablen Polynoms $h(X) \in K[X]$ über K, damit nach Satz 5.2.1 galoissch. □

Wir kommen nun zum 1. Hauptkriterium. Obwohl es unter allgemeineren Voraussetzungen gilt, behandeln wir es der Einfachheit halber nur für Körper der Charakteristik Null.

Satz 5.3.5 (1. Hauptkriterium)
Es sei K ein Körper mit $\mathrm{char}(K) = 0$. Ist ein separables Polynom $f(X) \in K[X]$ über K auflösbar, so ist $G(f, K)$ nach Definition 1.9.2(b) auflösbar.

Beweis
Es sei L ein Zerfällungskörper von $f(X)$ über K. Wir beweisen die Auflösbarkeit von $G(L/K) = G(f, K)$. Nach Definition 5.3.1 bedeutet die Auflösbarkeit von $f(X)$ über K die Existenz einer Erweiterung M/L und einer endlichen Körperkette

$$\begin{aligned} &(1) \qquad K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M \text{ mit} \\ &(2) \qquad M_{j+1} = M_j(\sqrt[m_j]{\beta_j}),\ \beta_j \in M_j \,,\ m_j \in \mathbb{N}. \end{aligned}$$

Diese Kette wird in zwei Schritten derart abgeändert, so dass Satz 5.3.1 über zyklische Erweiterungen angewendet werden kann, und das Endglied galoissch über K ist.

1. Schritt:
Um Satz 5.3.1 anwenden zu können, führen wir in die Körperkette (1) die nötigen Einheitswurzeln ein.

Dazu sei $m = m_0 \cdot m_1 \cdots m_{r-1}$ und ζ_m eine primitive m-te Einheitswurzel über M. Mit der Abkürzung $L_j = M_j(\zeta_m)$ wird aus (1) die Kette

$$(3)\quad K \subseteq K(\zeta_m) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r \qquad L_{j+1} = L_j(\sqrt[m_j]{\beta_j})\ ,\ \beta_j \in L_j\ .$$

2. Schritt:
Wir erweitern die Körperkette (3) derart, dass ihr Endglied galoissch über K wird. Dabei wird induktiv jedes L_j durch ein $L'_j \supseteq L_j$ ersetzt, so dass L'_j/K galoissch ist. Im Fall $j = 0$ ist $L'_0 = L_0$ galoissch über K. Andernfalls sei L'_j/K bereits galoissch. Zu L'_j adjungieren wir sukzessive m_j-te Wurzeln von $\beta_j^{(k)}$ für $k = 1 \ldots n_j$, wobei $\beta_j^{(1)} = \beta_j$ und $\beta_j^{(k)}$ sämtliche Konjugierten von β_j über K in L'_j bezeichnet (diese liegen in L'_j, da dieser Körper nach Konstruktion über K normal ist). Wir setzen

$$L'_{j,d} \;=\; L'_j\left(\sqrt[m_j]{\beta_j^{(1)}}, \ldots,\ \sqrt[m_j]{\beta_j^{(d)}}\right)$$

bzw. $L'_{j+1} = L'_{j,n_j}$ und erhalten die Kette

$$(4)\quad \cdots \subseteq L'_j \subseteq L'_{j,1} \subseteq L'_{j,2} \subseteq \cdots \subseteq L'_{j,n_j-1} \subseteq L'_{j+1} \subseteq L'_{j+1,1} \subseteq \cdots$$

wobei nach Satz 5.3.4 die Erweiterungen L'_j/K galoissch sind. Damit ist auch jeweils $L'_{j+1}/L'_{j,k}$ galoissch für alle k. Dieser Körperfolge entspricht die Folge von Gruppen

$$(5)\quad G(L'_{j+1}/L'_j) \triangleright G(L'_{j+1}/L'_{j,1}) \triangleright G(L'_{j+1}/L'_{j,2}) \triangleright \cdots \triangleright G(L'_{j+1}/L'_{j,n_j-1}) \triangleright G(L'_{j+1}/L'_{j+1}) \;\cong\; \{1\}\ .$$

Nach den Sätzen 5.2.4(d) und 5.3.1 sind die Faktoren

$$G(L'_{j+1}/L'_{j,d}) \,/\, G(L'_{j+1}/L'_{j,d+1}) \;\cong\; G(L'_{j,d+1}/L'_{j,d})$$

sämtlich zyklisch. Nach Definition 1.9.2(b) ist $G(L'_{j+1}/L'_j)$ für alle j Auflösbar. Die Körperkette (3) ist also ersetzt durch (4) mit

$$(6)\quad K \subseteq L'_0 \subseteq L'_1 \subseteq \cdots \subseteq L'_j \subseteq L'_{j+1} \subseteq \cdots \subseteq L'_r$$

mit L'_j/K jeweils galoissch und $G(L'_{j+1}/L'_j)$ auflösbar. Der Kette (6) entspricht die Folge der Galoisgruppen

$$(7)\quad G(L'_r/K) \trianglerighteq G(L'_r/L'_0) \triangleright G(L'_r/L'_1) \triangleright \cdots \triangleright G(L'_r/L'_r) \;\cong\; \{1\}\ .$$

Nach Satz 5.2.4(d) sind die Faktoren

$$G(L'_r/L'_j) \,/\, G(L'_r/L'_{j+1}) \;\cong\; G(L'_{j+1}/L'_j)$$

sämtlich auflösbar. Das Startglied $G(L'_r/K)/G(L'_r/L_0) \;\cong\; G(L'_0/K)$ ist zyklisch, also trivial oder auflösbar. Wiederholte Anwendung von Satz 1.9.4(b) ergibt, dass die Gruppe $G(L'_r/K)$ auflösbar ist. Nach Satz 1.9.3(a) ist $G(f, K) = G(L/K)$ auflösbar. □

Zum Beweis des zweiten Hauptkriteriums, der Umkehrung des 1. Hauptkriteriums, benötigen wir als Vorbereitung folgenden

Satz 5.3.6
Es sei L/K galoissch, sowie M eine Erweiterung von K, die mit L einen gemeinsamen Oberkörper besitzt. Dann ist $L(M)/M$ galoissch und $G(L(M)/M)$ isomorph zu einer Untergruppe von $G(L/K)$.

Beweis
(Übungsaufgabe) □

Bei der Formulierung des zweiten Hauptkriteriums beschränken wir uns wieder auf den Fall der Charakteristik Null.

Satz 5.3.7 (2. Hauptkriterium)
Es sei $f(X)$ ein separables Polynoms in $K[X]$ mit $\mathrm{char}(K) = 0$*, so dass $G(f,K)$ auflösbar nach Definition 1.9.2(b) ist. Dann ist $f(X)$ auflösbar über K.*

Bemerkung 5.3.1
Mit etwas mehr Aufwand lässt sich zeigen, dass $f(X)$ über K dann sogar durch irreduzible Radikale auflösbar ist.

Beweis
Es sei L ein Zerfällungskörper von $f(X)$ über K und $|G(f,K)| = m$ sowie ζ_m eine primitive m-te Einheitswurzel über L. Es sei $K' = K(\zeta_m)$ bzw. $L' = L(\zeta_m)$. Nach Satz 5.3.6 ist L'/K' galoissch, und die Gruppe $G_0 = G(L'/K')$ ist isomorph zu einer Untergruppe von $G(L/K) = G(f,K)$. Nach Satz 1.9.3(a) ist G_0 auflösbar und besitzt daher nach Satz 1.9.5 eine Normalreihe

$$G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r \cong \{1\} ,$$

deren Faktoren sämtlich zyklisch und von Primzahlordnung sind (wir nehmen ohne Einschränkung $|G_0| > 1$, d. h. $L' \neq K'$ an). Bezeichne

$$K' = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L'$$

die Reihe der zugehörigen Fixkörper in L'. Nach dem Hauptsatz der Galoistheorie ist für $0 \leq j \leq r-1$ die Erweiterung K_{j+1}/K_j galoissch und

$$G(K_{j+1}/K_j) \cong G_j \,/\, G_{j+1} ,$$

also zyklisch von Primzahlordnung, etwa p_j. Nach Satz 5.3.1 gibt es für alle j jeweils ein $\beta_j \in K_j$ mit $K_{j+1} = K_j(\sqrt[p_j]{\beta_j})$. Nach Definition 5.3.1 ist damit $f(X)$ auflösbar über K. □

Das 1. und 2. Hauptkriterium lassen sich zusammenfassen zum

Satz 5.3.8 (Hauptsatz über Auflösbarkeit von Polynomen)
Es sei $\mathrm{char}(K) = 0$ *und $f(X) \in K[X]$ separabel, dann gilt:*

$f(X)$ auflösbar über K (Definition 5.3.1) $\iff$ *$G(f,K)$ auflösbar (Definition 1.9.2).*

5.4. Symmetrische Funktionen

Nachdem wir die allgemeine Theorie der Auflösbarkeit durch Radikalerweiterungen entwickelt haben, wenden wir uns nun Anwendungen zu. Insbesondere wollen wir Lösungen für quadratische Gleichungen (seit der Antike bekannt) und für kubische Gleichungen (zurückgehend auf Cardano, 1501-1576) mittels der Galoistheorie erklären. Die folgenden Abschnitte dienen als Vorbereitung.

Definition 5.4.1
Im Folgenden sei K ein Körper und $X_1, \ldots, X_n$ unabhängige Unbestimmte über K. Dann betrachten wir den Quotientenkörper

$$K_{\mathrm{rat}} := \mathrm{Quot}(K[X_1, \ldots, X_n]) = K(X_1, \ldots, X_n)$$

der rationalen Funktionen in den Unbestimmten $X_1, \ldots, X_n$. Für jedes $\sigma \in \mathfrak{S}_n$ gibt es genau einen K-Automorphismus $\varphi_\sigma : K(X_1, \ldots, X_n) \to K(X_1, \ldots, X_n)$ mit $\varphi_\sigma(X_j) = X_{\sigma(j)}$ für $j = 1 \ldots n$. Es sei $G := \{\varphi_\sigma \mid \sigma \in \mathfrak{S}_n\} \cong \mathfrak{S}_n$.

Definition 5.4.2
Man setzt

$$K_{\mathrm{sym}} = K_{\mathrm{rat}}^G = \{F(X_1, \ldots, X_n) = f(X_1, \ldots, X_n)/g(X_1, \ldots, X_n) \mid \varphi(F) = F \ \forall \varphi \in G\} ,$$

und bezeichnet den Fixkörper K_{sym} als den Körper der symmetrischen Funktionen über K in n Unbestimmten. Ein $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n] \cap K_{\mathrm{sym}}$ heißt symmetrisches Polynom über K in n Unbestimmten.

Beispiel 5.4.1
Ist Y eine Unbestimmte über $K[X_1, \ldots, X_n]$, so betrachte man

$$(Y - X_1) \cdots (Y - X_n) \;=\; \sum_{j=0}^{n} (-1)^j s_j \cdot Y^{n-j} \,.$$

Die dadurch definierten Koeffizienten $s_0, \ldots, s_n \in K[X_1, \ldots, X_n] \cap K_{\mathrm{sym}}$ sind symmetrische Polynome:

$$\begin{array}{rcl} s_0 & = & 1 \\ s_1 & = & X_1 + \cdots + X_n \\ & \vdots & \\ s_n & = & X_1 \cdots X_n \qquad . \end{array}$$

Allgemein gilt

$$s_k \;=\; \sum_{1 \le i_1 \le \cdots \le i_k \le n} X_{i_1} \cdots X_{i_k} \,.$$

Definition 5.4.3
Man nennt $s_j \in K[X_1, \ldots, X_n]$ das j-te elementarsymmetrische Polynom in n Unbestimmten.

Durch leichte Rechnung kann man zeigen, dass Summen, Produkte und K-Vielfache von symmetrischen Funktionen (bzw. Polynomen) wieder symmetrisch sind. Insbesondere ist der durch die elementarsymmetrischen Polynome erzeugte Körper $K_s = K(s_1, \ldots, s_n)$ ein Teilkörper von K_{sym}. Der folgende Grundlegende Satz zeigt, dass sich jede symmetrische Funktion schon aus den elementarsymmetrische Polynomen erzeugen lässt:

Satz 5.4.1 (Hauptsatz über symmetrische Funktionen)
Mit den obigen Bezeichnungen gilt:

(a) *Die Körpererweiterung $K_{\mathrm{rat}}/K_{\mathrm{sym}}$ ist galoissch mit Galoisgruppe $\mathfrak{S}_n$ und $[K_{\mathrm{rat}} : K_{\mathrm{sym}}] = n!$.*
(b) *Für jedes $i = 1 \ldots n$ ist*

$$f_i(Y) \;=\; (Y - X_1) \cdots (Y - X_i)$$

das Minimalpolynom der Unbestimmten X_i über $K_s(X_{i+1}, \ldots, X_n)$.
(c) $K_{\mathrm{sym}} = K_s = K(s_1, \ldots, s_n)$.

Beweis
Teil a) folgt aus dem Hauptsatz der Galoistheorie, da K_{sym} als Fixkörper unter einer zu $\mathfrak{S}_n$ isomorphen Gruppe definiert ist. Zu b): Wir bestimmen die zu den sukzessiven Erweiterungen

$$K_s \;\subset\; K_s(X_n) \;\subset\; K_s(X_{n-1}, X_n) \;\subset \cdots \subset K_s(X_1, \ldots, X_n) \;=\; K_{\mathrm{rat}}$$

gehörenden Minimalpolynome. Zunächst ist

$$f_n(Y) \;=\; (Y - X_1) \cdots (Y - X_n) \;=\; \sum_{j=0}^{n} (-1)^j s_j \cdot Y^{n-j} \;\in\; K_s[Y]$$

ein Polynom vom Grad n über dem ersten Körper der Kette, das offenbar die Unbestimmte X_n als Nullstelle besitzt. Also gilt $[K_s(X_n) : K_s] \le n$. Abspalten der Nullstelle in $K_s(X_n)[Y]$ ergibt $f_n(Y) = (Y - X_n) \cdot f_{n-1}(Y)$ mit $\deg(f_{n-1}) = n - 1$, insbesondere liegt $f_{n-1}(Y)$ im Polynomring über $K_s(X_n)$. So fortfahrend erhält man

$$(*) \quad [K_s(X_i, \ldots, X_n) : K_s(X_{i+1}, \ldots, X_n)] \;\le\; \deg(f_i) \;=\; i$$

mit den Polynomen $f_i(Y) = (Y - X_1) \cdots (Y - X_i) \in K_s(X_{i+1}, \ldots, X_n)[Y]$ und $f_i(Y) = f_{i-1}(Y) \cdot (Y - X_i)$. Daraus folgt

$$[K_{\mathrm{rat}} : K_s] \;=\; \prod_{i=1}^{n} [K_s(X_i, \ldots, X_n) : K_s(X_{i+1}, \ldots, X_n)] \;\le\; n! \,.$$

Andererseits ist $K_s \subseteq K_{\text{sym}}$, und nach Teil a) ist $[K_{\text{rat}} : K_{\text{sym}}] = n!$. Der Grad der Erweiterung $[K_{\text{rat}} : K_s]$ kann also nicht kleiner als $n!$ sein, daraus folgt $K_s = K_{\text{sym}}$, insbesondere muss in den Ungleichungen $(*)$ jeweils das Gleichheitszeichen stehen, woraus die Irreduzibilität der $f_i(Y)$ folgt. Damit sind die Teile b) und c) gezeigt. □

5.5. Norm und Spur

Definition 5.5.1
Es sei L/K galoissch und $\alpha \in L$, dann heißt

$$N_{L/K}(\alpha) \;=\; \prod_{\sigma \in G(L/K)} \sigma(\alpha)$$

die Norm von α über K und

$$S_{L/K}(\alpha) \;=\; \sum_{\sigma \in G(L/K)} \sigma(\alpha)$$

die Spur von α über K.

Satz 5.5.1
Es sei L/K galoissch und $\alpha \in L$, dann gilt $N_{L/K}(\alpha), S_{L/K}(\alpha) \in K$.

Beweis
Sei $\tau \in G(L/K)$ beliebig, dann gilt

$$\tau(N_{L/K}(\alpha)) \;=\; \prod_{\sigma \in G(L/K)} \tau(\sigma(\alpha))\,,$$

aber da $\tau \circ G(L/K) = G(L/K)$ gilt ist $\tau(N_{L/K}(\alpha)) = N_{L/K}(\alpha)$ für alle τ, d. h. die Norm ist ein Element des Fixkörpers $L^{G(L/K)} = K$. Die gleiche Rechnung gilt für die Spur. □

Satz 5.5.2
Es sei L/K galoissch und $L = K(\alpha)$ mit einem primitiven Element $\alpha \in L$. Für das Minimalpolynom $m_\alpha(X) \in K[X]$ von α gelte

$$m_\alpha(X) \;=\; \sum_{i=0}^{n} (-1)^i a_i \cdot X^{n-i}\,,$$

dann gilt $a_1 = S_{L/K}(\alpha)$ und $a_n = N_{L/K}(\alpha)$.

Beweis
Nach Satz 5.3.3(c) ist

$$m_\alpha(X) \;=\; \prod_{\sigma \in G(L/K)} (X - \sigma(\alpha)) \;=\; X^n \;-\; \left(\sum_{\sigma} \sigma(\alpha)\right) X^{n-1} + \cdots + (-1)^n \prod_{\sigma} \sigma(\alpha)\,,$$

woraus die Behauptung folgt. □

Satz 5.5.3
Norm und Spur sind transitiv: ist $M/L/K$ ein Turm galoisscher Erweiterungen, d. h. sind M/K und L/K (und damit nach Satz 5.2.4(c) auch M/L) galoissch, so gilt für alle $\alpha \in M$:

$$\begin{array}{rcll} N_{M/K}(\alpha) & = & N_{L/K}(N_{M/L}(\alpha)) & \text{und} \\ S_{M/K}(\alpha) & = & S_{L/K}(S_{M/L}(\alpha)) & . \end{array}$$

Beweis
Nach Satz 5.2.4(c) ist $G(L/K) \cong G(M/K)/G(L/K)$. In dessen Beweis ergab sich diese Isomorphie mittels der Restriktion

$$\psi \;=\; \begin{cases} G(M/K) & \to & G(L/K) \\ \sigma & \mapsto & \sigma|_L \end{cases}$$

mit $\mathrm{Ker}(\psi) = G(M/L)$. Nach dem Homomorphiesatz gibt es dann $\sigma_1, \ldots, \sigma_r \in G(M/K)$, so dass $G(L/K) = \{\psi(\sigma_1), \ldots, \psi(\sigma_r)\}$ und

$$G(M/K) \;=\; \sigma_1 G(M/L) \,\dot\cup\, \cdots \,\dot\cup\, \sigma_r G(M/L)$$

die Zerlegung von $G(M/K)$ in die Nebenklassen bzgl. des Kerns von ψ ist. Daraus folgt

$$N_{M/K}(\alpha) = \prod_{j=1}^{r} \sigma_j\Big(\prod_{\sigma\in G(M/L)} \sigma(\alpha)\Big) = \prod_{j=1}^{r} \sigma_j|_L(N_{M/L}(\alpha)) = \prod_{\sigma\in G(L/K)} \sigma(N_{M/L}(\alpha)) = N_{L/K}(N_{M/L}(\alpha)).$$

Die gleiche Rechnung gilt für die Spur. □

5.6. Lösungsformeln für Polynome zweiten und dritten Grades

Da die symmetrische Gruppe $\mathfrak{S}_\mathfrak{n}$ für $n \le 4$ auflösbar ist, sind Polynome vom Grad ≤ 4 stets auflösbar über ihrem Koeffizientenkörper. Die Konzepte der Galoistheorie erlauben darüber hinaus, auch die zugehörigen Lösungsformeln zu finden. Wir wollen dies für die Fälle der Gleichungen 2. und 3. Grades in diesem Abschnitt illustrieren. Wir haben gesehen, dass die Galoisgruppe des allgemeinen Polynoms n-ten Grades stets $\mathfrak{S}_n$ ist. Dies bedeutet: Sind $X_1, \ldots, X_n, Y$ unabhängige Unbestimmte über K und $s_0, \ldots, s_n \in K[X_1, \ldots, X_n]$ die elementarsymmetrischen Polynome mit

$$K_{\mathrm{rat}} \;=\; K(X_1, \ldots, X_n) \;\;,\;\; K_{\mathrm{sym}} \;=\; K(s_1, \ldots, s_n) \;\;,\;\; f(Y) \;=\; \prod (Y - X_i) \;=\; \sum_{i=0}^{n} (-1)^i s_i \cdot Y^{n-i}\,,$$

dann ist K_{rat} der Zerfällungskörper von $f(Y)$ über K_{sym} und $G(f, K_{\mathrm{sym}}) = G(K_{\mathrm{rat}}/K_{\mathrm{sym}}) \cong \mathfrak{S}_n$. Im Allgemeinen ist nach Definition 5.3.2 die Galoisgruppe eines Polynoms vom Grad n eine Untergruppe von $\mathfrak{S}_n$. Die Galoisgruppe kann echt kleiner sein, beispielsweise im Falle zyklischer Erweiterungen. Die größte echte Untergruppe von $\mathfrak{S}_n$ ist die alternierende Gruppe $\mathcal{A}_n \trianglelefteq \mathfrak{S}_n$ der geraden Permutationen. Die Diskriminante eines Polynoms gibt ein einfaches Kriterium dafür, ob die Galoisgruppe schon in $\mathcal{A}_n$ enthalten ist:

Definition 5.6.1
Es sei $f(X) \in K[X]$ normiert und

$$f(X) \;=\; (X - \alpha_1) \cdots (X - \alpha_n)$$

in einem Zerfällungskörper L von $f(X)$ über K. Unter der Diskriminante von $f(X)$ versteht man

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

Satz 5.6.1
Es sei $D(f)$ die Diskriminante eines $f(X) = \sum(-1)^i a_i X^{n-i} \in K[X]$, dann gilt:

(a) *$D(f)$ ist ein Element von K.*
(b) *Die Diskriminante lässt sich als Polynom in den Koeffizienten a_i ausdrücken.*
(c) *$G(f, K) \le \mathcal{A}_n \;\Leftrightarrow\; \sqrt{D(f)} \in K$.*
(d) *$D(f) = 0 \;\Leftrightarrow\; f$ inseparabel.*

Beweis
Ohne Einschränkung sei $a_0 = 1$, d. h. $f(X)$ normiert. Wir setzen

$$D(X_1, \ldots, X_n) \;=\; \prod_{1\le i<j\le n} (X_i - X_j)^2$$

in $K[X_1,\ldots,X_n]$. Ein $\sigma \in \mathfrak{S}_n$ tauscht dann nur die Produktreihenfolge bzw. das Vorzeichen unter dem Quadrat, d. h.

$$D(\sigma(X_1),\ldots,\sigma(X_n)) \;=\; \prod_{1\le i<j\le n} (X_{\sigma(i)} - X_{\sigma(j)})^2 \;=\; D(X_1,\ldots,X_n)\,,$$

woraus $D(X_1,\ldots,X_n) \in K_{\text{sym}}$ folgt. Nach Satz 5.4.1(c) ist $D(X_1,\ldots,X_n) = g(s_1,\ldots,s_n)$ für ein $g(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$. Wir betrachten nun den Einsetzhomomorphismus

$$\varphi \;=\; \begin{cases} K[X_1,\ldots,X_n] & \to & K(\alpha_1,\ldots,\alpha_n) & = & L \\ f(X_1,\ldots,X_n) & \mapsto & f(\alpha_1,\ldots,\alpha_n) \end{cases}$$

als Fortsetzung der Zuordnungen $X_i \mapsto \alpha_i$. Dann ist

$$D(f) \;=\; D(\alpha_1,\ldots,\alpha_n) \;=\; \varphi(D(X_1,\ldots,X_n)) \;=\; \varphi(g(s_1,\ldots,s_n)) \;=\; g(a_1,\ldots,a_n) \;\in\; K\,.$$

Daraus folgen a) und b). Zu c): Wir betrachten das Vandermonde-Polynom

$$V(f) \;=\; V(\alpha_1,\ldots,\alpha_n) \;=\; \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)\,.$$

Offenbar ist $V(f) = \sqrt{D(f)}$ in L. Für ein $\sigma \in \mathfrak{S}_n$ gilt

$$\sigma(V(\alpha_1,\ldots,\alpha_n)) \;=\; \prod_{1\le i<j\le n} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})\,.$$

Für ein Paar $i<j$ sei $i' = \min\{\sigma(i),\sigma(j)\}$ bzw. $j' = \max\{\sigma(i),\sigma(j)\}$. Mit Definition 1.6.4 gilt dann

$$\alpha_{\sigma(i)} - \alpha_{\sigma(j)} \;=\; \begin{cases} \alpha_{i'} - \alpha_{j'} & \text{falls } (i,j) \text{ keine Inversion von } \sigma \text{ ist} \\ -(\alpha_{i'} - \alpha_{j'}) & \text{falls } (i,j) \text{ eine Inversion von } \sigma \text{ ist} \end{cases}\,.$$

Also ist $\sigma(V(\alpha_1,\ldots,\alpha_n)) = (-1)^{I(\sigma)} \cdot V(\alpha_1,\ldots,\alpha_n)$. Nach dem Hauptsatz der Galoistheorie gilt

$$V(\alpha_1,\ldots,\alpha_n) \in K \;\Leftrightarrow\; V(\alpha_1,\ldots,\alpha_n) \in L^{G(L/K)} \;\Leftrightarrow\; \forall \sigma \in G(f,K):\ (-1)^{I(\sigma)} = 1 \;\Leftrightarrow\; G(f,K) \in \mathcal{A}_n\,.$$

Teil d) ist trivial. □

Wir kommen nun zur

Lösungsformel für das Polynom vom Grad 2:

Es sei K ein Körper mit $\text{char}(K) \neq 2$ und $f(X) = X^2 + pX + q \in K[X]$ irreduzibel und normiert vom Grad 2. Dann ist $G(f,K) = \mathfrak{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$ und damit $\sqrt{D} \notin K$ nach Satz 5.6.1. In einem Zerfällungskörper L sei $f(X) = (X-\alpha_1)(X-\alpha_2)$, dann ist

$$D \;=\; (\alpha_1 - \alpha_2)^2 \;=\; (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 \;=\; p^2 - 4q$$

und damit $L = K(\sqrt{p^2-4q})$. Aus $\alpha_1 - \alpha_2 = \pm\sqrt{D} = \pm\sqrt{p^2-4q}$ und $\alpha_1 + \alpha_2 = -p$ folgt die bekannte Lösungsformel

$$\alpha_1, \alpha_2 \;=\; \frac{-p \pm \sqrt{p^2-4q}}{2}\,.$$

Lösungsformel für das Polynom vom Grad 3:

Es sei K ein Körper mit $K^{(3)} \subseteq K$ und $\text{char}(K) \neq 2,3$ und $f(X) \in K[X]$ mit

$$f(X) \;=\; X^3 + b_2X^2 + b_1X + b_0$$

ein irreduzibles und normiertes Polynom vom Grad 3. Ein erster Schritt zum Auffinden einer Formel für die Nullstellen von $f(X)$ besteht in einer Vereinfachung des Polynoms. Durch die lineare Substitution $X := X^* - \frac{1}{3}b_2$ erhält man

$$f(X) \;=\; (X^* - \frac{1}{3}b_2)^3 + b_2(X^* - \frac{1}{3}b_2)^2 + b_1(X^* - \frac{1}{3}b_2) + b_0 \;=\; (X^*)^3 + pX^* + q$$

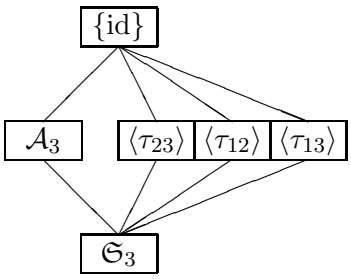
mit $p = b_1 - \frac{1}{3}b_2^2$ und $q = \frac{2}{27}b_2^3 - \frac{1}{3}b_1b_2 + b_0$. Wir können uns daher im Folgenden auf die Betrachtung von Polynomen der Form

$$f(X) \;=\; X^3 + pX + q$$

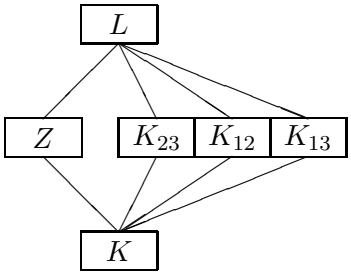
mit $p, q \in K$ beschränken und betrachten die Galoisgruppe $G(f, K)$. Nach Satz 5.3.3(c) ist $G(f, K)$ eine transitive Untergruppe von $\mathfrak{S}_3$. Man sieht leicht, dass die einzigen transitiven Untergruppen von $\mathfrak{S}_3$ die alternierende Gruppe $\mathcal{A}_3$ sowie $\mathfrak{S}_3$ selbst sind. Wir beschränken uns auf den komplizierteren Fall $G(f, K) \cong \mathfrak{S}_3$. Die sich hier ergebende Lösungsformel wird dann auch für den Fall $G(f, K) \cong \mathcal{A}_3$ gelten. Es sei L ein Zerfällungskörper von $f(X)$ über K. Zur Bestimmung der Zwischenkörper $L/Z/K$ wenden wir den Hauptsatz der Galoistheorie an. Der einzige nichttriviale Normalteiler sowie die einzige Untergruppe vom Index 2 ist $\mathcal{A}_3 \trianglelefteq \mathfrak{S}_3$. Nach dem Hauptsatz der Galoistheorie gibt es damit einen eindeutig bestimmten Zwischenkörper $Z = L^{\mathcal{A}_3}$ mit $[L : Z] = 2$. Nach Satz 5.6.1(c) ist $Z = K(\sqrt{D})$ ein solcher echter Zwischenkörper. Die weiteren nichttrivialen Untergruppen von $\mathfrak{S}_3$ sind sämtlich Gruppen der Ordnung 2, die von den Transpositionen

$$\tau_{12} \;=\; \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad , \quad \tau_{13} \;=\; \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad , \quad \tau_{23} \;=\; \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

erzeugt werden. Wir erhalten den Untergruppenverband



mit $\mathcal{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ bzw. gleichbedeutend den Zwischenkörperverband



mit $Z = K(\sqrt{D})$ vom Index $6/2 = 3$ in L. Insbesondere ist L/Z vom Grad 3, und damit eine zyklische Körpererweiterung:

$$(1) \;\; G(L/Z) \;\cong\; \langle\sigma\rangle \;\;,\;\; \mathrm{ord}(\sigma) = 3\,.$$

Diese Erweiterung lässt sich mittels der im Beweis von Satz 5.3.1 benutzten Lagrangeschen Resolventen gewinnen. Nach dem Satz vom primitiven Element gibt es ein $\gamma_0 \in L$ mit $L = K(\sqrt{D}, \gamma_0)$. Jeder der drei Automorphismen τ_{ij} ist eine Fortsetzung des Automorphismus

$$\tau :\; K(\sqrt{D}) \to K(\sqrt{D})\,,\; \sqrt{D} \mapsto -\sqrt{D}\,.$$

Wir definieren γ_1 durch $\gamma_1 := \tau_{12}(\gamma_0) = \tau_{13}(\gamma_0) = \tau_{23}(\gamma_0)$. Aus γ_0, γ_1 und σ bilden wir die Resolventen

$$\begin{aligned} \vartheta_0 &= \gamma_0 + \zeta_3\sigma(\gamma_0) + \zeta_3^2\sigma^2(\gamma_0) \\ \vartheta_1 &= \gamma_1 + \zeta_3\sigma(\gamma_1) + \zeta_3^2\sigma^2(\gamma_1) \quad . \end{aligned}$$

Wie im Beweis von Satz 5.3.1 ist $\beta_i = \vartheta_i^3 \in Z$ und $L = K(\sqrt{D}, \vartheta_i)$ jeweils für $i = 0, 1$. Aus der Relationstreue der Automorphismen folgt

$$\beta_0 \;=\; a_0 + a_1\sqrt{D} \;\;,\;\; \beta_1 \;=\; a_0 - a_1\sqrt{D}$$

mit $a_0, a_1 \in K$. Wir betrachten nun Basen der Erweiterungen L/Z und Z/K. Eine Basis für letztere Erweiterung ist offensichtlich $\{1, \sqrt{D}\}$. Eine Basis von L/Z ist $\{1, \vartheta_i, \vartheta_i^2\}$ jeweils für $i = 0$ und $i = 1$. Nach Satz 3.2.1 sind $B_i = \{1, \vartheta_i, \vartheta_i^2, \sqrt{D}, \sqrt{D}\vartheta_i, \sqrt{D}\vartheta_i^2\}$ Basen der Erweiterung L/K für $i = 0, 1$ und damit

$$L \;=\; \{(c_0 + c_1\sqrt{D}) + (c_2 + c_3\sqrt{D})\vartheta_i + (c_4 + c_5\sqrt{D})\vartheta_i^2 \mid c_0, \ldots, c_5 \in K\}\,.$$

Es sei nun

$$f(X) \;=\; X^3 + pX + q \;=\; (X - \alpha_0)(X - \alpha_1)(X - \alpha_2)$$

mit $\alpha_i \in L$. Dann gibt es eine eindeutige Darstellung

$$(2)\quad \alpha_0 \;=\; (c_0 + c_1\sqrt{D}) + (c_2 + c_3\sqrt{D})\vartheta_0 + (c_4 + c_5\sqrt{D})\vartheta_0^2$$

mit $c_j \in K$. Der Automorphismus σ aus (1) permutiert die Nullstellen α_i zyklisch, und es ist $\sigma(\vartheta_0) = \zeta_3^2\vartheta_0$. Nach eventueller Umordnung ist $\sigma(\alpha_0) = \alpha_2$ und $\sigma(\alpha_2) = \alpha_1$. Aus (2) folgt dann

$$\begin{array}{rcccccc} \alpha_1 & = & (c_{00} + c_{01}\sqrt{D}) & + & (c_{02} + c_{03}\sqrt{D})\zeta_3\vartheta_0 & + & (c_{04} + c_{05}\sqrt{D})\zeta_3^2\vartheta_0^2 \\ \alpha_2 & = & (c_{00} + c_{01}\sqrt{D}) & + & (c_{02} + c_{03}\sqrt{D})\zeta_3^2\vartheta_0 & + & (c_{04} + c_{05}\sqrt{D})\zeta_3\vartheta_0^2 \quad . \end{array}$$

Wegen $S_{L/K}(\alpha_0) = \alpha_0 + \alpha_1 + \alpha_2$ folgt $c_{00} = c_{01} = 0$. Aus (2) und $\beta_0 = a_0 + a_1\sqrt{D}$ folgt dann

$$\begin{array}{rcccccc} (3)\quad \alpha_0 & = & (c_{02} + c_{03}\sqrt{D})\sqrt[3]{a_0 + a_1\sqrt{D}} & + & (c_{04} + c_{05}\sqrt{D})(\sqrt[3]{a_0 + a_1\sqrt{D}})^2 \\ \alpha_1 & = & \zeta_3(c_{02} + c_{03}\sqrt{D})\sqrt[3]{a_0 + a_1\sqrt{D}} & + & \zeta_3^2(c_{04} + c_{05}\sqrt{D})(\sqrt[3]{a_0 + a_1\sqrt{D}})^2 \\ \alpha_2 & = & \zeta_3^2(c_{02} + c_{03}\sqrt{D})\sqrt[3]{a_0 + a_1\sqrt{D}} & + & \zeta_3(c_{04} + c_{05}\sqrt{D})(\sqrt[3]{a_0 + a_1\sqrt{D}})^2 \quad . \end{array}$$

Wir betrachten die Operationen der Automorphismen τ_{ij} der Ordnung 2. Wegen $Z = K(\sqrt{D}) \neq L^{\langle\tau_{ij}\rangle}$ ist $\tau_{ij}|_Z = \tau :\; Z \to Z,\; \sqrt{D} \mapsto -\sqrt{D}$. Für das Minimalpolynom von ϑ_0 über Z gilt

$$m_{\vartheta_0}(X) \;=\; (X - \sqrt[3]{a_0 + a_1\sqrt{D}}) \cdot (X - \sqrt[3]{a_0 + a_1\sqrt{D}}\zeta_3) \cdot (X - \sqrt[3]{a_0 + a_1\sqrt{D}}\zeta_3^2) \;=\; X^3 - (a_0 + a_1\sqrt{D})\,.$$

Nach Satz 3.3.2 sind die Elemente $\tau_{ij}(\sqrt[3]{a_0 + a_1\sqrt{D}})$ Nullstellen von

$$m_{\vartheta_0}^{(\tau_{ij})}(X) = X^3 - \tau_{ij}(a_0 + a_1\sqrt{D}) = (X - \sqrt[3]{a_0 - a_1\sqrt{D}}) \cdot (X - \sqrt[3]{a_0 - a_1\sqrt{D}}\zeta_3) \cdot (X - \sqrt[3]{a_0 - a_1\sqrt{D}}\zeta_3^2).$$

Daraus folgt

$$\tau_{ij}\left(\sqrt[3]{a_0 + a_1\sqrt{D}}\right) \;=\; \left(\sqrt[3]{a_0 - a_1\sqrt{D}}\right) \cdot \zeta_3^{l(i,j)} \quad l(i,j) \in \{0, 1, 2\}\,,$$

aber wegen $\tau_{ij}^2 = \mathrm{id}$ ist nur $l(i,j) = 0$ möglich, also

$$\tau_{ij}\left(\sqrt[3]{a_0 + a_1\sqrt{D}}\right) \;=\; \sqrt[3]{a_0 - a_1\sqrt{D}}\,.$$

Nun sei

$$\eta \;=\; \sqrt[3]{(a_0 + a_1\sqrt{D})(a_0 - a_1\sqrt{D})}\,,$$

dann ist $\tau_{ij}(\eta) = \eta$ für alle τ_{ij}. Da die Transpositionen aber die ganze Gruppe $G(L/K) \cong \mathfrak{S}_3$ erzeugen (Satz 1.6.3) gilt $\eta \in L^{G(L/K)} = K$. Wegen

$$\sqrt[3]{a_0 + a_1\sqrt{D}} \quad \cdot \quad \left(\sqrt[3]{a_0 + a_1\sqrt{D}}\right)^2 \quad \in \quad Z \;=\; K(\sqrt{D})$$

$$\sqrt[3]{a_0 + a_1\sqrt{D}} \quad \cdot \quad \sqrt[3]{a_0 - a_1\sqrt{D}} \quad \in \quad K$$

$$\Rightarrow \qquad (4) \qquad \sqrt[3]{a_0 - a_1\sqrt{D}} \quad = \quad (b_0 + b_1\sqrt{D}) \quad \cdot \quad \left(\sqrt[3]{a_0 + a_1\sqrt{D}}\right)^2$$

mit gewissen $b_0, b_1 \in K$. Wir beobachten ferner, dass τ_{ij} die Nullstellen α_i und α_j vertauscht und α_k mit $k \notin \{i, j\}$ fest lässt. Aus (3) und (4) folgt damit

$$\begin{aligned}
\alpha_0 &= (c_{02} + c_{03}\sqrt{D})\sqrt[3]{a_0 + a_1\sqrt{D}} + (d_{04} + d_{05}\sqrt{D})\sqrt[3]{a_0 - a_1\sqrt{D}} \\
\alpha_1 &= \zeta_3(c_{02} + c_{03}\sqrt{D})\sqrt[3]{a_0 + a_1\sqrt{D}} + \zeta_3^2(d_{04} + d_{05}\sqrt{D})\sqrt[3]{a_0 - a_1\sqrt{D}} \\
\alpha_2 &= \zeta_3^2(c_{02} + c_{03}\sqrt{D})\sqrt[3]{a_0 + a_1\sqrt{D}} + \zeta_3(d_{04} + d_{05}\sqrt{D})\sqrt[3]{a_0 - a_1\sqrt{D}} \quad ,
\end{aligned}$$

mit $d_{ij} \in K$. Für $A = (c_{02} + c_{03}\sqrt{D})^3(a_0 + a_1\sqrt{D}) \in Z$ sowie $B = (d_{04} + d_{05}\sqrt{D})^3(a_0 - a_1\sqrt{D}) \in Z$ gilt dann

$$\alpha_0 \;=\; \sqrt[3]{A} + \sqrt[3]{B} \quad , \quad \alpha_1 \;=\; \zeta_3\sqrt[3]{A} + \zeta_3^2\sqrt[3]{B} \quad , \quad \alpha_2 \;=\; \zeta_3^2\sqrt[3]{A} + \zeta_3\sqrt[3]{B}\,.$$

Wir bestimmen nun A und B durch Berechnung der elementarsymmetrischen Funktionen der α_i. Es ist

$$\begin{aligned}
N_{L/K}(\alpha_0) \;=\; \alpha_0\alpha_1\alpha_2 \;&=\; (\sqrt[3]{A} + \sqrt[3]{B}) \cdot (\zeta_3\sqrt[3]{A} + \zeta_3^2\sqrt[3]{B}) \cdot (\zeta_3^2\sqrt[3]{A} + \zeta_3\sqrt[3]{B}) \\
&=\; \zeta_3\zeta_3^2 \cdot (\sqrt[3]{A} + \sqrt[3]{B}) \cdot (\sqrt[3]{A} + \zeta_3\sqrt[3]{B}) \cdot (\sqrt[3]{A} + \zeta_3^2\sqrt[3]{B}) \;=\; A + B \quad .
\end{aligned}$$

Also folgt aus der Darstellung der Norm als Koeffizient im zugehörigen Minimalpolynom

$$(5) \quad A + B \;=\; \alpha_0\alpha_1\alpha_2 \;=\; -q\,.$$

Mit $s_2(X_0, X_1, X_2) = X_0X_1 + X_0X_2 + X_1X_2$ gilt ferner

$$\begin{aligned}
s_2(\alpha_0, \alpha_1, \alpha_2) \;&=\; (\sqrt[3]{A} + \sqrt[3]{B})(\zeta_3\sqrt[3]{A} + \zeta_3^2\sqrt[3]{B}) \\
&+\; (\sqrt[3]{A} + \sqrt[3]{B})(\zeta_3^2\sqrt[3]{A} + \zeta_3\sqrt[3]{B}) \\
&+\; (\zeta_3\sqrt[3]{A} + \zeta_3^2\sqrt[3]{B})(\zeta_3^2\sqrt[3]{A} + \zeta_3\sqrt[3]{B}) \\
&=\; (\sqrt[3]{A})^2 \cdot (1 + \zeta_3 + \zeta_3^2) \\
&+\; (\sqrt[3]{B})^2 \cdot (1 + \zeta_3 + \zeta_3^2) \\
&+\; 3\sqrt[3]{A}\sqrt[3]{B}(\zeta_3 + \zeta_3^2) \\
&=\; -3\sqrt[3]{A}\sqrt[3]{B}
\end{aligned}$$

wegen $\zeta_3^0 + \zeta_3^1 + \zeta_3^2 = 0$. Also gilt

$$(6) \quad \sqrt[3]{A}\sqrt[3]{B} \;=\; -\frac{1}{3}(\alpha_0\alpha_1 + \alpha_0\alpha_2 + \alpha_1\alpha_2) \;=\; -\frac{p}{3}\,.$$

Eine elementare aber etwas längliche Rechnung ergibt für die Diskriminante

$$D \;=\; -4p^3 - 27q2\,.$$

Daraus folgt:

$$A \;=\; -\frac{q}{2} + c\sqrt{D} \quad , \quad B \;=\; -\frac{q}{2} - c\sqrt{D}\,.$$

Einsetzen von (6) ergibt

$$A \;=\; -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad , \quad B \;=\; -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\,.$$

Wegen $\mathrm{char}(K) \neq 2,3$ sind alle Brüche wohldefiniert. Insgesamt folgt der

Satz 5.6.2 (Cardano)
Es sei K ein Körper mit $\mathrm{char}(K) \neq 2,3$ und $f(X) = X^3 + pX + q \in K[X]$. Dazu sei ζ_3 eine primitive dritte Einheitswurzel über K und

$$A = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \ , \quad B = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \, .$$

Die dritten Wurzeln $\sqrt[3]{A}$ und $\sqrt[3]{B}$ seien so gewählt, dass $\sqrt[3]{A}\sqrt[3]{B} = -\frac{p}{3}$ gilt. Dann sind die Lösungen der Gleichung $f(X) = 0$ gegeben durch

$$\alpha_0 = \sqrt[3]{A} + \sqrt[3]{B} \ , \quad \alpha_1 = \zeta_3\sqrt[3]{A} + \zeta_3^2\sqrt[3]{B} \ , \quad \alpha_2 = \zeta_3^2\sqrt[3]{A} + \zeta_3\sqrt[3]{B} \, .$$

5.7. Konstruktionen mit Zirkel und Lineal

Zunächst wollen wir präzisieren, was unter „Konstruktion mit Zirkel und Lineal“zu verstehen ist. Dazu identifizieren wir auf offensichtliche Weise die Punkte der Ebene mit den komplexen Zahlen $\mathbb{C}$, und sprechen künftig nur noch von der Konstruierbarkeit von komplexen Zahlen. Ist $z \in \mathbb{C}$ in der Darstellung $z = x + iy$ gegeben, so sei stets $x = \mathrm{Re}(z)$, $y = \mathrm{Im}(z)$ und $i^2 = -1$.

Definition 5.7.1
Wir betrachten die folgenden geometrischen Objekte:

(a) Es seien $u, v \in \mathbb{C}$ gegeben. Unter der Geraden durch u und v versteht man die Menge

$$\overline{uv} = \{u + \lambda(v - u) \mid \lambda \in \mathbb{R}\} \, .$$

(b) Es seien $p_0 \in \mathbb{C}$ und $r \in (0, \infty)$ gegeben. Unter dem Kreis um p_0 mit Radius r versteht man

$$k(p_0, r) = \{z \in \mathbb{C} \mid |z - p_0| = r\} \, .$$

Definition 5.7.2
Es sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ beliebig:

(a) Eine Teilmenge $l \subseteq \mathbb{C}$ heißt M-Gerade, falls es $u, v \in M$ mit $l = \overline{uv}$ gibt.
(b) Ein $k \subseteq \mathbb{C}$ heißt M-Kreis, falls es $p_0, u, v \in M$ mit $u \neq v$ und $k = k(p_0, |u - v|)$ gibt.

Definition 5.7.3
Es sei $M \subseteq \mathbb{C}$. Ein Punkt $z \in \mathbb{C}$ heißt aus M elementar konstruierbar, wenn z Schnittpunkt von

(i) zwei verschiedenen M-Geraden, oder
(ii) einer M-Gerade und einem M-Kreis, oder
(iii) zwei verschiedenen M-Kreisen ist.

Ein Punkt $z \in \mathbb{C}$ heißt aus M konstruierbar (mit Zirkel und Lineal), wenn es eine endliche Kette von Teilmengen $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r \subseteq \mathbb{C}$ mit $z \in M_r$ gibt, so dass jeder Punkt aus M_{j+1} elementar aus M_j konstruierbar ist für $j = 1 \ldots r$. Man setzt

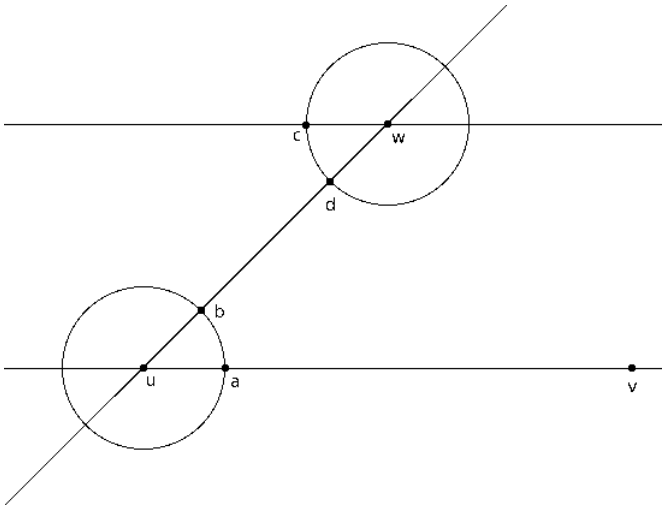
$$\mathrm{Kon}(M) = \{z \in \mathbb{C} \mid z \text{ aus } M \text{ konstruierbar}\} \, .$$

Lemma 5.7.1
Es sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $\overline{M} = \{z \in \mathbb{C} \mid \bar{z} \in M\}$ die konjugierte Menge. Dann gilt:

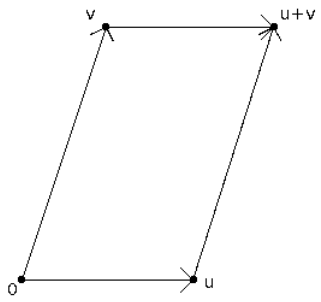
(a) *$\mathrm{Kon}(M) \subseteq \mathbb{C}$ ist ein Unterkörper von $\mathbb{C}$ mit $\mathbb{Q}(M \cup \overline{M}) \subseteq \mathrm{Kon}(M)$.*
(b) *Ist $b \in \mathbb{C}$ mit $b^2 \in \mathrm{Kon}(M)$, so gilt $b \in \mathrm{Kon}(M)$.*

Beweisskizze

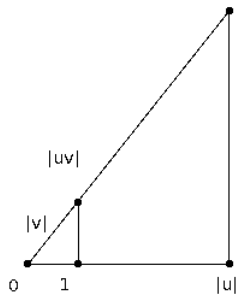
Wir skizzieren kurz die Konstruktionen, welche die Körpereigenschaften von $\mathrm{Kon}(M)$ beweisen. Es seien $u \neq v$ Elemente von M und $w \in M$ mit $w \notin \overline{uv}$ gegeben. Dann ist die Parallele zu $\overline{uv}$ durch w wie folgt konstruierbar:



Der Kreis $k(u, 1)$ schneide $\overline{uv}$ im Punkt a sowie $\overline{uw}$ im Punkt b. Der Kreis $k(w, 1)$ schneide $\overline{uw}$ im Punkt d. Schneidet dann der Kreis $k(d, |a - b|)$ den Kreis $k(w, 1)$ im Punkt c, so ist $\overline{cw}$ die gesuchte Parallele. Die Addition von $u, v \in M$ lässt sich mittels eines Parallelogramms durchführen:



Da sich $-u$ für $u \in M$ konstruieren lässt, können auch Differenzen $u - v$ konstruiert werden. Die Multiplikation von $u, v \in M$ ergibt sich durch Winkeladdition und Multiplikation der Beträge. Letztere kann mittels des Strahlensatzes durchgeführt werden:



Ebenso lässt sich $\sqrt{z}$ konstruieren. Man überlegt sich leicht, dass man von einem Punkt $z \notin l$ das Lot auf die Gerade l fällen kann. Damit lässt sich $\bar{z}$ aus z konstruieren. Für $r > 0$ lässt sich $\sqrt{r}$ aus r mittels des Höhensatzes konstruieren. Die Quadratwurzel aus $c = b^2 \in \mathbb{C}$ erhält man nun durch die Winkelhalbierende und Konstruktion von $\sqrt{|c|}$. □

LEMMA 5.7.2
Es sei $L \subseteq \mathbb{C}$ ein Unterkörper mit $L = \overline{L}$ und $i \in L$. Ist $z \in \mathbb{C}$ elementar aus L konstruierbar, so gibt es $w \in \mathbb{C}$ mit $w^2 \in L$ und $z \in L(w)$.

BEWEIS
Wegen $L = \overline{L}$ gilt für $p \in L$ stets

$$\mathrm{Re}(p) \;=\; \frac{p+\bar{p}}{2} \;\in\; L \quad , \quad \mathrm{Im}(p) \;=\; \frac{p-\bar{p}}{2} \;\in\; L\,.$$

Es sei also $z \in \mathbb{C}$ aus L elementar konstruierbar. Nach Definition 5.7.3 kann diese Konstruktion auf drei Weisen erfolgen:

(i) z ist der Schnittpunkt von zwei L-Geraden l_1 und l_2. Aus Definition 5.7.1 folgt leicht, dass die Gleichungen von l_1 und l_2 in der Form

$$a_j x + b_j y \;=\; c_j \qquad a_j, b_j, c_j \in L$$

für $j = 1, 2$ geschrieben werden können. Es liegen $\mathrm{Re}(z)$ sowie $\mathrm{Im}(z)$ in L, damit auch z.

(ii) z ist der Schnittpunkt einer L-Geraden $\overline{uv}$ mit einem L-Kreis $k = k(p_0, r)$ für $r = |s - t|$ mit $p_0, s, t \in L$. Es ist $r^2 = (\mathrm{Re}(s-t))^2 + (\mathrm{Im}(s-t))^2 \in L$. Zudem ist

$$(*) \quad z \;=\; s + \lambda(t - s) \quad (\lambda \in \mathbb{R})\,.$$

Aus $|z - p_0|^2 = r^2$ folgt

$$r^2 \;=\; (\lambda \mathrm{Re}(t-s) + \mathrm{Re}(s-p_0))^2 + (\lambda \mathrm{Im}(t-s) + \mathrm{Im}(s-p_0))^2\,.$$

Damit ist λ Nullstelle eines Polynoms $f(X) \in L[X]$ mit $\deg(f) = 2$. Also $\lambda \in L(\sqrt{D})$ mit $D = D(f) \in L$, mit $(*)$ folgt $z \in L(\sqrt{D})$.

(iii) z ist der Schnittpunkt zweier L-Kreise: $z \in k_1 \cap k_2$ mit

$$k_j \;=\; k(a_j + ib_j, r_j) \quad a, b_j, r_j^2 \in L\,.$$

Es erfüllt $z = x + iy$ die Gleichungen

$$(x - a_1)^2 \;+\; (y - b_1)^2 \;=\; r_1^2$$

$$(x - a_2)^2 \;+\; (y - b_2)^2 \;=\; r_2^2$$

und damit auch die Geradengleichung $(a_1 - a_2)x + (b_1 - b_2)y = c$. Somit ist z Schnittpunkt einer L-Geraden mit einem L-Kreis, und die Behauptung folgt aus (ii).

□

Satz 5.7.3
Es sei $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$. Für $z \in \mathbb{C}$ sind äquivalent:

(i) $z \in \mathrm{Kon}(M)$.
(ii) *Es gibt einen Körperturm $\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq \cdots \subseteq L_r \subseteq \mathbb{C}$ mit $z \in L_r$ und $[L_{j+1} : L_j] = 2$.*

Beweis
$(ii) \Rightarrow (i)$:
Wir beweisen durch Induktion nach j: $L_j \subseteq \mathrm{Kon}(M)$. Der Fall $j = 0$ ist durch Lemma 5.7.1(a) gezeigt. Ist $z \in L_j - L_{j-1}$ beliebig, so gilt $L_j = L_{j-1}(z)$ und es gibt $a, b \in L_{j-1}$ mit $z^2 + az + b = 0$. Somit ist $(z+\frac{1}{2}a)^2 \in L_{j-1}$, woraus $L_j = L_{j-1}(z+\frac{1}{2}a)$ folgt. Nach Lemma 5.7.1 ist $x+\frac{1}{2}a$ aus L_{j-1} konstruierbar, also $L_j \subseteq \mathrm{Kon}(M)$, da $\mathrm{Kon}(M)$ ein Körper ist.

$(i) \Rightarrow (ii)$:
Ist $z \in \mathrm{Kon}(M)$, so gibt es eine Kette von Teilmengen $M = M_0 \subseteq \cdots \subseteq M_r \subseteq \mathbb{C}$, so dass M_j aus M_{j-1} jeweils elementar konstruierbar ist und $z \in M_r$ gilt. Wir machen ferner folgende Beobachtung: Bei der elementaren Konstruktion von M_j aus M_{j-1} werden höchstens 6 Punkte von M_{j-1} verwendet: bei dem Schnitt zweier M_{j-1}-Kreise werden die zwei Mittelpunkte sowie vier Punkte für die Radien benutzt. Bei den anderen Konstruktionen werden weniger als sechs Punkte verwendet. Ohne Einschränkung kann angenommen werden, dass $|M_j - M_{j-1}| < \infty$ ist. Es sei $L_0 = \mathbb{Q}(M \cup \overline{M} \cup \{i\})$. Damit erfüllt L_0 die Voraussetzungen von Lemma 5.7.2. Es sei $M_1 = M_0 \cup \{z_{1,1}, \ldots, z_{1,m_1}\}$. Da die $z_{1,k}$ für $k = 1 \ldots m_1$ elementar aus M_0 konstruierbar sind, gibt es nach Lemma 5.7.2 Elemente $w_{1,k}$ mit $w_{1,k}^2 \in L_0$ und $z_{1,k} \in L_0(w_{1,k})$. Es sei $L_1 = L_0(w_{1,1}, \ldots, w_{1,m_1}, \bar{w}_{1,1}, \ldots, \bar{w}_{1,m_1})$. Dann erfüllt auch L_1 die Bedingungen von Lemma 5.7.2, und es ist $[L_1 : L_0] = 2^{n_1}$. Nun seien $L_1, \ldots, L_{d-1}$ schon konstruiert, so dass $M_j \subseteq L_j$ sowie $[L_j : L_{j-1}] = 2^{n_j}$ für $1 \leq j \leq d-1$ gilt. Die L_j mögen jeweils die Voraussetzungen von Lemma 5.7.2 erfüllen. Es sei $M_d = M_{d-1} \cup \{z_{d,1}, \ldots, z_{d,m_d}\}$. Wiederum gibt es nach Lemma 5.7.2 Elemente $w_{d,k} \in \mathbb{C}$ mit $w_{d,k}^2 \in L_{d-1}$ und $z_{d,k} \in L_{d-1}(w_{d,k})$. Wir setzen $L_d = L_{d-1}(w_{d,1}, \ldots, w_{d,m_d}, \bar{w}_{d,1}, \ldots, \bar{w}_{d,m_d}\}$, dann ist $[L_d : L_{d-1}] = 2^{n_d}$. Somit erhält man einen Körperturm mit den gewünschten Eigenschaften. □

Satz 5.7.4
Es sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $L = \mathbb{Q}(M \cup \overline{M})$. Ist $z \in \mathrm{Kon}(M)$, so ist z algebraisch über L und $[L(z) : L]$ ist eine Potenz von 2.

Beweis
Dies folgt unmittelbar aus Satz 5.7.3. □

Wir wollen diese Betrachtungen zunächst auf die Frage der Konstruierbarkeit des regelmäßigen n-Ecks anwenden. Hier spielen die Fermatschen Primzahlen eine entscheidende Rolle:

Definition 5.7.4
Für $n \in \mathbb{N}$ heißt $F_n = 2^{(2^n)} + 1$ die n-te Fermatsche Zahl.

Es gilt $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sowie

$$F_5 \;=\; 2^{32} + 1 \;=\; 4294967297 \;=\; 641 \cdot 6700417\,.$$

Die Zahlen $F_0, \ldots, F_4$ sind Primzahlen, jedoch ist F_5 nicht prim. Es ist auch keine weitere Primzahl unter den F_n bekannt. Es ist auch nicht bekannt, ob es unendlich viele Primzahlen unter den F_n gibt.

Bemerkung 5.7.1
Ist p eine ungerade Primzahl der Form $p = 2^m + 1$, so ist p eine Fermatsche Zahl.

Beweis
Ist $m = l \cdot q$ mit $q > 2$ ungerade, so gilt

$$p \;=\; 2^{lq} + 1 \;=\; (2^l + 1) \cdot (2^{l(q-1)} - \cdots - 2^l + 1) \;=\; (2^l + 1) \cdot \sum_{j=0}^{q-1} (-2^l)^j \,,$$

und p ist keine Primzahl, also ist nur $m = 2^k$ für ein $k \in \mathbb{N}_0$ möglich. □

Satz 5.7.5 (Gauß)
Es sei $n \geq 3$ eine natürliche Zahl. Dann sind äquivalent:

(i) *Das regelmäßige n-Eck ist mit Zirkel und Lineal konstruierbar.*
(ii) *$\varphi(n)$ ist eine Potenz von 2,*
(iii) *$n = 2^m \cdot p_1 \cdots p_r$, wobei $p_1, \ldots, p_r$ paarweise verschiedene Fermatsche Primzahlen sind.*

Beweis
Die Konstruktion des regelmäßigen n-Ecks ist offenbar äquivalent zur Konstruktion der n-ten primitiven Einheitswurzel $\zeta_n = e^{\frac{2\pi i}{n}}$.

$\underline{(i) \Rightarrow (ii)}$:
Nach Satz 4.1.6 ist $m_{\zeta_n}(X) = \Phi_n(X)$, also $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Aus Satz 5.7.4 folgt, dass $\varphi(n)$ eine Potenz von 2 ist.

$\underline{(ii) \Leftrightarrow (iii)}$:
Ist $n = 2^{e_0} \cdot p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von n, so gilt

$$\varphi(n) \;=\; 2^{e_0 - 1} \cdot p_1^{e_1 - 1} \cdots p_r^{e_r - 1} \cdot (p_1 - 1) \cdots (p_r - 1) \,.$$

Somit ist $\varphi(n)$ genau dann eine Potenz von 2, wenn $e_1 = \cdots = e_r = 1$ und jeweils $p_j - 1$ eine Zweierpotenz ist. Nach Bemerkung 5.7.1 ist letzteres äquivalent dazu, dass die p_j Fermatsche Primzahlen sind.

$\underline{(ii) \Rightarrow (i)}$:
Die Erweiterung $\mathbb{Q}(\zeta_n)/Q$ ist galoissch mit Galoisgruppe $G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Insbesondere ist $|G(\mathbb{Q}(\zeta_m)/\mathbb{Q})| = \varphi(n)$, also ist die Galoisgruppe wegen (ii) eine 2-Gruppe (Definition 1.8.7). Nach den Sätzen 1.9.5 und 1.9.6 besitzt $G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ eine Normalreihe

$$G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \;=\; G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m \;=\; \{\mathrm{id}\}$$

mit $[G_{j-1} : G_j] = 2$. Der Turm der zugehörigen Fixkörper

$$\mathbb{Q} \;=\; \mathbb{Q}(\zeta_n)^{G_0} \;\subseteq\; \mathbb{Q}(\zeta_n)^{G_1} \;\subseteq\; \cdots \;\subseteq\; \mathbb{Q}(\zeta_n)^{G_m} \;=\; \mathbb{Q}(\zeta_n)$$

erfüllt die Bedingungen von Satz 5.7.3. Damit ist $\zeta_n \in \mathrm{Kon}(\{0, 1\})$. □

Mit Satz 5.7.4 können auch die klassischen Konstruktionsprobleme der alten Griechen beantwortet werden:

Satz 5.7.6 (Unlösbarkeit der klassischen Konstruktionsprobleme)
Die folgenden Konstruktionsprobleme sind unlösbar:

(a) *Die Dreiteilung des Winkels,*
(b) *die Würfelverdopplung,*
(c) *die Quadratur des Kreises.*

Beweis
Wir können nur (a) und (b) beweisen. Teil (a) folgt beispielsweise aus der Unmöglichkeit der Konstruktion des regelmäßigen 9-Ecks, welche sich als Spezialfall von Satz 5.7.5 ergibt. Zu (b): Wegen $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist die Verdopplung des Würfels nach Satz 5.7.5 unmöglich. Zu (c): Es geht um die Konstruktion eines Quadrats, dessen Flächeninhalt dem eines vorgegebenen Kreises entspricht, also um die Konstruktion von $\sqrt{\pi}$ aus $\{0, 1\}$. Das ist unmöglich, weil π transzendent ist. Dies wurde von Lindemann 1882 bewiesen. Der Beweis liegt außerhalb des Rahmens dieser Vorlesung. □

6. Algebraische Zahlentheorie

6.1. Moduln

DEFINITION 6.1.1
Es sei R ein Ring, M eine Menge.

(a) Man sagt: R operiert auf M (von links), wenn eine Abbildung
$$R \times M \ \to \ M \ , \ (r, m) \mapsto rm$$
gegeben ist mit
- $1m = m$ für alle $m \in M$,
- $r_1(r_2 m) = (r_1 r_2)m$ für alle $m \in M$ und $r_1, r_2 \in R$.

(b) Eine abelsche Gruppe $(M, +)$ heißt R-(Links-)Modul, falls R (von links) auf M operiert und zusätzlich gilt:
- $(r_1 + r_2)m = r_1 m + r_2 m$ für alle $r_1, r_2 \in R$ und $m \in M$,
- für jedes $r \in R$ ist die Abbildung $\Phi(r) : \ M \to M, \ m \mapsto rm$ ein Homomorphismus von $(M, +)$, also
$$r(m_1 + m_2) = rm_1 + rm_2 \ , \ \forall m_1, m_2 \in M \ .$$

(c) M_1 und M_2 seien R-Moduln. Die Abbildung $\varphi : \ M_1 \to M_2$ heißt R-Modulhomomorphismus, falls φ ein Homomorphismus der abelschen Gruppen $(M_1, +)$ und $(M_2, +)$ ist und $\varphi(rm) = r\varphi(m)$ für alle $r \in R$ und $m \in M$ gilt.

(d) Es sei M ein R-Modul. Eine Teilmenge $N \subseteq M$ heißt Untermodul von M, falls $(N, +)$ eine Untergruppe von $(M, +)$ ist und $rn \in N$ für alle $r \in R$ und $n \in N$ gilt.

BEISPIEL 6.1.1
Es gibt zwei wichtige Spezialfälle von Moduln:

(a) Ist K ein Körper und $R = K$, dann sind die K-Moduln gerade die aus der Linearen Algebra bekannten Vektorräume über K. Die Modulhomomorphismen zwischen zwei Vektorräumen V_1 und V_2 über K sind gerade die linearen Abbildungen von V_1 und V_2.

(b) Ist M eine abelsche Gruppe, so ist M ein $\mathbb{Z}$-Modul mit der Operation
$$zm \ := \begin{cases} 0_M & \text{falls} \quad z = 0_{\mathbb{Z}} \\ \underbrace{m + \cdots + m}_{z-\text{mal}} & \text{falls} \quad z > 0 \\ -(\underbrace{m + \cdots + m}_{|z|-\text{mal}}) & \text{falls} \quad z < 0 \end{cases}$$

DEFINITION 6.1.2
Es sei R ein Ring, M ein R-Modul, $S \in M$ eine Teilmenge von M. Unter dem von S erzeugten Untermodul von M (Schreibweise $\langle S \rangle$) versteht man
$$\langle S \rangle \ = \bigcap_{\substack{N \subseteq M \ \text{Untermodul} \\ S \subseteq N}} N \, .$$
Ist $\langle S \rangle = M$, so heißt S ein Erzeugendensystem von M über R. M heißt endlich erzeugt, wenn es ein endliches Erzeugendensystem besitzt.

BEMERKUNG 6.1.1
Man sieht unmittelbar
$$\langle S \rangle \ = \ \left\{ \sum_{i=1}^{n} r_i s_i \mid r_i \in N \ , \ s_i \in S \ , \ n \in \mathbb{N} \right\} \, .$$

Definition 6.1.3
Es sei R ein Ring und M ein R-Modul. Ein Erzeugendensystem B von M heißt Basis (von M über R), falls aus $r_1b_1 + \cdots + r_nb_n = 0$ mit $r_i \in R$, paarweise verschiedenen $b_i \in B$ und $n \in \mathbb{N}$ stets $r_i = 0$ für alle i folgt. M heißt frei, falls M eine Basis besitzt.

Bemerkung 6.1.2
Man sieht unmittelbar, dass aus der Existenz einer Basis B die eindeutige Darstellbarkeit von jedem $m \in M$ in der Form $m = r_1b_1 + \cdots + r_nb_n$ folgt.

Satz 6.1.1
Es sei R ein Ring und $n \in \mathbb{N}$. Dann gibt es einen freien Modul M über R mit einer Basis der Mächtigkeit n.

Beweis
Es sei $M = \{(x_1, \ldots, x_n) \mid x_i \in R\}$ sowie $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit der Eins an der i-ten Stelle. Dann ist $B = \{e_1, \ldots, e_n\}$ eine Basis der gewünschten Form. □

Definition 6.1.4
Es sei R ein Ring, M und M' seien Moduln über R mit Basen $B = \{b_1, \ldots, b_n\}$ bzw. $B' = \{b'_1, \ldots, b'_m\}$. Es sei $\varphi : M \to M'$ ein Modulhomomorphismus und $a_{ij} \in R$ mit $1 \leq i \leq m$, $1 \leq j \leq n$ eindeutig bestimmt durch

$$\varphi(b_j) = \sum_{i=1}^{m} a_{ij} b'_i \,.$$

Dann heißt die Matrix $A = (a_{ij}) \in R^{(m,n)}$ die zum Homomorphismus φ bzgl. der Basen B und B' gehörige Matrix. Schreibweise: $A = \mathcal{M}(\varphi, B, B')$.

Satz 6.1.2
Es sei R ein Ring und M, M', M'' Moduln über R mit Basen B, B' und B''. Es seien $\varphi_1 : M \to M'$ bzw $\varphi_2 : M' \to M''$ Modulhomomorphismen mit zugehörigen Matrizen $A_1 = \mathcal{M}(\varphi_1, B, B')$ und $A_2 = \mathcal{M}(\varphi_2, B', B'')$. Dann gehört zum Modulhomomorphismus $\varphi_2 \circ \varphi_1 : M \to M''$ bzgl. der Basen B und B'' die Matrix $\mathcal{M}(\varphi_2 \circ \varphi_1, B, B'') = A_2 \cdot A_1$.

Beweis
Wie in der Linearen Algebra durch Nachrechnen. □

Definition 6.1.5
Es sei R ein Ring und $n \in \mathbb{N}$. Die Einheitsmatrix E_n vom Typ (n, n) ist

$$E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} .$$

Eine Matrix $A \in R^{(n,n)}$ heißt invertierbar, wenn es $A' \in R^{(n,n)}$ gibt mit $A \cdot A' = E_n$ oder $A' \cdot A = E_n$.

Satz 6.1.3
Es sei R ein Ring. Ein $A \in R^{(n,n)}$ ist invertierbar genau dann, wenn es $A^{-1} \in R^{(n,n)}$ gibt mit $AA^{-1} = A^{-1}A = E_n$.

Beweis
Es sei M der nach Satz 6.1.1 existierende Modul über R mit einer Basis B mit $|B| = n$. Es sei $\varphi : M \to M$ definiert durch $\mathcal{M}(\varphi, B, B) = A$. Dann ist A invertierbar genau dann, wenn die Abbildung φ es ist. $A^{-1} = \mathcal{M}(\varphi^{-1}, B, B)$ ist die gesuchte Matrix. □

Definition 6.1.6
Die Matrix A^{-1} aus Satz 6.1.3 heißt die zu A inverse Matrix.

Wir nehmen im Folgenden an, dass R ein Hauptidealring ist. Manche der Aussagen gelten auch unter allgemeineren Voraussetzungen.

Satz 6.1.4
Es sei M ein Modul über R mit einer Basis der Mächtigkeit n, dann hat jede endliche Basis von M die Mächtigkeit n.

Beweis
Es sei $B = \{b_1, \ldots, b_n\}$ eine Basis von M, $\mathfrak{m}$ ein maximales Ideal von R. Dann ist die Faktorgruppe $(M/\mathfrak{m}M, +)$ offenbar ein Modul über dem Körper $R/\mathfrak{m}$, also ein Vektorraum. Man sieht leicht, dass $B' = \{b_1 + \mathfrak{m}M, \ldots, b_n + \mathfrak{m}M\}$ eine Basis von $M/\mathfrak{m}M$ über $R/\mathfrak{m}$ ist. Aus der Linearen Algebra ist bekannt, dass n eindeutig bestimmt ist. □

Definition 6.1.7
Es sei M ein freier R-Modul mit einer endlichen Basis. Die nach Satz 6.1.4 eindeutig bestimmte Mächtigkeit jeder endlichen Basis von M heißt die Dimension von M über R (Schreibweise: $\dim(M)$ oder $\dim_R(M)$).

Wir untersuchen als nächstes die Beziehung zwischen verschiedenen Basen eines freien, endlich erzeugten Moduls. Es seien $B_1 = \{b_1, \ldots, b_n\}$ und $B_2 = \{b'_1, \ldots, b'_n\}$ zwei Basen des Moduls M über R. Dann gibt es Elemente $a_{ij} \in R$ $(1 \leq i \leq n,\ 1 \leq j \leq n)$ mit

$$b'_i \;=\; \sum_{j=1}^{n} a_{ij} b_j \,.$$

Wir betrachten die Matrix $A = (a_{ij})$. Dann ist

$$\begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} \;=\; A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \,.$$

Satz 6.1.5
Es sei M ein freier R-Modul mit der Basis $B = \{b_1, \ldots, b_n\}$. Dazu sei $B' = \{b'_1, \ldots, b'_n\}$ für ein $A \in R^{(n,n)}$ mit

$$\begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} \;=\; A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \,.$$

Dann gilt: B' ist Basis von $M \;\Leftrightarrow\; A$ ist invertierbar.

Beweis
Hinrichtung: B' sei Basis von M, dann gibt es $\tilde{A} \in R^{(n,n)}$, so dass

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \;=\; \tilde{A} \cdot \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} \;=\; \tilde{A} \cdot A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \,.$$

Es folgt: $\tilde{A}A = E_n$, also ist A invertierbar.
Rückrichtung: Es sei A invertierbar, dann ist

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \;=\; A^{-1} \cdot \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} \,,$$

d. h. B' ist ein Erzeugendensystem. Es bleibt die lineare Unabhängigkeit zu zeigen. Es gelte $r_1 b'_1 + \cdots + r_n b'_n = 0$, zu zeigen ist $r_1 = \cdots = r_n = 0$. Es folgt

$$(r_1, \ldots, r_n) \cdot A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \;=\; 0\,,$$

und damit $(r_1, \ldots, r_n) \cdot A = (0, \ldots, 0)$, da B eine Basis ist. Damit gilt aber auch $(r_1, \ldots, r_n) \cdot A \cdot A^{-1} = (r_1, \ldots, r_n) = (0, \ldots, 0)$. □

Satz 6.1.6
Es sei M ein R-Modul mit $\dim_R(M) = n$ und N ein Untermodul von M. Dann hat auch N eine endliche Basis und es ist $\dim_R(N) \leq \dim_R(M) = n$.

Beweis
Es sei $B = \{b_1, \ldots, b_n\}$ eine Basis von M und

$$N_m \;=\; N \cap \langle \{b_1, \ldots, b_m\} \rangle$$

für $1 \leq m \leq n$. Wir zeigen durch Induktion: $N_m = \{0\}$ oder N_m besitzt eine endliche Basis und $\dim_R(N_m) \leq m$.

$\underline{m = 1:}$
Es sei $N_1 = \{s_1 b_1 \mid s_1 \in I_1\}$. Aus der Moduleigenschaft von N_1 folgt sofort, dass I_1 ein Ideal von R ist. Da R ein Hauptidealring ist, folgt $I_1 = (r_1) = \{r_1 t \mid t \in R\}$. Ist $r_1 = 0_R$, so ist $N_1 = \{0\}$. Andernfalls ist $N_1 = \langle r_1 b_1 \rangle$ mit Basis $B_1 = \{r_1 b_1\}$.

$\underline{m - 1 \to m:}$
Es sei $N_{m-1} = \{0\}$ oder andernfalls $B_{m-1} = \{c_1, \ldots, c_{m-1}\}$ eine Basis von N_{m-1}. Es sei I_m die Menge aller $s_j \in R$, so dass $x \in N$ existiert mit $x = s_1 b_1 + \cdots + s_{m-1} b_{m-1} + s_m b_m$. Aus der Moduleigenschaft von N_m folgt wiederum, dass I_m ein Ideal ist. Also $I_m = \{0\}$ oder $I_m = (r_m) = \{r_m t \mid t \in R\}$. Ist $I_m = \{0\}$, so ist $N_m = N_{m-1}$ und die zu zeigende Aussage gilt nach der Induktionshypothese. Es sei $x \in N_m$ und $r_m \neq 0$ und $w_m \in N_m$ so gewählt, dass $w_m = u_1 b_1 + \cdots + u_{m-1} b_{m-1} + r_m b_m$ gilt. Dann gibt es $t \in R$, so dass $x - t w_m \in N_{m-1}$. Dies zeigt, dass $B_{m-1} \cup \{w_m\}$ eine Basis von N_m ist. □

6.2. Noethersche Ringe

Definition 6.2.1
Ein kommutativer Ring R heißt Noethersch, falls jedes Ideal ein endliches Erzeugendensystem besitzt, d. h. Ist $I \trianglelefteq R$, so gibt es $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in I$, so dass

$$I \;=\; (a_1, \ldots, a_n) \;=\; \bigcap_{\substack{J \trianglelefteq R \\ a_1, \ldots, a_n \in J}} J\,.$$

Bemerkung 6.2.1
Es ist also $I = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$.

Beispiel 6.2.1
Jeder Hauptidealring ist Noethersch. Andererseits ist $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring, dennoch ist dieser Ring Noethersch (Beweis später).

Im Folgenden sei R stets ein kommutativer Ring.

Satz 6.2.1
Folgende Aussagen sind äquivalent:

(i) *R ist Noethersch,*
(ii) *Es gilt der Teilerkettensatz für Ideale: Es gibt keine unendliche echt aufsteigende Kette* $I_1 \subsetneq I_2 \subsetneq \cdots$ *von Idealen in R.*
(iii) *Es gilt die Maximalbedingung für Ideale: Jede nichtleere Menge* $\mathcal{I}$ *von Idealen von R enthält ein maximales Element, d. h. es gibt ein* $I \in \mathcal{I}$*, das in keinem anderen Ideal von* $\mathcal{I}$ *enthalten ist.*

Beweis
$(i) \Rightarrow (ii)$:
Sei $I_1 \subsetneq I_2 \subsetneq \cdots$ eine unendliche echt aufsteigende Kette von Idealen. Auch die unendliche Vereinigung

$$I = \bigcup_{j \in \mathbb{N}} I_j$$

ist ein Ideal von R, und wegen (i) wird es von endlich vielen Elementen $a_1, \ldots, a_m \in R$ erzeugt. Für jedes k gibt es ein i_k, so dass a_k in I_{i_k} und damit in allen Nachfolgern liegt. Für $j = \max(i_1, \ldots, i_m)$ liegen also alle Erzeuger in I_j, woraus $I_j \supseteq I$ und damit $I_j = I$ folgt. Dann ist $I_{i+1} \supsetneq I_i = I$ ein Widerspruch zur Definition von I.

$(ii) \Rightarrow (iii)$:
Eine Menge $\mathcal{I}$ von Idealen von R verletze die Maximalbedingung. Sei $I_1 \in \mathcal{I}$, dann existiert $I_2 \in \mathcal{I}$ mit $I_1 \subsetneq I_2$. Dazu gibt es $I_3 \in \mathcal{I}$ mit $I_2 \subsetneq I_3$, und so weiter. Die Kette $I_1 \subsetneq I_2 \subsetneq \cdots$ ist dann ein Widerspruch zu (ii).

$(iii) \Rightarrow (ii)$:
Folgt mit der Wahl $\mathcal{I} = \{I_j \mid j \in \mathbb{N}\}$ für eine unendliche echt aufsteigende Kette (I_j).

$(ii) \Rightarrow (i)$:
Es sei $I \trianglelefteq R$. Ist I nicht endlich erzeugbar, so existiert eine unendliche Folge $a_i \in R$ mit $(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots$ im Widerspruch zu (ii). □

6.3. Ganzheit

Definition 6.3.1
Ein algebraischer Zahlkörper ist eine endliche Erweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen. Eine algebraische Zahl heißt ganz, wenn sie Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[X]$ ist. Die Menge der ganzen Zahlen eines algebraischen Zahlkörpers wird mit $\mathcal{O}_K$ bezeichnet.

Man kann zeigen, dass $\mathcal{O}_K$ ein Ring ist. Dieser hat mit dem Ring $\mathbb{Z}$ der gewöhnlichen ganzen Zahlen (den ganzen Zahlen den Körpers $\mathbb{Q}$) manche Eigenschaften gemeinsam. Einige dieser Eigenschaften gelten für alle, andere nur für spezielle Zahlkörper. Viele Begriffe im Ring $\mathbb{Z}$ (Teilbarkeit, Zerlegung in Primelemente) lassen sich auf $\mathcal{O}_K$ übertragen. Die „Arithmetik in $\mathcal{O}_K$“bildet den Gegenstand der algebraischen Zahlentheorie. Es empfiehlt sich (aus mehreren Gründen) den Begriff der Ganzheit in größerer Allgemeinheit zu behandeln. Die im Folgenden auftretenden Ringe werden als kommutativ vorausgesetzt.

Definition 6.3.2
Es sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt ganz über A, wenn es Nullstelle eines normierten Polynoms $f \in A[X]$ mit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ und $n \geq 1$ ist. Der Ring B heißt ganz über A, wenn alle Elemente $b \in B$ ganz über A sind.

Man erwartet, dass die Menge der Elemente, die über A ganz sind, einen Ring bilden. Diese Tatsache ist nicht unmittelbar, sondern folgt mit Hilfe der Modultheorie.

Satz 6.3.1
Endlich viele $b_1, \ldots, b_n \in B$ sind genau dann sämtlich ganz über A, wenn der Ring $A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt ist.

Als Vorbereitung benutzen wir

Lemma 6.3.2 (Entwicklungssatz von Laplace)
Es sei R ein kommutativer Ring und $n \in \mathbb{N}$. Es sei $A = (a_{ij}) \in R^{(n,n)}$. Dazu sei $A^* = (a^*_{ij})$ die adjungierte Matrix, d. h. $a^*_{ij} = (-1)^{i+j} \cdot \det(A_{ij})$, wobei A_{ij} die Teilmatrix ist, die durch Streichung von Zeile j und Spalte i aus A entsteht. Dann gilt

$$A \cdot A^* \;=\; A^* \cdot A \;=\; \det(A) \cdot E_n \,.$$

Für $\vec{x} \in R^n$ gilt: $A\vec{x} = \vec{0} \;\Rightarrow\; (\det(A))\vec{x} = \vec{0}$.

Beweis
Der Beweis aus der Linearen Algebra, in dem R als Körper vorausgesetzt wird, benutzt die Leibniz-Formel

$$\det(A) \;=\; \sum_{\pi \in \mathfrak{S}_n} \operatorname{sgn}(\pi) \prod_{j=1}^{n} a_{j,\pi(j)}$$

und kann auf beliebige kommutative Ringe R übertragen werden. □

Lemma 6.3.3
Es sei $R \subseteq S$ eine Ringerweiterung und M ein S-Modul. Ist S endlich erzeugt als R-Modul und M endlich erzeugt über S, so ist M auch endlich erzeugt als R-Modul.

Beweis
Es sei $\mathcal{S} = \{s_1, \ldots, s_r\}$ ein Erzeugendensystem von S über R sowie $\mathcal{T} = \{t_1, \ldots, t_l\}$ ein Erzeugendensystem von M über S. Dann ist $\mathcal{U} = \{s_i t_j \mid 1 \le i \le r \;,\; 1 \le j \le l\}$ ein Erzeugendensystem von M über R. □

Beweis zu Satz 6.3.1
Hinrichtung:
Wir beweisen die Behauptung durch Induktion nach n. Fall $n = 1$: Es sei $b \in B$ ganz über A und $f \in A[X]$ normiert vom Grad $n \ge 1$ mit $f(b) = 0$. Ist $g \in A[X]$, so gibt es $q(X), r(X) \in A[X]$ mit $\deg(r) < n$ so dass $g(X) = q(X)f(X) + r(X)$ gilt. Einsetzen von b ergibt $g(b) = r(b) = a_0 + a_1 b + a_2 b^2 + \cdots + a_{n-1} b^{n-1}$ Daher besitzt der A-Modul $A[b]$ das Erzeugendensystem $\{1, b, b^2, \ldots, b^{n-1}\}$. Fall $n - 1 \to n$: Es seien $b_1, \ldots, b_n \in B$ sämtlich ganz über A und $R = A[b_1, \ldots, b_{n-1}]$. Dann ist b_n ganz über R, und da der Fall $n = 1$ schon behandelt ist folgt, dass der R-Modul $R[b_n] = A[b_1, \ldots, b_n]$ endlich erzeugt über R ist. Nach Induktionshypothese ist R endlich erzeugt über A. Nach Lemma 6.3.3 ist $R[b_n]$ dann endlich erzeugt über A.

Rückrichtung:
Der A-Modul $A[b_1, \ldots, b_n]$ sei endlich erzeugt mit einem Erzeugendensystem $\mathcal{A} = \{w_1, \ldots, w_r\}$. Für $b \in A[b_1, \ldots, b_n]$ gibt es dann $c_{ij} \in A$ mit $1 \le i, j \le r$ so dass

$$b w_i \;=\; \sum_{j=1}^{r} c_{ij} w_j$$

gilt für $i = 1 \ldots r$. Es sei $C = (c_{ij}) \in A^{(r,r)}$. Dann folgt

$$(bE_n - C) \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \,.$$

Nach Lemma 6.3.2 gilt $\det(bE_n - C)w_i = 0$ für alle $1 \leq i \leq r$. Da es eine Darstellung $1 = d_1w_1 + \cdots + d_rw_r$ mit $d_i \in A$ gibt, folgt $\det(bE_n - C) = 0$. Die Entwicklung der Determinante liefert eine Gleichung $f(b) = 0$ mit normiertem $f \in A[X]$, also ist b ganz. □

Definition 6.3.3
Es sei $A \subseteq B$ eine Ringerweiterung. Die Menge $\overline{A} = \overline{A_B} = \{b \in B \mid b \text{ ganz über } A\}$ heißt der ganze Abschluss von A in B.

Satz 6.3.4
Es sei $A \subseteq B$ eine Ringerweiterung. Dann ist der ganze Abschluss $\overline{A}$ von A in B ein Teilring von B.

Beweis
Es seien $b_1, b_2 \in \overline{A}$. Nach Satz 6.3.1 ist der A-Modul $A[b_1, b_2]$ endlich erzeugt über A. Dann sind auch $A[b_1, b_2, b_1 - b_2] = A[b_1, b_2]$ und $A[b_1, b_2, b_1b_2] = A[b_1, b_2]$ endlich erzeugt über A. Also sind nach Satz 6.3.1 auch $b_1 - b_2$ und b_1b_2 ganz über A und damit Elemente von $\overline{A}$. Damit ist $\overline{A}$ ein Teilring von B. □

Satz 6.3.5
Es seien $A \subseteq B \subseteq C$ Ringerweiterungen. Ist C ganz über B und B ganz über A, so ist C ganz über A.

Beweis
Es sei $c \in C$ ganz über B. Dann gibt es $b_i \in B$ mit $c^n + b_{n-1}c^{n-1} + \cdots + b_1c + b_0 = 0$. Es sei $R = A[b_1, \ldots, b_n]$, dann ist $R[c]$ ein endlich erzeugter R-Modul. Nach Satz 6.3.1 ist R auch endlich erzeugt über A. Nach Lemma 6.3.3 ist der A-Modul $R[c]$ endlich erzeugt über A, und damit c ganz über A. □

Definition 6.3.4
Es sei $A \subseteq B$ eine Ringerweiterung. A heißt ganzabgeschlossen in B, wenn $A = \overline{A_B}$ ist. Es sei A ein Integritätsbereich mit Quotientenkörper K. Der ganze Abschluss $\overline{A}$ von A in K heißt Normalisierung von A. A heißt ganzabgeschlossen schlechthin, wenn $\overline{A} = A$ ist, d. h. wenn A ganzabgeschlossen in seinem Quotientenkörper ist.

Satz 6.3.6
Es sei $A \subseteq B$ eine Ringerweiterung:

(a) *Der ganze Abschluss $\overline{A}$ von A ist ganzabgeschlossen in B.*
(b) *Jeder faktorielle Ring ist ganzabgeschlossen.*

Beweis
Zu a): Es sei $b \in B$ ganz über $\overline{A}$. Dann ist nach Satz 6.3.3 $\overline{A}[b]$ ganz über $\overline{A}$. Nach Satz 6.3.4 ist $\overline{A}[b]$ ganz über A, also $b \in \overline{A}$. Zu b): Es sei $\frac{a}{b} \in K$ beliebig mit $a, b \in A$ und $b \neq 0$. Da A faktoriell ist kann man den Bruch kürzen, und $\mathrm{ggT}(a, b) = 1_A$ annehmen. Dann gibt es $a_i \in A$, so dass

$$(\frac{a}{b})^n + a_{n-1}(\frac{a}{b})^{n-1} + \cdots + a_1\frac{a}{b} + a_0 \;=\; 0$$

ist. Für jedes Primelement $\pi \in A$ gilt: $\pi | b \Rightarrow \pi | a$, aus der angenommenen Teilerfremdheit folgt $b \in A^*$ und damit $\frac{a}{b} \in A$. □

Im Folgenden sei A ein ganzabgeschlossener Integritätsring mit Quotientenkörper $K = \mathrm{Quot}(A)$, und L/K eine endliche separable Körpererweiterung, sowie B der ganze Abschluss von A in L.

Definition 6.3.5
Unter einer Ganzheitsbasis von B über A (oder auch A-Basis von B) versteht man ein System von Elementen $\omega_1, \ldots, \omega_n \in B$ derart, dass sich jedes $b \in B$ in eindeutiger Weise als Linearkombination $b = a_1\omega_1 + \cdots + a_n\omega_n$ mit Koeffizienten $a_i \in A$ darstellen lässt.

Bemerkung 6.3.1
Die Existenz einer Ganzheitsbasis $\{\omega_1, \ldots, \omega_n\}$ bedeutet, dass B ein freier A-Modul mit $\dim_A(B) = n$ ist.

Wir wollen im Folgenden die Existenz einer Ganzheitsbasis für den Fall sicherstellen, dass A ein Hauptidealring ist. Wichtig für das Studium der Ganzheit sind Spur, Norm und die Diskriminante. Nach dem Satz vom primitiven Element (Satz 5.1.1) können wir im Folgenden annehmen, dass $L = K(\theta)$ ist. Weiter sei Z ein Zerfällungskörper des Minimalpolynoms $m_\theta(X)$ von θ über K mit linearem Zerfall $m_\theta(X) = (X - \theta_1) \cdots (X - \theta_n)$. Nach Satz 3.2.2(b) gibt es genau einen K-Isomorphismus σ_i von L zu jeder Nullstelle θ_i, der durch die Zuordnung $\theta \mapsto \theta_i$ festgelegt ist. Mit $\sigma_1, \ldots, \sigma_n$ seien im Folgenden stets diese Isomorphismen gemeint. Wir betrachten L als Vektorraum über K. Dann ist

$$\begin{array}{rcl} S_{L/K}(\alpha) & = & S(T_\alpha) \\ N_{L/K}(\alpha) & = & \det(T_\alpha) \end{array}$$

mit der Darstellungsmatrix $T_\alpha \in K^{(n,n)}$ des K-Vektorraumhomomorphismus $\varphi_\alpha : L \to L,\ x \mapsto \alpha \cdot x$. Wie aus der Linearen Algebra bekannt, finden wir in dem charakteristischen Polynom

$$f_\alpha(X) \ = \ \det(X \cdot E_n - T_\alpha) \ = \ X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

von T_α Spur und Norm durch $S_{L/K}(\alpha) = -a_{n-1}$ und $N_{L/K}(\alpha) = (-1)^n a_0$.

Satz 6.3.7
Es gilt

$$\begin{array}{rcl} f_\alpha(X) & = & \prod(X - \sigma_i(\alpha)) \\ S_{L/K}(\alpha) & = & \sum \sigma_i(\alpha) \\ N_{L/K}(\alpha) & = & \prod \sigma_i(\alpha) \end{array}$$

wobei die Summen/Produkte über $i = 1 \ldots n$ laufen.

Beweis
Es sei $m = [K(\alpha) : K]$ und $m_\alpha(X) = X^m + c_{m-1}X^{m-1} + \cdots + c_1 X + c_0$ das Minimalpolynom von α über K. Dann ist $\{1, \alpha, \ldots, \alpha^{m-1}\}$ eine Basis der Körpererweiterung $K(\alpha)/K$. Ist $\{\beta_1, \ldots, \beta_d\}$ eine Basis der Erweiterung $L/K(\alpha)$, so ist $\{\beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{m-1}, \ldots\ldots, \beta_d, \beta_d\alpha, \ldots, \beta_d\alpha^{m-1}\}$ eine Basis von L/K. Die Darstellungsmatrix von φ_α hat bzgl. dieser Basis dann die Blockgestalt

$$T_\alpha \ = \ \underbrace{\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}}_{d-\text{mal}}$$

mit der Matrix

$$A \ = \ \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{m-1} \end{pmatrix}.$$

Man rechnet leicht nach, dass

$$f_\alpha(X) \ = \ \pm \det(A - XE_n)^d \ = \ (c_0 + c_1 X + \cdots + c_{m-1}X^{m-1} + X^m)^d \ = \ m_\alpha(X)^d$$

gilt. Insbesondere ist das charakteristische Polynom von α eine Potenz des Minimalpolynoms. Die Menge $\{\sigma_1, \ldots, \sigma_n\}$ zerfällt unter der Relation $\sigma_i \sim \sigma_j \Leftrightarrow \sigma_i(\alpha) = \sigma_j(\alpha)$ in m Äquivalenzklassen der Mächtigkeit d. Es sei $\{\sigma_{k_1}, \ldots, \sigma_{k_m}\}$ ein Repräsentantensystem. Dann gilt

$$m_\alpha(X) \;=\; \prod_{l=1}^{m}(X - \sigma_{k_l}(\alpha))$$

$$\Rightarrow\; f_\alpha(X) \;=\; \prod_{l=1}^{m}(X - \sigma_{k_l}(\alpha))^d \;=\; \prod_{l=1}^{m}\prod_{\sigma_i \sim \sigma_{k_l}}(X - \sigma_i(\alpha)) \;=\; \prod_{i=1}^{n}(X - \sigma_i(\alpha))\,.$$

Damit folgen auch die angegebenen Darstellungen von Norm und Spur. □

Wir definieren nun die Diskriminante in einer etwas allgemeineren Situation als in Definition 5.7.1. Im folgenden Satz werden wir jedoch sehen, dass die neue Definition mit Definition 5.7.1 eng zusammenhängt.

Definition 6.3.6
Es seien $\alpha_1, \ldots, \alpha_n \in L$ mit $n = [L : K]$. Unter der Diskriminante $d(\alpha_1, \ldots, \alpha_n)$ versteht man

$$d(\alpha_1, \ldots, \alpha_n) \;=\; \det(S_{L/K}(\alpha_i\alpha_j)_{\substack{1\le i\le n\\ 1\le j\le n}})\,.$$

Satz 6.3.8
Es seien $\alpha_1, \ldots, \alpha_n \in L$ beliebig und $m_\theta(X)$ das Minimalpolynom eines primitiven Elements $\theta \in L$ über K. Dann gilt:

(a) *Es ist $d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i(\alpha_j)))^2$.*
(b) *$d(1, \theta, \ldots, \theta^{n-1}) = D(m_\theta(X))$ im Sinne von Definition 5.7.1.*

Beweis
Es sei $A = (\sigma_i(\alpha_j)) \in L^{(n,n)}$. Dann ist

$$A^T \cdot A \;=\; (S_{L/K}(\alpha_i\alpha_j)_{\substack{1\le i\le n\\ 1\le j\le n}})$$

und $d(\alpha_1, \ldots, \alpha_n) = \det(A^T A) = \det(A)^2 = \det(\sigma_i(\alpha_j))^2$, woraus Behauptung a) folgt. Nun sei $m_\alpha(X) \in K[X]$ das Minimalpolynom von θ mit Zerfall $m_\alpha(X) = \prod(X - \theta_i)$ im Zerfällungskörper Z und $\theta_1 = \theta$. Dann gilt

$$D(m_\alpha(X)) \;=\; \prod_{i<j}(\theta_i - \theta_j)^2 \;=\; \det(V)^2$$

mit der Vandermonde-Matrix

$$V \;=\; \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix}\,.$$

Dies sieht man, indem man jede der $(n-1)$ ersten Spalten mit θ_1 multipliziert, von den folgenden subtrahiert, und so fortfährt. Die Behauptung b) folgt damit aus a). □

Satz 6.3.9
Es sei A ein Teilring von K, so dass $K = \mathrm{Quot}(A)$ ist mit ganzem Abschluss $\overline{A} = \overline{A_K}$ in K und dem ganzen Abschluss $B = \overline{A_L}$ im Erweiterungskörper L, dann gilt:

(a) *Ist $\alpha \in \overline{A}$, so gilt $S_{L/K}(\alpha) \in A$ und $N_{L/K}(\alpha) \in A$.*
(b) *Für jedes $\alpha \in B$ gilt die Äquivalenz $\alpha \in B^* \Leftrightarrow N_{L/K}(\alpha) \in A^*$.*

Beweis
Zu a): Ist α ganz über A, so auch $\sigma_i(\alpha)$ für $i = 1 \dots n$. Die Behauptung folgt dann aus Satz 6.3.7. Zu b): Hinrichtung: Ist $\alpha \in B$ eine Einheit des Rings B, so ist auch $\sigma_i(\alpha) \in B^*$ für alle i, nach Satz 6.3.7 also $N_{L/K} \in A^*$. Rückrichtung: Es sei $a \cdot N_{L/K}(\alpha) = 1$ für ein $a \in A$. Dann ist $1 = a \cdot \prod \sigma_i(\alpha) = \gamma\alpha$ mit $\gamma \in B$. □

Satz 6.3.10
Es sei $\{\alpha_1, \dots, \alpha_n\}$ eine in B gelegene Basis von L/K mit Diskriminante $d = d(\alpha_1, \dots, \alpha_n)$. Dann gilt:

$$d \cdot B \subseteq A\alpha_1 \oplus \cdots \oplus A\alpha_n .$$

Beweis
Es sei $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$ mit $a_i \in K$. $x_i = a_i$ sind die Lösungen des linearen Gleichungssystems

$$\sum_{j=1}^{n} S_{L/K}(\alpha_i\alpha_j)x_j = S_{L/K}(\alpha_i\alpha) \;\; 1 \le i \le n .$$

Nach der Cramerschen Regel berechnen sich die a_j als Quotienten zweier Determinanten. Die Determinante im Zähler ist wegen $S_{L/K}(\alpha_i\alpha_j) \in A$ aus A, die Nennerdeterminante ist $\det(S_{L/K}(\alpha_i\alpha_j)) = d$. Also folgt $d \cdot a_j \in A$, damit $d \cdot \alpha \in A\alpha_1 \oplus \cdots \oplus A\alpha_n$. □

Wir beweisen nun die Existenz der Ganzheitsbasis für den Fall, dass A ein Hauptidealring ist:

Satz 6.3.11
Ist A ein Hauptidealring, so ist jeder endlich erzeugte B-Untermodul $M \neq \{0\}$ von L ein freier A-Modul mit $\dim_A(M) = [L : K]$. Insbesondere besitzt B eine Ganzheitsbasis über A.

Zum Beweis benötigen wir

Lemma 6.3.12
Es ist $L = \{\frac{a}{b} \mid b \in B \,,\; a \in A - \{0\}\}$.

Beweis
Es sei

$$(1): \; a_n\beta^n + \cdots + a_1\beta + a_0 = 0 \quad a_i \in A,\; a_n \neq 0 .$$

Dann ist $b = a_n\beta$ ganz über A, weil Multiplikation von (1) mit a_n^{n-1} eine Gleichung

$$(a_n\beta)^n + \cdots + a_1'(a_n\beta) + a_0' = 0 \quad a_i' \in A$$

ergibt. □

Beweis von Satz 6.3.11
Es sei $M \neq \{0\}$ ein endlich erzeugter B-Untermodul von L und $\{\alpha_1, \dots, \alpha_n\}$ eine Basis von L/K. Nach Lemma 6.3.12 können wir durch Multiplikation mit einem Element aus A erreichen, dass sie in B liegt. Nach Satz 6.3.10 ist dann $d \cdot B \subseteq A\alpha_1 \oplus \cdots \oplus A\alpha_n$. Es sei $\{\mu_1, \dots, \mu_r\} \subseteq M$ ein Erzeugendensystem des B-Moduls M. Es gibt ein $a \in A$ mit $a\mu_i \in B$ für alle $i = 1 \dots r$, also $a \cdot M \subseteq B$. Damit ist

$$a \cdot d \cdot M \subseteq d \cdot B \subseteq A\alpha_1 \oplus \cdots \oplus A\alpha_n =: M_0 .$$

Nach Satz 6.1.6 ist mit M_0 auch $a \cdot d \cdot M$, also auch M ein freier A-Modul. Wegen $\dim_A(M) = \dim_A(dM) \le \dim_A(M_0) \le \dim_A(M)$ ist $\dim_A(M) = \dim_A(M_0) = [L : K]$. □

Der wichtigste Spezialfall unserer Betrachtungen ist der ganze Abschluss $\mathcal{O}_K \subseteq K$ von $\mathbb{Z} \subseteq \mathbb{Q}$ in einem algebraische Zahlkörper K. Nach Satz 6.3.11 besitzt jeder endlich erzeugte $\mathcal{O}_K$-Untermodul M von K eine $\mathbb{Z}$-Basis $\{\alpha_1, \dots, \alpha_n\}$, d. h. $M = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. Die Diskriminante $d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$

hängt nicht von der Wahl dieser $\mathbb{Z}$-Basis ab. Ist nämlich $\{\alpha'_1, \ldots, \alpha'_n\}$ eine andere Basis, so ist nach Satz 6.1.5

$$\begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix} \;=\; C \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

mit einem invertierbaren $C \in \mathbb{Z}^{(n,n)}$. Wegen dem Determinantenmultiplikationssatz ist dann auch $\det(C) \in \mathbb{Z}$ invertierbar, was nur für $\det(C) = \pm 1$ möglich ist. Wegen $(\sigma_i(\alpha'_j)) = C \cdot (\sigma_i(\alpha_j))$ folgt $d(\alpha_1, \ldots, \alpha_n) = d(\alpha'_1, \ldots, \alpha'_n)$. Insbesondere hat auch $d(\omega_1, \ldots, \omega_n)$ für jede $\mathbb{Z}$-Basis $\{\omega_1, \ldots, \omega_n\}$ den gleichen Wert.

Definition 6.3.7
Unter der Diskriminante des Zahlkörpers K versteht man $d_K = d(O_K) = d(\omega_1, \ldots, \omega_n)$ mit einer beliebigen $\mathbb{Z}$-Basis $\{\omega_1, \ldots, \omega_n\}$ von $\mathcal{O}_K$.

6.4. Ideale

Es sei K ein algebraischer Zahlkörper mit dem Ring $\mathcal{O}_K$ der ganzen algebraischen Zahlen in K. Wie in $\mathbb{Z}$, so lässt sich auch in $\mathcal{O}_K$ jede Nichteinheit $\alpha \neq 0$ in ein Produkt von irreduziblen Elementen zerlegen. Denn wenn α nicht selbst irreduzibel ist, so zerfällt es in ein Produkt $\alpha = \beta\gamma$ von zwei Nichteinheiten, so dass nach Satz 6.3.9(b) gilt:

$$\begin{array}{rcccl} 1 & < & |N_{K/Q}(\beta)| & < & |N_{K/\mathbb{Q}}(\alpha)| \quad , \\ 1 & < & |N_{K/Q}(\gamma)| & < & |N_{K/\mathbb{Q}}(\alpha)| \quad . \end{array}$$

Die Zerlegung in irreduzible Elemente folgt mittels vollständiger Induktion, da es nur endlich viele Normbilder in $\mathbb{Z}$ mit beschränktem Betrag gibt. Diese Zerlegung ist jedoch im Allgemeinen nicht eindeutig:

Beispiel 6.4.1
Im Körper $K = \mathbb{Q}(\sqrt{-5})$ ist (wie wir später sehen werden) der Ring der ganzen Zahlen gegeben durch $\mathcal{O}_K = \mathbb{Z} \oplus \sqrt{-5}\mathbb{Z}$. Nach Beispiel 2.4.1 besitzt 9 die verschiedenen Zerlegungen

$$9 \;=\; 3 \cdot 3 \;=\; (2 + \sqrt{-5})(2 - \sqrt{-5})$$

in unzerlegbare Elemente von $\mathcal{O}_K$.

Die Idee von Eduard Kummer war, dass es für die Zahlen in $\mathcal{O}_K$ einen erweiterten Bereich neuer idealer Zahlen geben müsse, in welchem sie sich eindeutig als Produkt idealer Primzahlen darstellen lassen würden. In der obigen Zerlegung wäre beispielsweise $3 = \mathfrak{p}_1\mathfrak{p}_2$ und $(2 + \sqrt{-5}) = \mathfrak{p}_1^2$ bzw. $(2 - \sqrt{-5}) = \mathfrak{p}_2^2$, womit die nun eindeutige Zerlegung von 9 in ideale Zahlen

$$9 \;=\; (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_1\mathfrak{p}_2) \;=\; \mathfrak{p}_1^2\mathfrak{p}_2^2$$

folgen würde. Aus den idealen Zahlen sind später die Ideale von $\mathcal{O}_K$ im Sinne von Definition 2.1.3(c) geworden. Grundlegend für das Folgende ist

Satz 6.4.1
Der Ring $\mathcal{O}_K$ ist Noethersch, ganzabgeschlossen, und jedes Primideal $\mathfrak{P} \neq \{0\}$ ist ein maximales Ideal.

Beweis
Nach Satz 6.3.11 ist jedes Ideal $\mathfrak{a}$ von $\mathcal{O}_K$ ein endlich erzeugter $\mathbb{Z}$-Modul, damit ist der Ring $\mathcal{O}_K$ nach Definition 6.2.1 Noethersch. Als ganzer Abschluss von $\mathbb{Z}$ in K ist $\mathcal{O}_K$ auch ganzabgeschlossen nach Satz 6.3.6. Es bleibt zu zeigen, dass jedes Primideal $\mathfrak{P} \neq \{0\}$ maximal ist. Offenbar ist $\mathfrak{P} \cap \mathbb{Z}$ ein von Null verschiedenes Primideal von $\mathbb{Z}$, also $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{N}$ nach Bemerkung 2.4.1. Es sei $y \in \mathfrak{P}$ mit $y \neq 0$ und

$$y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 \;=\; 0$$

mit $a_i \in \mathbb{Z}$ und $a_0 \neq 0$. Dann ist $a_0 \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Der Integritätsbereich $\overline{O} = \mathcal{O}_K/\mathfrak{P}$ entsteht aus dem Körper $\kappa = \mathbb{Z}/p\mathbb{Z}$ durch Adjunktion algebraischer Elemente und ist somit ein Körper, da $F(\alpha) = F[\alpha]$ für jeden Körper F und jedes über F algebraische α ist Nach Satz 2.1.4 ist $\mathfrak{P}$ dann ein maximales Ideal. □

Definition 6.4.1
Ein Noetherscher, ganzabgeschlossener Integritätsring, in dem jedes von $\{0\}$ verschiedene Primideal maximal ist, heißt Dedekindring.

Definition 6.4.2
Es sei R ein Ring und $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ Ideale von R. Wir sagen: $\mathfrak{a}$ teilt $\mathfrak{b}$ (geschrieben $\mathfrak{a}|\mathfrak{b}$), falls $\mathfrak{b} \subseteq \mathfrak{a}$ ist.

Satz 6.4.2
Es sei $\mathcal{O}$ ein Dedekindring. Jedes von $(0) = \{0\}$ und $(1) = \mathcal{O}$ verschiedene Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}$ besitzt eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung

$$\mathfrak{a} \;=\; \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

als Produkt von Primidealen $\mathfrak{P}_i \trianglelefteq \mathcal{O}$.

Lemma 6.4.3
Zu jedem Ideal $\mathfrak{a} \neq (0)$ von $\mathcal{O}$ gibt es von Null verschiedene Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \trianglelefteq \mathcal{O}$ mit $\mathfrak{a} \supseteq \mathfrak{P}_1 \cdots \mathfrak{P}_r$.

Beweis
Es sei $\mathcal{I}$ die Menge aller Ideale, für welche die Behauptung des Lemmas falsch ist. Wir zeigen zunächst:

$$(1): \;\; \forall \mathfrak{a} \in \mathcal{I} \exists \mathfrak{b} \in \mathcal{I}: \; \mathfrak{a} \subsetneq \mathfrak{b}\,.$$

Ein $\mathfrak{a} \in \mathcal{I}$ kann kein Primideal sein, also gibt es $b_1, b_2 \in \mathfrak{a}$ mit $b_1 b_2 \in \mathfrak{a}$ aber $b_1, b_2 \notin \mathfrak{a}$. Wir setzen $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$ und $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$, woraus $\mathfrak{a} \subsetneq \mathfrak{a}_1, \mathfrak{a}_2$ folgt. Es ist andererseits $\mathfrak{a}_1\mathfrak{a}_2 = \{(r_1 b_1 + a_1)(r_2 b_2 + a_2) \mid r_i \in \mathcal{O}\ ,\ a_i \in \mathfrak{a}\} = \{r_1 r_2 b_1 b_2 + r_1 b_2 a_2 + r_2 b_2 a_2 + a_1 a_2 \mid r_i \in \mathcal{O}\ ,\ a_i \in \mathfrak{a}\} \subseteq \mathfrak{a}$. Wären $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathcal{I}$, so enthielten beide Produkte von Primidealen, also auch $\mathfrak{a}$, woraus der Widerspruch $\mathfrak{a} \notin \mathcal{I}$ folgen würde. Damit ist $\mathfrak{a}_1 \in \mathcal{I}$ oder $\mathfrak{a}_2 \in \mathcal{I}$, und (1) ist gezeigt. Annahme: $\mathcal{I} \neq \emptyset$. Nach (1) gibt es dann eine unendliche echt aufsteigende Kette $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots$ von Idealen in $\mathcal{O}$ im Widerspruch zu Satz 6.2.1. □

Lemma 6.4.4
Es sei K der Quotientenkörper eines Dedekindrings $\mathcal{O}$. Ist $\mathfrak{P} \trianglelefteq \mathcal{O}$ ein Primideal und

$$\mathfrak{P}^{-1} \;=\; \{x \in K \mid x\mathfrak{P} \subseteq \mathcal{O}\}\,,$$

so ist

$$\mathfrak{a}\mathfrak{P}^{-1} \;=\; \{\sum a_i x_i \mid a_i \in \mathfrak{a}\ ,\ x_i \in \mathfrak{P}^{-1}\} \;\neq \mathfrak{a}\,.$$

für jedes Ideal $\mathfrak{a} \neq (0)$.

Beweis
Es sei $a \in \mathfrak{P}$ mit $a \neq 0$ und $\mathfrak{P}_1 \cdots \mathfrak{P}_r \subseteq (a) \subseteq \mathfrak{P}$ mit Primidealen $\mathfrak{P}_i \neq 0$ und minimalem r. Eines der $\mathfrak{P}_i$, ohne Einschränkung $\mathfrak{P}_1$, ist in $\mathfrak{P}$ enthalten, denn sonst gäbe es für jedes i ein $a_i \in \mathfrak{P} - \mathfrak{P}_i$ mit $a_1 \cdots a_r \in \mathfrak{P}$. Wegen der Maximalität von $\mathfrak{P}_1$ folgt $\mathfrak{P}_1 = \mathfrak{P}$. Wegen $\mathfrak{P}_2 \cdots \mathfrak{P}_r \subsetneq (a)$ gibt es ein $b \in \mathfrak{P}_2 \cdots \mathfrak{P}_r$ mit $b \notin (a)$, damit ist $a^{-1}b \notin \mathcal{O}$. Andererseits ist aber $b\mathfrak{P} = b\mathfrak{P}_1 \subseteq (a)$, also $a^{-1}b\mathfrak{P} \subseteq \mathcal{O}$ und somit $a^{-1}b \in \mathfrak{P}^{-1}$. Daraus folgt $\mathfrak{P}^{-1} \neq \mathcal{O}$. Es sei nun $\mathfrak{a} \neq (0)$ ein Ideal von $\mathcal{O}$ und $\{\alpha_1, \ldots, \alpha_n\}$ ein Erzeugendensystem. Annahme: $\mathfrak{a}\mathfrak{P}^{-1} = \mathfrak{a}$. Dann gilt für jedes $x \in \mathfrak{P}^{-1}$:

$$x\alpha_i \;=\; \sum_{j=1}^{n} a_{ij}\alpha_j \;\text{ mit } a_{ij} \in \mathcal{O}\,.$$

Es sei $A = xE_n - (a_{ij}) \in K^{(n,n)}$. Dann ist

$$A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \vec{0}$$

und damit $\det(A) = 0$. Daher ist x als Nullstelle des normierten Polynoms $f(X) = \det(XE_n - (a_{ij})) \in \mathcal{O}[X]$ ganz über $\mathcal{O}$, d. h. $x \in \mathcal{O}$. Daraus folgt aber der Widerspruch $\mathfrak{P}^{-1} = \mathcal{O}_K$. □

Beweis von Satz 6.4.2
Wir beweisen zunächst die Existenz, dann die Eindeutigkeit der Zerlegung in Primideale.

Existenz:
Es sei $\mathcal{I}$ die Menge aller Ideale, die nicht als Produkt von Primidealen darstellbar sind. Annahme: $\mathcal{I} \neq \emptyset$. Nach Satz 6.2.1 enthält $\mathcal{I}$ ein maximales Element $\mathfrak{a}$, d. h. $\mathfrak{a} \subsetneq \mathfrak{b}$ für alle $\mathfrak{b} \in \mathcal{I} - \{\mathfrak{a}\}$. Wiederum nach Satz 6.2.1 ist $\mathfrak{a} \subseteq \mathfrak{P}$ für ein maximales Ideal $\mathfrak{P}$. Wir erhalten wegen $\mathcal{O} \subseteq \mathfrak{P}^{-1}$ die Inklusionen $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{P}^{-1} \subseteq \mathfrak{P}\mathfrak{P}^{-1} \subseteq \mathfrak{a}$. Nach Lemma 6.4.4 ist $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{P}^{-1}$ und $\mathfrak{P} \subsetneq \mathfrak{P}\mathfrak{P}^{-1} \subseteq \mathcal{O}$. Da $\mathfrak{P}$ ein maximales Ideal ist folgt $\mathfrak{P}\mathfrak{P}^{-1} = \mathcal{O}$. Wegen der Maximalität von $\mathfrak{a}$ in $\mathcal{I}$ und wegen $\mathfrak{a} \neq \mathfrak{P}$, also $\mathfrak{a}\mathfrak{P}^{-1} \neq \mathcal{O}$, besitzt $\mathfrak{a}\mathfrak{P}^{-1}$ eine Primzerlegung $\mathfrak{a}\mathfrak{P}^{-1} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$, damit aber auch $\mathfrak{a} = \mathfrak{a}\mathfrak{P}\mathfrak{P}^{-1} = \mathfrak{P}_1 \cdots \mathfrak{P}_r\mathfrak{P}$, Widerspruch.

Eindeutigkeit:
Für ein Primideal gilt: $\mathfrak{P}|\mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{P}|\mathfrak{a}$ oder $\mathfrak{P}|\mathfrak{b}$. Es seien nun

$$\mathfrak{a} = \mathfrak{P}_1 \cdots \mathfrak{P}_r = \mathfrak{Q}_1 \cdots \mathfrak{Q}_s$$

zwei Zerlegungen von $\mathfrak{a}$ in Primideale. Dann teilt $\mathfrak{P}_1$ einen Faktor $\mathfrak{Q}_j$, ohne Einschränkung $\mathfrak{Q}_1$. Da Primideale in Dedekindringen maximale Ideale sind, folgt $\mathfrak{P}_1 = \mathfrak{Q}_1$. Wir multiplizieren auf beiden Seiten mit $\mathfrak{P}_1^{-1}$ und erhalten wegen $\mathfrak{P}_1\mathfrak{P}_1^{-1} = \mathcal{O}$ die mit $\mathfrak{P}_1$ gekürzte Darstellung

$$\mathfrak{P}_2 \cdots \mathfrak{P}_r = \mathfrak{Q}_2 \cdots \mathfrak{Q}_s \,.$$

So fortfahrend erhalten wir $r = s$ und nach Umordnung $\mathfrak{P}_i = \mathfrak{Q}_i$ für $i = 1 \ldots r$. □

Definition 6.4.3
Fasst man in der Primzerlegung eines Ideals $\mathfrak{a} \neq 0$ in einem Dedekindring $\mathcal{O}$ die gleichen Primideale zusammen, so erhält man eine Produktdarstellung

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}^{e_r} \;\; e_i \in \mathbb{N} \,.$$

Jede solche Gleichung ist so zu verstehen, dass die $\mathfrak{P}_i$ paarweise verschieden sind. Ist $\mathfrak{a} = (a)$ ein Hauptideal, so schreibt man auch

$$a = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \,.$$

Definition 6.4.4
Es sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K. Ein gebrochenes Ideal von K ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq \{0\}$ von K. Die gewöhnlichen Ideale $\mathfrak{a} \trianglelefteq \mathcal{O}$ bezeichnet man in diesem Zusammenhang auch als ganze Ideale.

Das Produkt zweier gebrochener Ideale definieren wir analog zum Produkt ganzer Ideale:

Definition 6.4.5
Unter dem Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ verstehen wir den $\mathcal{O}$-Modul

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum a_i b_i \mid a_i \in \mathfrak{a} \,,\; b_i \in \mathfrak{b} \right\}$$

von K.

Satz 6.4.5
Gebrochene Ideale erfüllen die folgenden Eigenschaften:

(a) *Eine Teilmenge* $\mathfrak{a} \subseteq K$ *ist ein gebrochenes Ideal genau dann, wenn es ein* $c \in \mathcal{O} - \{0\}$ *gibt, so dass* $c \cdot \mathfrak{a}$ *ein ganze Ideal von* $\mathcal{O}$ *ist.*
(b) *Die Menge der gebrochenen Ideale von* K *bildet bzgl. der Multiplikation eine abelsche Gruppe, die Idealgruppe* $\mathcal{J}_K$ *von* K*.*
(c) *Das Einselement ist* $(1) = \mathcal{O}$*, das Inverse zu* $\mathfrak{a}$ *ist* $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$*.*

Beweis
Zu a): Es sei $\mathfrak{a}$ ein gebrochenes Ideal und $\{b_1, \ldots, b_n\}$ ein Erzeugendensystem von $\mathfrak{a}$ als $\mathcal{O}$-Modul. Dann gibt es $c \in \mathcal{O}$, so dass $cb_i \in \mathcal{O}$ ist für $i = 1 \ldots n$. Damit ist offenbar $c\mathfrak{a}$ ein ganzes Ideal von $\mathcal{O}$. Die Rückrichtung der Aussage ist klar. Zu b) und c): Assoziativität und Kommutativität sowie $\mathfrak{a}(1) = (1)\mathfrak{a} = \mathfrak{a}$ sind klar. Für ein Primideal $\mathfrak{P}$ gilt $\mathfrak{P} \subsetneq \mathfrak{P}\mathfrak{P}^{-1}$ nach Lemma 6.4.4, also $\mathfrak{P}\mathfrak{P}^{-1} = \mathcal{O} = (1)$ wegen der Maximalität von Primidealen im Dedekindring $\mathcal{O}$. Ist $\mathfrak{a} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ ein ganzes Ideal, so ist hiernach $\mathfrak{b} = \mathfrak{P}_1^{-1} \cdots \mathfrak{P}_r^{-1}$ das Inverse: wegen $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ ist $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Es sei nun umgekehrt $x \in \mathfrak{a}^{-1}$, also $x\mathfrak{a} \subseteq \mathcal{O}$. Dann ist $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, also $x \in \mathfrak{b}$ wegen $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Daher ist $\mathfrak{b} = \mathfrak{a}^{-1}$. Ist $\mathfrak{a}$ ein gebrochenes Ideal und $c \in \mathcal{O}$ mit $c \neq 0$ und $c\mathfrak{a} \subseteq \mathcal{O}$, so ist $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ das Inverse von $c\mathfrak{a}$. □

Satz 6.4.6
Jedes gebrochene Ideal $\mathfrak{a}$ *besitzt eine eindeutige Produktdarstellung*

$$\mathfrak{a} = \prod_{\substack{\mathfrak{P} \text{ ganzes} \\ \text{Primideal}}} \mathfrak{P}^{e_\mathfrak{P}}$$

mit Exponenten $e_\mathfrak{P} \in \mathbb{Z}$ *und* $e_\mathfrak{P} = 0$ *für fast alle* $\mathfrak{P}$*.*

Beweis
Nach Satz 6.4.5(a) gibt es ganze Ideale $\mathfrak{b}$ und $\mathfrak{c}$, so dass $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ ist. Daraus folgt die Existenz der Produktdarstellung mit Koeffizienten in $\mathbb{Z}$. Es seien

$$\mathfrak{a} = \prod_\mathfrak{P} \mathfrak{P}^{d_\mathfrak{P}} \cdot \prod_\mathfrak{P} \mathfrak{P}^{-e_\mathfrak{P}} = \prod_\mathfrak{Q} \mathfrak{Q}^{f_\mathfrak{Q}} \cdot \prod_\mathfrak{Q} \mathfrak{Q}^{-g_\mathfrak{Q}}$$

zwei Produktdarstellungen von $\mathfrak{a}$ mit positiven $d_\mathfrak{P}, e_\mathfrak{P}, f_\mathfrak{P}, g_\mathfrak{P} \in \mathbb{N}$. Es folgt

$$\prod_\mathfrak{P} \mathfrak{P}^{d_\mathfrak{P}} \cdot \prod_\mathfrak{Q} \mathfrak{Q}^{g_\mathfrak{Q}} = \prod_\mathfrak{Q} \mathfrak{Q}^{f_\mathfrak{Q}} \cdot \prod_\mathfrak{P} \mathfrak{P}^{e_\mathfrak{P}} ,$$

und mit Satz 6.4.2 folgt die Behauptung. □

Definition 6.4.6
Die gebrochenen Hauptideale $(a) = a\mathcal{O}$ mit $a \in K^*$ bilden eine Untergruppe der Idealgruppe $\mathcal{J}_K$. Sie wird mit $\mathcal{P}_K$ bezeichnet. Die Faktorgruppe $\mathrm{Cl}_K = \mathcal{J}_K/\mathcal{P}_K$ heißt die Idealklassengruppe von K, oder auch kurz Klassengruppe.

Bemerkung 6.4.1
Offenbar ist Cl_K trivial genau dann, wenn $\mathcal{O}$ ein Hauptidealring ist.

6.5. Gitter

In der Theorie der algebraischen Zahlkörper spielen geometrische Überlegungen eine zentrale Rolle. Dies wird schon am Beispiel des einfachsten Zahlkörpers $\mathbb{Q}(i)$ deutlich. $\mathbb{Q}(i)$ kann in natürlicher Weise als Teil der komplexen Ebene $\mathbb{C}$ angesehen werden. Die Menge $\mathbb{Z}[i]$ der ganzen Zahlen von $\mathbb{Q}(i)$ besteht aus den Gitterpunkten von $\mathbb{C}$, d. h. den Punkten $a + bi$ mit ganzzahligen Koordinaten $a, b \in \mathbb{Z}$. Diese Betrachtungsweise ist von Minkowski auf beliebige Zahlkörper ausgedehnt worden.

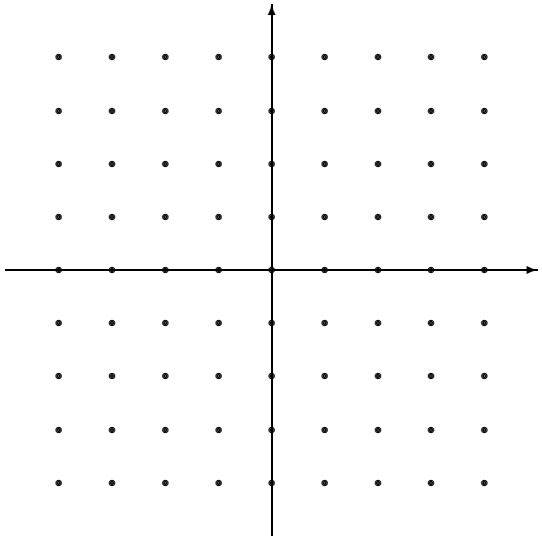
Definition 6.5.1
Es sei V ein n-dimensionaler Vektorraum über $\mathbb{R}$. Ein Gitter in V ist eine Untergruppe der Form

$$\Gamma \;=\; \mathbb{Z}\vec{v}_1 \;\oplus\; \cdots \;\oplus\; \mathbb{Z}\vec{v}_m$$

mit linear unabhängigen Vektoren $\vec{v}_1, \ldots, \vec{v}_m \in V$. Das m-Tupel $(\vec{v}_1, \ldots, \vec{v}_m)$ heißt eine Basis, und die Menge

$$\Phi \;=\; \{x_1\vec{v}_1 + \cdots + x_m\vec{v}_m \mid x_i \in \mathbb{R}\ ,\ 0 \le x_i < 1\}$$

eine Grundmasche des Gitters Γ. Das Gitter heißt vollständig oder eine $\mathbb{Z}$-Struktur von V, falls $m = n = \dim(V)$ ist.



Das Gitter $\mathbb{Z}\binom{1}{0} \oplus \mathbb{Z}\binom{0}{1}$ im $\mathbb{R}^2$.

Die Vollständigkeit des Gitters ist offenbar gleichbedeutend damit, dass die sämtlichen Verschiebungen $\Phi + \gamma$ der Grundmasche für $\gamma \in \Gamma$ den ganzen Raum V überdecken. Wir benötigen eine Charakterisierung des Gitters, die von der Wahl der Basisvektoren $\vec{v}_1, \ldots, \vec{v}_m$ unabhängig ist:

Definition 6.5.2
Es sei V ein n-dimensionaler Vektorraum über $\mathbb{R}$ mit Basis $\{\vec{v}_1, \ldots, \vec{v}_n\}$. Eine Untergruppe Γ von V heißt diskret, falls jedes Punkt $\gamma \in \Gamma$ ein isolierter Punkt ist, d. h. ist $\gamma = a_1\vec{v}_1 + \cdots + a_n\vec{v}_n \in \Gamma$ mit $a_i \in \mathbb{R}$, so gibt es ein $\varepsilon > 0$ so dass gilt:

$$\gamma' = a_1'\vec{v}_1 + \cdots + a_n'\vec{v}_n \in \Gamma \text{ und } \forall i:\ |a_i - a_i'| < \varepsilon \;\Rightarrow\; \gamma = \gamma'\ .$$

Lemma 6.5.1
Es sei $\Gamma \subseteq V$ eine Untergruppe:

(a) *Die Diskretheit nach Definition 6.5.2 ist wohldefiniert, d. h. sie hängt nicht von der Wahl der Basis ab.*
(b) *Γ ist diskret genau dann, wenn $0 \in \Gamma$ ein isolierter Punkt ist.*

Beweis
Es ist klar, dass es zu zeigen genügt, dass die Isoliertheit von 0 nicht von der Wahl der Basis abhängt. Es seien $B = \{\vec{v}_1, \ldots, \vec{v}_n\}$ sowie $B' = \{\vec{v}_1', \ldots, \vec{v}_n'\}$ Basen von V. Es genügt dann, die Äquivalenz der folgenden Bedingungen zu zeigen:

$$(1):\quad \exists\varepsilon > 0 \quad \text{mit}: \qquad a_1\vec{v}_1 + \cdots + a_n\vec{v}_n \in \Gamma \quad \text{und} \quad \forall i:\ |a_i| < \varepsilon \quad \Rightarrow \quad \forall i:\ a_i = 0$$

$$(2):\quad \exists\varepsilon > 0 \quad \text{mit}: \qquad a_1'\vec{v}_1' + \cdots + a_n'\vec{v}_n' \in \Gamma \quad \text{und} \quad \forall i:\ |a_i'| < \varepsilon \quad \Rightarrow \quad \forall i:\ a_i' = 0 \quad .$$

Es gibt eine Matrix $A = (a_{ij}) \in \mathrm{GL}(n, \mathbb{R})$ die den Basiswechsel von B zu B' vermittelt, dann ist $\sum a_i \vec{v}_i = \sum a'_i \vec{v}'_i$, wobei die Koeffizienten mittels

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \;=\; A \cdot \begin{pmatrix} a'_1 \\ \vdots \\ a'_n \end{pmatrix}$$

verbunden sind. Die Zeilensummennorm von A ist gegeben durch

$$\|A\| \;=\; \max_{1 \le i \le n} \left(\sum_{j=1}^{n} |a_{ij}| \right) .$$

Damit folgt

$$\max_{1 \le i \le n} |a_i| \;\le\; \|A\| \cdot \max_{1 \le i \le n} |a'_i| \;\;,\;\; \max_{1 \le i \le n} |a'_i| \;\le\; \|A^{-1}\| \cdot \max_{1 \le i \le n} |a_i|$$

und damit die Äquivalenz von (1) und (2). □

Satz 6.5.2
Eine Untergruppe $\Gamma \subseteq V$ ist genau dann ein Gitter, wenn sie diskret ist.

Beweis
Es sei Γ eine diskrete Untergruppe von V und $V_0 = \langle \Gamma \rangle$ der von Γ aufgespannte Untervektorraum mit $\dim(V_0) = m \le n = \dim(V)$. Es sei $U = \{\vec{u}_1, \ldots, \vec{u}_m\}$ eine in Γ gelegene Basis von V_0. Dann ist $\Gamma_0 = \mathbb{Z}\vec{u}_1 \oplus \cdots \oplus \mathbb{Z}\vec{u}_m$ ein vollständiges Gitter von V_0. Wir zeigen zunächst, dass der Index $(\Gamma : \Gamma_0)$ endlich ist. $\gamma_i \in \Gamma$ durchlaufe ein Repräsentantensystem für die Nebenklassen von Γ/Γ_0. Da Γ_0 vollständig in V_0 ist, überdecken die Verschiebungen $\Phi_0 + \gamma$ mit $\gamma \in \Gamma_0$ und der Grundmasche Φ_0 von Γ_0 den Vektorraum V_0. Daher können wir

$$\gamma_i \;=\; \mu_i + \gamma_{i,0} \text{ mit } \mu_i \in \Phi_0, \gamma_{i,0} \in \Gamma_0 \subseteq V_0$$

schreiben. Da die $\mu_i = \gamma_i - \gamma_{i,0} \in \Gamma$ in der beschränkten Menge Φ_0 liegen und isolierte Punkte sind, muss ihre Anzahl endlich sein. Es sei also $q = (\Gamma : \Gamma_0) < \infty$. Dann ist $q\Gamma \subseteq \Gamma_0$, also $\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}(\frac{1}{q}\vec{u}_1) \oplus \cdots \oplus \mathbb{Z}(\frac{1}{q})\vec{u}_m$. Nach Satz 6.1.6 besitzt Γ eine $\mathbb{Z}$-Basis $\vec{v}_1, \ldots, \vec{v}_r \in V$ mit $r \le n$ und $\Gamma = \mathbb{Z}\vec{v}_1 \oplus \cdots \oplus \mathbb{Z}\vec{v}_r$, d. h. Γ ist ein Gitter in V. □

Lemma 6.5.3
Es sei V ein endlichdimensionaler R-Vektorraum. Ein Gitter Γ in V ist genau dann vollständig, wenn es eine beschränkte Teilmenge $M \subseteq V$ gibt, deren sämtliche Verschiebungen $M + \gamma$ mit $\gamma \in \Gamma$ den ganzen Raum V überdecken.

Beweis
Ist $\Gamma = \mathbb{Z}\vec{v}_1 \oplus \cdots \oplus \mathbb{Z}\vec{v}_n$ vollständig, so kann man $M = \Phi$ für die Grundmasche $\Phi = \{x_1\vec{v}_1 + \cdots + x_n\vec{v}_n \mid x_i \in [0, 1)\}$ wählen. Es sei andererseits M eine beschränkte Teilmenge von V, deren Verschiebungen um $\gamma \in \Gamma$ den ganzen Raum V überdecken. Es sei V_0 der von Γ aufgespannte Unterraum von V. Wir zeigen, dass $V = V_0$ ist. Es sei dazu $\vec{v} \in V$ beliebig. Wegen

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

können wir für jedes $d \in \mathbb{N}$ schreiben: $d\vec{v} = a_d + \gamma_d$ mit $a_d \in M$ und $\gamma_d \in \Gamma \subseteq V_0$. Da M beschränkt ist gilt

$$\lim_{d \to \infty} \frac{1}{d} a_d \;=\; \vec{0}\,.$$

Wegen der Abgeschlossenheit von V_0 in V folgt

$$\vec{v} \;=\; \lim_{d \to \infty} \frac{1}{d} a_d \;+\; \lim_{d \to \infty} \frac{1}{d} \gamma_d \;=\; \lim_{d \to \infty} \frac{1}{d} \gamma_d \;\in\; V_0\,.$$

□

Es sei nun V ein Euklidischer Vektorraum der Dimension n, d. h. ein Raum mit einem inneren Produkt. Wir erinnern an den Begriff des inneren Produkts aus der Linearen Algebra:

DEFINITION 6.5.3
Es sei V ein Vektorraum über $\mathbb{R}$. Eine Abbildung $\langle\cdot|\cdot\rangle : V \times V \to \mathbb{R}$ heißt inneres Produkt, wenn sie folgende Eigenschaften erfüllt:

(i) $\langle\vec{x}|\vec{y}\rangle = \langle\vec{y}|\vec{x}\rangle$ für alle $\vec{x}, \vec{y} \in V$ (Symmetrie),
(ii) $\langle\lambda_1\vec{x}_1 + \lambda_2\vec{x}_2|\vec{y}\rangle = \lambda_1\langle\vec{x}_1|\vec{y}\rangle + \lambda_2\langle\vec{x}_2|\vec{y}\rangle$ für $\lambda_i \in \mathbb{R}$ (Linearität),
(iii) $\langle\vec{x}|\vec{x}\rangle \geq 0$ für alle $\vec{x} \in V$, und $\langle\vec{x}|\vec{x}\rangle = 0$ genau dann, wenn $\vec{x} = \vec{0}$ ist (Positiv-Definitheit).

Eine Menge $B = \{\vec{e}_1, \ldots, \vec{e}_n\}$ mit $n = \dim(V)$ von Vektoren heißt Orthonormalbasis (ONB), wenn gilt:

$$\langle\vec{e}_i|\vec{e}_j\rangle \;=\; \begin{cases} 1 & \text{falls} \quad i = j \\ 0 & \text{sonst} \end{cases} .$$

Für Vektorräume über $\mathbb{C}$ tritt an die Stelle des Euklidischen Vektorraums der Begriff des unitären Vektorraums. Das innere Produkt erfüllt wiederum die Eigenschaften (ii) und (iii) von Definition 6.5.3, während (i) zu ersetzen ist durch

$$(i') : \;\; \langle\vec{x}|\vec{y}\rangle \;=\; \overline{\langle\vec{y}|\vec{x}\rangle} \, .$$

Auf jedem Euklidischen Vektorraum V lässt sich das Volumen einführen. Wir verzichten auf die Definition und erwähnen nur die folgenden Eigenschaften: Der zu einer Orthonormalbasis $\{\vec{e}_1, \ldots, \vec{e}_n\}$ gehörende Würfel

$$W \;=\; \Big\{ \sum a_j\vec{e}_j \mid a_j \in [0,1] \Big\}$$

erhält das Volumen 1, und das zu den Vektoren

$$\vec{v}_i \;=\; \sum_{j=1}^{n} a_{ij} e_j$$

gehörende Parallelepiped

$$\Phi \;=\; \Big\{ \sum a_j\vec{v}_j \mid a_j \in [0,1] \Big\}$$

erhält das Volumen $|\det(A)|$ mit der Matrix $A = (a_{ij})$. Wegen

$$\left(\langle\vec{v}_i|\vec{v}_k\rangle\right)_{\substack{1\leq i\leq n \\ 1\leq k\leq n}} \;=\; \left(\sum_{j,l} a_{ij}a_{kl} \langle\vec{e}_j|\vec{e}_l\rangle \right)_{ik} \;=\; \left(\sum_{j,l} a_{ij}a_{kl} \right)_{ik} \;=\; AA^T$$

gilt auch

$$\mathrm{vol}(\Phi) \;=\; \sqrt{|\det((\langle\vec{v}_j|\vec{v}_k\rangle))|} \, ,$$

woraus die Unabhängigkeit von der Wahl der ONB ersichtlich wird. Die Abbildung $\mathrm{vol}(\cdot)$, die bestimmten Teilmengen von V ein Volumen $\mathrm{vol}(M) \geq 0$ zuordnet, ist daher für den Euklidischen Vektorraum V schlechthin definiert. Dieses Volumen besitzt zwei wichtige Eigenschaften:

Endliche Additivität:
Seien $M_1, \ldots, M_k$ disjunkte Teilmengen von V, so ist $\mathrm{vol}(\bigcup M_j) = \sum \mathrm{vol}(M_j)$.

Translationsinvarianz:
Für $\vec{v} \in V$ ist $\mathrm{vol}(\vec{v} + M) = \mathrm{vol}(M)$.

DEFINITION 6.5.4
Es sei V ein Euklidischer Vektorraum mit $\dim(V) = n$ und Γ ein vollständiges Gitter in V mit Grundmasche Φ. Das Volumen des Gitters Γ ist $\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)$.

Bemerkung 6.5.1
Das Volumen vol(Γ) ist unabhängig von der Wahl der Grundmasche, da der Übergang von einer Gitterbasis zu einer anderen durch eine Matrix mit Determinante ± 1 vermittelt wird.

Definition 6.5.5
Es sei V ein Vektorraum über $\mathbb{R}$. Eine Teilmenge $X \subseteq V$ heißt zentralsymmetrisch, wenn gilt: $\vec{x} \in X \Leftrightarrow -\vec{x} \in X$. $X \subseteq V$ heißt konvex, falls mit $x, y \in X$ auch jede Konvexkombination $ty + (1-t)x$ für $t \in [0,1]$ in X liegt. Das ist gleichbedeutend damit, dass zu zwei Punkten auch die Verbindungsstrecke der Punkte in der Menge enthalten ist.

Wir kommen nun zum zentralen Satz über Gitter:

Satz 6.5.4 (Gitterpunktsatz von Minkowski)
Es sei $\Gamma \subseteq V$ ein vollständiges Gitter in einem Euklidischen Vektorraum der Dimension n und X eine zentralsymmetrische und konvexe Teilmenge von V. Gilt

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

so enthält X mindestens einen von Null verschiedenen Gitterpunkt $\gamma \in \Gamma$.

Beweis
Wir betrachten die Mengen $M_\gamma = \frac{1}{2}X + \gamma$ für $\gamma \in \Gamma$. Annahme: die Mengen M_γ sind paarweise disjunkt. Es sei Φ die Grundmasche von Γ. Dann sind auch die Durchschnitte $\Phi \cap M_\gamma$ paarweise disjunkt, und wegen der endlichen Additivität folgt

$$\mathrm{vol}(\Phi) \; = \; \sum_{\gamma \in \Gamma} \mathrm{vol}(\Phi \cap M_\gamma) \, .$$

Aus $\Phi \cap M_\gamma$ entsteht durch Translation mit $-\gamma$ die Menge $(\Phi - \gamma) \cap \frac{1}{2}X$. Die Mengen $\Phi - \gamma$ überdecken V und damit auch $\frac{1}{2}X$. Daher gilt

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

ein Widerspruch. Die Annahme ist also falsch, es gibt $\gamma_1, \gamma_2 \in \Gamma$ mit $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$. Es sei $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x + \gamma_2$ für $x_1, x_2 \in X$. Dann ist $\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$ der Mittelpunkte der Strecke von x_2 nach $-x_1$ ein Element der konvexen Menge X. Es folgt $\gamma \in X \cap \Gamma$. □

6.6. Minkowski-Theorie

Wir wollen nun die im vorigen Abschnitt entwickelte Theorie der Gitter auf die Theorie der algebraischen Zahlkörper anwenden. Dazu sollen zunächst die Punkte eines algebraischen Zahlkörpers K mit $[K : \mathbb{Q}] = n$ mit Punkten des $\mathbb{R}^n$ identifiziert werden. Dazu verwenden wir eine Konstruktion, die derjenigen ähnelt, die in Abschnitt 6.3 zu Definition der Diskriminanten entwickelt wurde. Dort wurde eine Körpererweiterung $K(\theta)/K$ betrachtet und n Isomorphismen σ_i durch Fortsetzung der Zuordnungen $\theta \mapsto \theta_i$ bestimmt, wobei die θ_i die Nullstelle des Minimalpolynoms von θ über K in einem Zerfällungskörper von K sind. In der jetzigen Situation sei $K = \mathbb{Q}(\theta)$ ein beliebiger Zahlkörper. Anstelle des Zerfällungskörpers des Minimalpolynoms von θ kann jetzt der Körper $\mathbb{C}$ der komplexen Zahlen genommen werden. Es sei

$$m_\theta(X) \; = \; (X - \theta_1) \cdots (X - \theta_n)$$

der lineare Zerfall des Minimalpolynoms in $\mathbb{C}[X]$ mit Konjugierten $\theta_i \in \mathbb{C}$.

Definition 6.6.1
Unter einer Einbettung τ von K in $\mathbb{C}$ versteht man einen Ringmonomorphismus $\tau : \, K \to \mathbb{C}$.

Satz 6.6.1
Es sei $K = \mathbb{Q}(\theta)$ mit $[K : \mathbb{Q}] = n$. Dann gibt es genau n Einbettungen τ_i von $\mathbb{Q}(\theta)$ in $\mathbb{C}$. Sie sind bestimmt durch $\tau_i : \theta \mapsto \theta_i$, wobei die θ_i die Konjugierten von θ sind.

Beweis
Das folgt aus Satz 3.3.1. □

Definition 6.6.2
Die Einbettung τ_i heißt reell, falls $\theta_i \in \mathbb{R}$ ist. Zwei nicht reelle Einbettungen $\tau, \bar{\tau}$ mit $\tau(\theta) = \theta_i$ und $\bar{\tau}(\theta) = \bar{\theta}_i$ heißen ein Paar konjugiert komplexer Einbettungen.

Die Anzahl der reellen Einbettungen bezeichnen wir mit r, die Anzahl der Paare komplex konjugierter Einbettungen mit s.

Beispiel 6.6.1
Es sei $K = \mathbb{Q}(\theta)$ mit $\theta = \sqrt[4]{2}$. Es ist

$$m_\theta(X) \;=\; X^4 - 2 \;=\; (X - \sqrt[4]{2})(X - (-\sqrt[4]{2}))(X - \sqrt[4]{2}i)(X - (-\sqrt[4]{2}i))\,.$$

Dann sind zwei reelle Einbettungen gegeben durch

$$\begin{aligned} \tau_1 :\; \sqrt[4]{2} &\mapsto \quad \sqrt[4]{2} \\ \tau_2 :\; \sqrt[4]{2} &\mapsto -\sqrt[4]{2} \end{aligned}$$

und das einzige Paar komplex konjugierter Einbettungen durch

$$\begin{aligned} \tau_3 :\; \sqrt[4]{2} &\mapsto \quad \sqrt[4]{2}i \\ \tau_4 :\; \sqrt[4]{2} &\mapsto -\sqrt[4]{2}i \end{aligned}$$

mit $\tau_4 = \bar{\tau}_3$.

Um die im vorigen Abschnitt entwickelte Theorie der Gitter ins Spiel bringen zu können, benutzen wir nun diese Einbettungen um die Elemente von K mit Punkten des $\mathbb{R}^n$ zu identifizieren. Wir definieren zunächst einen Vektorraum über $\mathbb{C}$:

Definition 6.6.3
Unter $K_\mathbb{C}$ verstehen wir

$$K_\mathbb{C} \;=\; \prod_\tau \mathbb{C}\,,$$

wobei τ über die Einbettungen von K in $\mathbb{C}$ läuft (die Reihenfolge ist zunächst beliebig). Das innere Produkt $\langle\cdot|\cdot\rangle$ auf $K_\mathbb{C}$ ist definiert durch

$$\langle (x_\tau) | (y_\tau) \rangle \;=\; \sum_\tau x_\tau \overline{y_\tau}\,.$$

Mittels der Abbildung $j :\; K \to K_\mathbb{C},\; a \mapsto (\tau(a))_\tau$ werden Elemente von K auf Punkte aus $K_\mathbb{C} = \mathbb{C}^n$ abgebildet.

Beispiel 6.6.2
Es sei $K = \mathbb{Q}(\sqrt[4]{2})$ und $a = a_0 + a_1\sqrt[4]{2} + a_2(\sqrt[4]{2})^2 + a_3(\sqrt[4]{2})^3$ mit $a_i \in \mathbb{Q}$ beliebig in K mit den Bezeichnungen aus Beispiel 6.6.1. Dann ist

$$\begin{aligned} j(a) \;=\; (\tau_1(a), \tau_2(a), \tau_3(a), \overline{\tau_3(a)}) \;= (&a_0 + a_1\sqrt[4]{2} + a_2(\sqrt[4]{2})^2 + a_3(\sqrt[4]{2})^3\,, \\ &a_0 - a_1\sqrt[4]{2} + a_2(\sqrt[4]{2})^2 - a_3(\sqrt[4]{2})^3\,, \\ &a_0 + a_1\sqrt[4]{2}\cdot i - a_2(\sqrt[4]{2})^2 - a_3(\sqrt[4]{2})^3\cdot i\,, \\ &a_0 - a_1\sqrt[4]{2}\cdot i - a_2(\sqrt[4]{2})^2 + a_3(\sqrt[4]{2})^3\cdot i\,). \end{aligned}$$

Das Bild $j(K)$ der Abbildung j trifft einen reellen Untervektorraum von $K_\mathbb{C}$, den so genannten Minkowski-Raum, den wir im Folgenden betrachten.

Definition 6.6.4
Es sei $F:\ K_{\mathbb{C}} \to K_{\mathbb{C}},\ (a_\tau) \mapsto (\overline{a_\tau})$ die komponentenweise Konjugation auf $\mathbb{K}_{\mathbb{C}}$ und

$$K_{\mathbb{R}} \ = \ \{(a_\tau)_\tau \mid F((a_\tau)) = (a_\tau)\}$$

der $\mathbb{R}$-Untervektorraum von $K_{\mathbb{C}}$, der unter F invariant bleibt. $K_{\mathbb{R}}$ heißt Minkowski-Raum.

Satz 6.6.2
Die Einschränkung des inneren Produkts $\langle\cdot|\cdot\rangle$ von $K_{\mathbb{C}} \times K_{\mathbb{C}}$ auf $K_{\mathbb{R}} \times K_{\mathbb{R}}$ ist ein inneres Produkt auf $K_{\mathbb{R}}$, das $K_{\mathbb{R}}$ zu einem Euklidischen Vektorraum macht.

Beweis
Durch Nachrechnen. □

Explizit lässt sich der Minkowski-Raum $K_{\mathbb{R}}$ wie folgt beschreiben: Es seien $\varrho_1, \ldots, \varrho_r$ die reellen Einbettungen von K, und $\eta_1, \bar{\eta}_1, \ldots, \eta_s, \bar{\eta}_s$ die Paare komplexer Einbettungen. Dann ist

$$K_{\mathbb{R}} \ = \ \left\{ (z_\tau) \in \prod_\tau \mathbb{C} \mid z_\varrho \in \mathbb{R}\ ,\ z_{\bar{\eta}} = \overline{z_\eta} \right\} .$$

Satz 6.6.3
Die Abbildung

$$f:\ K_{\mathbb{R}} \to \prod_\tau \mathbb{R} \ = \ \mathbb{R}^{r+2s}$$

definiert über $(z_\tau) \mapsto (x_\tau)$ mit

$$x_\varrho \ = \ z_\varrho \quad , \quad x_\eta \ = \ \mathrm{Re}(z_\eta) \quad , \quad x_{\bar{\eta}} \ = \ \mathrm{Im}(z_\eta)$$

ist ein Isomorphismus von $\mathbb{R}$-Vektorräumen. Dieser überführt das innere Produkt $\langle\cdot|\cdot\rangle$ auf $K_{\mathbb{R}}$ in das innere Produkt $(\vec{x}|\vec{y}) = \sum \alpha_\tau x_\tau y_\tau$ auf $\mathbb{R}^{r+2s}$, wobei $\alpha_\tau = 1$ für reelle τ ist und $\alpha_\tau = 2$ für komplexe τ, d. h. es gilt $\langle (w_\tau)|(z_\tau)\rangle \ = \ (\vec{x}|\vec{y})$ falls $f((w_\tau)) = \vec{x}$ und $f((z_\tau)) = \vec{y}$ ist.

Beweis
Durch Nachrechnen. □

Satz 6.6.4
Ist $\mathfrak{a} \neq (0)$ ein ganzes Ideal von $\mathcal{O}_K$, so ist $\Gamma = j(\mathfrak{a})$ ein vollständiges Gitter im Minkowski-Raum $K_{\mathbb{R}}$ mit dem Grundmaschenvolumen

$$\mathrm{vol}(\Gamma) \ = \ \sqrt{|d_K|} \cdot (\mathcal{O}_K : \mathfrak{a})\, .$$

Beweis
(ohne Beweis) □

Die folgende Tatsache wird auch als Grundlemma für globale Körper bezeichnet:

Satz 6.6.5
Es sei $\mathfrak{a} \neq (0)$ ein ganzes Ideal von K, und es seien $c_\tau > 0$ durch die Einbettungen τ parametrisierte reelle Zahlen mit $c_\tau = c_{\bar{\tau}}$ für die komplexen Einbettungen und

$$\prod_\tau c_j \ > \ A \cdot (\mathcal{O}_K : \mathfrak{a}) \quad , \quad A \ = \ \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|}\, .$$

Dann gibt es ein $a \in \mathfrak{a}$ mit $a \neq 0$ und $|\tau(a)| < c_\tau$ für alle τ.

BEWEIS
Die Menge $X = \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Ihr Volumen $\mathrm{vol}(X)$ ergibt sich über die Abbildung $f: K_\mathbb{R} \to \prod_\tau \mathbb{R}$ als das 2^s-fache des Lebesgue-Inhalts des Quaders

$$f(X) = \left\{(x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\varrho| < c_\varrho \,,\; x_\eta^2 + x_{\bar\eta}^2 < c_\eta^2\right\} .$$

Es ist also

$$\mathrm{vol}(X) = 2^s \cdot \mathrm{vol}_{\mathbb{R}^n}(f(X)) = 2^s \cdot \prod_{\substack{\varrho \\ \text{reell}}} 2c_\varrho \cdot \prod_{\substack{\eta \\ \text{komplex}}} (\pi c_\eta^2) = 2^{r+s} \cdot \pi^s \cdot \prod_\tau c_\tau .$$

Anwendung von Satz 6.6.5 ergibt

$$\mathrm{vol}(X) = 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) = 2^n \mathrm{vol}(\Gamma) .$$

Damit existiert nach dem Gitterpunktsatz ein Gitterpunkt $j(a) \in X$ mit $a \neq 0$ und $a \in \mathfrak{a}$. □

BEMERKUNG 6.6.1
Satz 6.6.3 ist grundlegend für den Beweis der Endlichkeit der Klassenzahl $h_K = |\mathrm{Cl}_K|$ eines Zahlkörpers.

6.7. Der Dirichletsche Einheitensatz - Überblick

Es sei K ein algebraischer Zahlkörper. Der Dirichletsche Einheitensatz macht eine Aussage über die Gruppe $\mathcal{O}_K^*$ der Einheiten des Rings $\mathcal{O}_K$ der ganzen Zahlen in K.

DEFINITION 6.7.1
Unter $\mu(K)$ versteht man die Gruppe der Einheitswurzeln in K.

SATZ 6.7.1 (Einheitensatz von Dirichlet)
Es sei K ein algebraischer Zahlkörper. Die Gruppe $\mu(K)$ ist eine endliche zyklische Gruppe. Die Einheitengruppe $\mathcal{O}_K^*$ von $\mathcal{O}_K$ ist das direkte Produkt der endlichen zyklischen Gruppe $\mu(K)$ und einem freien $\mathbb{Z}$-Modul vom Rang $r+s-1$, d. h. es gibt Einheiten $\epsilon_1, \ldots, \epsilon_t \in \mathcal{O}_K^*$ mit $t = r+s-1$, die so genannten Grundeinheiten, so dass sich jede Einheit ϵ aus $\mathcal{O}_K^*$ eindeutig in der Form

$$\epsilon = \zeta \cdot \epsilon_1^{e_1} \cdots \epsilon_t^{e_t}$$

mit einer Einheitswurzel $\zeta \in \mu(K)$ und Exponenten $e_j \in \mathbb{Z}$ schreiben lässt.

BEISPIEL 6.7.1
Es sei $K = \mathbb{Q}(\sqrt{2})$. Die Einbettungen $\tau_1: \sqrt{2} \mapsto \sqrt{2}$ und $\tau_2: \sqrt{2} \mapsto -\sqrt{2}$ sind reell, es ist also $r = 2$ und $s = 0$ bzw. $r+s-1 = 1$. Man kann zeigen, dass $\mathcal{O}_K^* = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$ ist. Nun sei $K = \mathbb{Q}(\theta)$ mit einer Nullstelle $\theta \in \mathbb{C}$ des Polynoms

$$f(X) = X^3 - 4X - 1 = (X-\theta_1)(X-\theta_2)(X-\theta_3) .$$

Dieses Polynom besitzt drei reelle Nullstellen, es gibt daher drei reelle Einbettungen $\tau_i: \theta \to \theta_i$, also $r = 3$ und $s = 0$, bzw. $t = 2$. Man kann zeigen, dass $\mathcal{O}_K^* = \{\pm\epsilon_1^{e_1}\epsilon_2^{e_2} \mid e_1, e_2 \in \mathbb{Z}\}$ ist mit $\epsilon_1 = \theta$ und $\epsilon_2 = 2 + \theta$ (es ist $\theta \cdot (\theta+2) \cdot (\theta-2) = \theta^3 - 4\theta = 1$).

Beweisidee zum Einheitensatz:
Um die Gittertheorie auf die multiplikative Struktur $\mathcal{O}_K^*$ anwenden zu können kombiniert man die Abbildung $j: K^* \to K_\mathbb{C}^* = \prod_\tau \mathbb{C}^*$ aus dem vorigen Abschnitt mit der logarithmischen Abbildung

$$l: K_\mathbb{C} \to \prod_\tau \mathbb{R} \;,\; (z_1, \ldots, z_n) \mapsto (\ln|z_1|, \ldots, \ln|z_n|) .$$

Ferner betrachtet man die auf den Minkowski-Raum übertragenen Norm-/Spurabbildungen

$$N: K_\mathbb{R}^* \to \mathbb{R}^* \;,\; (z_1, \ldots, z_n) \mapsto \prod z_i \quad \text{und} \quad S: K_\mathbb{R} \to \mathbb{R} \;,\; (z_1, \ldots, z_n) \mapsto \sum z_i .$$

Dann ist das folgende Diagramm kommutativ:

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_\tau \mathbb{R} \\ \downarrow N & & \downarrow N & & \downarrow S \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow[\ln|\cdot|]{} & \mathbb{R} \end{array}$$

Durch Einschränkung auf Untergruppen erhält man ein Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & (\prod \mathbb{R})^+ \\ \downarrow N & & \downarrow N & & \downarrow S \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow[\ln|\cdot|]{} & \mathbb{R} \end{array}$$

Hierbei ist $(\prod_\tau \mathbb{R})^+ = \{(x_\tau) \mid x_\tau = x_{\bar{\tau}}\}$ der unter F fixe Teilraum. Das Bild der Einheitengruppe $\mathcal{O}_K^*$ unter j liegt in der Norm-Eins-Fläche $N_1 = \{(z_1, \ldots, z_n) \in K_{\mathbb{R}}^* \mid \prod z_j = 1\}$. Das Bild von N_1 unter l ist die Spur-Null-Hyperebene $S_0 = \{(x_1, \ldots, x_n) \in (\prod_\tau \mathbb{R})^+ \mid \sum x_j = 0\}$. Mit den Methoden der vorigen Abschnitte zeigt man, dass $(l \circ j)(\mathcal{O}_K^*)$ ein vollständiges Gitter des $(r+s-1)$-dimensionalen reellen Vektorraums S_0 ist. Andererseits liegen die Einheitswurzeln $\mu(K)$ im Kern der Abbildung $l \circ j$, womit die Behauptung aus dem Homomorphiesatz für Gruppen folgt.

Beispiel 6.7.2
Für $K = \mathbb{Q}(\sqrt{2})$ ist $\mathcal{O}_K^* = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$. Es ist

$$\begin{array}{rcl} j(a_0 + a_1\sqrt{2}) & = & (a_0 + a_1\sqrt{2}, a_0 - a_1\sqrt{2}) \\ (l \circ j)(a_0 + a_1\sqrt{2}) & = & (\ln|a_0 + a_1\sqrt{2}|, \ln|a_0 - a_1\sqrt{2}|) \quad . \end{array}$$

Anhang

Die Inhalte des Anhangs sind nicht prüfungsrelevant für den Vorlesungszyklus Algebra I/II.

7. Norm, Spur, Hauptpolynom

7.1. Definition über Lineare Algebra

Im Folgenden sei L/K eine endliche Körpererweiterung vom Grad n, nach Definition ist L dann ein n-dimensionaler K-Vektorraum. Zu einem Element α in L bezeichne

$$\varphi_\alpha \;=\; \begin{cases} L & \to & L \\ \beta & \mapsto & \alpha\beta \end{cases}$$

die Multiplikation mit α. Es sei $\mathrm{End}_K(L)$ der Ring der K-Vektorraumendomorphismen von L, versehen mit der Addition $(\varphi+\varphi')(\beta) = \varphi(\beta)+\varphi'(\beta)$ und der Multiplikation $(\varphi\circ\varphi')(\beta) = \varphi(\varphi'(\beta))$. Man rechnet leicht nach, dass die Endomorphismen damit tatsächlich einen Ring bilden, und die Zuordnung

$$\Phi \;=\; \begin{cases} L & \to & \mathrm{End}_K(V) \\ \alpha & \mapsto & \varphi_\alpha \end{cases}$$

ein Monomorphismus von Ringen ist. Für eine fest gewählte Basis $B = \{\beta_1, \ldots, \beta_n\}$ von L über K besitzt jedes $\varphi \in \mathrm{End}_K(L)$ bzgl. B genau eine Darstellungsmatrix $A = (a_{ij}) \in K^{(n,n)}$, diese ist durch die Wirkung von φ auf den Basiselementen festgelegt:

$$\varphi(\beta_i) \;=\; \sum_{j=1}^{n} a_{ij}\beta_j \,.$$

Die Darstellungsmatrix von φ bzgl. B sei mit $\mathcal{M}(\varphi)$ bezeichnet. Die Zuordnungskette

$$\begin{array}{ccccc} L & \longrightarrow & \mathrm{End}_K(L) & \longrightarrow & K^{(n,n)} \\ \alpha & \mapsto & \varphi_\alpha & \mapsto & \mathcal{M}(\varphi_\alpha) \end{array}$$

definiert einen Ringmonomorphismus von L in den Matrizenring $K^{(n,n)}$. Die Zuordnung Φ ist nicht surjektiv, denn die K-Dimension von $K^{(n,n)}$ bzw. $\mathrm{End}_K(L)$ ist n^2, die Dimension von L ist aber nur n. Werden die Abbildungen auf die Einheitengruppen der betrachteten Ringe eingeschränkt, so erhält man die Kette

$$\begin{array}{ccccc} L^* & \longrightarrow & \mathrm{Aut}_K(L) & \longrightarrow & \mathrm{GL}(n,K) \\ \alpha & \mapsto & \varphi_\alpha & \mapsto & \mathcal{M}(\varphi_\alpha) \end{array}$$

von Gruppenmonomorphismen, die ebenfalls nicht surjektiv ist.

Definition 7.1.1
Norm, Spur und Hauptpolynom eines Elements $\alpha \in L$ über K sind gegeben durch

$$\begin{array}{rcl} N_{L/K}(\alpha) & = & \det(\mathcal{M}(\alpha)) \\ S_{L/K}(\alpha) & = & S(\mathcal{M}(\alpha)) \\ f_\alpha(X) & = & f_{\mathcal{M}(\alpha)}(X) \end{array}$$

mit der Spurabbildung $S:\ K^{(n,n)} \to K,\ (a_{ij}) \mapsto a_{11} + \cdots + a_{nn}$ und dem charakteristischen Polynom $f_A(X) = \det(E_n X - A)$ für Matrizen.

Wie in der Linearen Algebra sind diese Kenngrößen unabhängig von der Wahl der K-Basis B von L. Einschränkung auf die zu den Ringoperationen in L gehörenden Gruppen liefert Ketten

$$\begin{array}{lccccccc} N_{L/K}: & (L^*,\cdot) & \to & (\mathrm{Aut}_K(L),\circ) & \to & (\mathrm{GL}(n,K),\cdot) & \to & (K^*,\cdot) \\ S_{L/K}: & (L,+) & \to & (\mathrm{End}_K(L),+) & \to & (K^{(n,n)},+) & \to & (K,+) \end{array}$$

von Gruppenhomomorphismen. Da die Darstellungsmatrix von φ_a für ein $a \in K$ aus dem Grundkörper die Form

$$\mathcal{M}(\varphi_a) = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$$

besitzt folgt $N_{L/K}(a) = a^n$, $S_{L/K}(a) = na$ und $f_a(X) = (X-a)^n$. Man sieht, dass Norm, Spur und Hauptpolynom von der betrachteten Körpererweiterung abhängen, und dass das Hauptpolynom nicht notwendig das Minimalpolynom des jeweiligen Elements ist.

7.2. Definition über Einbettungen

Wieder sei L/K eine endliche Körpererweiterung. Ist L/K galoissch, so können Norm, Spur und Hauptpolynom auch über

$$\begin{array}{rcl} N_{L/K}(\alpha) & = & \prod \sigma(\alpha) \\ S_{L/K}(\alpha) & = & \sum \sigma(\alpha) \\ f_\alpha(X) & = & \prod (X - \sigma(\alpha)) \end{array}$$

definiert werden (vgl. Definition 5.5.1), wobei Summen/Produkte über die $\sigma \in G(L/K)$ laufen. Ist die Erweiterung nicht galoissch, so entstehen zwei Probleme: K-Isomorphismen von L besitzen nicht notwendig Bilder in L, und die Isomorphismen können nur in Spezialfällen (z.B. im Falle der Existenz eines primitiven Elements) explizit angegeben werden. Im Fall einer allgemeinen endlichen Erweiterung können statt dessen injektive Ringhomomorphismen (genannt Einbettungen) benutzt werden, die L in einen umfassenden Körper einbetten:

Definition 7.2.1
Ein algebraischer Abschluss K' eines Körper K ist ein Oberkörper von K, in dem alle Polynome $f(X) \in K[X]$ linear zerfallen, und der minimal mit dieser Eigenschaft ist.

Für die endlichen Körper $\mathbb{F}_p$ gibt es einen algebraischen Abschluss: die unendliche Vereinigung aller $\mathbb{F}_{p^n}$. Der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ wurde in einer Übungsaufgabe in Algebra I vorgestellt. Für allgemeine Körper ist die Existenz eines Abschlusses nicht unmittelbar nachzuweisen, und tatsächlich ist der Beweis für $\mathbb{Q}$ nur deshalb einfach, weil die explizite Konstruktion der Mengen $\mathbb{R}$ und $\mathbb{C}$ stillschweigend übergangen wurde. Der allgemeine Satz ist durchaus nicht trivial:

Satz 7.2.1
Zu jedem Körper K gibt es einen algebraischen Abschluss $\overline{K}$ von K, und jeder weitere Abschluss von K ist zu $\overline{K}$ isomorph.

Beweis
(siehe Abschnitt 3.4, Korollare 7 und 10 aus *Algebra* von R. Bosch) □

Daher spricht man auch von *dem* algebraischen Abschluss von K (Schreibweise: $\overline{K}$).

Definition 7.2.2
Eine Einbettung zur Körpererweiterung L/K ist eine Abbildung $\sigma: L \to \overline{K}$, die ein K-linearer injektiver Ringhomomorphismus ist.

Beispiel 7.2.1
Ist die endliche Erweiterung L/K einfach mit primitivem Element $\theta \in L$, so bilden alle Einbettungen σ den Körper K schon in den Zerfällungskörper Z des Minimalpolynoms von θ über K ab, der ein Teilkörper des zugehörigen Abschlusses ist. In diesem Fall sind die Einbettungen eindeutig parametrisiert durch die Zuordnungen $\theta \mapsto \theta_i$ des primitiven Elements zu seinen Konjugierten im Zerfällungskörper.

Es bezeichne $\mathrm{Hom}_K^1(L, \overline{K})$ stets die Menge der Einbettungen zur endlichen Körpererweiterung L/K. Im Galoisfall bildet sie die Galoisgruppe, da dann alle Einbettungen wieder in L abbilden, und damit K-Automorphismen $\sigma : L \to L$ sind.

Definition 7.2.3
Es sei L/K endlich und separabel. Norm, Spur und Hauptpolynom eines Elements $\alpha \in L$ sind

$$\begin{array}{rcl} N_{L/K}(\alpha) & = & \prod \sigma(\alpha) \\ S_{L/K}(\alpha) & = & \sum \sigma(\alpha) \\ f_\alpha(X) & = & \prod (X - \sigma(\alpha)) \end{array}$$

wobei σ über die Einbettungen in $\mathrm{Hom}_K^1(L, \overline{K})$ läuft.

Diese Definitionen stimmen für separable Erweiterungen mit der Definition über die Darstellungsmatrix überein, vgl. Abschnitt 4.7 Satz 4 aus *Algebra* von R. Bosch.

7.3. Hilberts Satz 90

Satz 7.3.1 (HS90 multiplikativ)
Ist L/K eine Galoiserweiterung mit zyklischer Galoisgruppe $G = \langle \sigma \rangle$ so gilt für jedes $\alpha \in L$:

$$N_{L/K}(\alpha) \;=\; 1 \quad \Leftrightarrow \quad \exists \beta \in L : \; \alpha = \frac{\beta}{\sigma(\beta)}$$

Beweis
Es sei $\alpha = \beta \cdot \sigma(\beta)^{-1}$ für ein $\beta \in L^*$. Da die Norm multiplikativ aber σ-invariant ist, folgt

$$N_{L/K}(\alpha) \;=\; N_{L/K}(\beta) \cdot N_{L/K}(\beta)^{-1} \;=\; 1 \,.$$

Sei nun umgekehrt $\alpha \in L$ beliebig mit $N_{L/K}(\alpha) = 1$ und $n = [L : K] = \mathrm{ord}(\sigma)$. Aufgrund der linearen Unabhängigkeit verschiedener Charaktere (Satz 5.3.2) ist die Zuordnung

$$\gamma \;\mapsto\; \sigma^0(\gamma) + \alpha\sigma^1(\gamma) + \alpha\sigma^1(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma)$$

als Abbildung $L^* \to L$ nicht die Nullabbildung. Also gibt es $\gamma \in L^*$ mit

$$\beta \;=\; \sigma^0(\gamma) + \alpha\sigma^1(\gamma) + \alpha\sigma^1(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma) \;\neq\; 0 \,.$$

Anwenden von σ und Multiplikation mit α ergibt

$$\alpha \cdot \sigma(\beta) \;=\; \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n(\gamma) \;=\; \beta$$

wegen $\sigma^n = \mathrm{id}$ und $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = N_{L/K}(\alpha) = 1$. Daraus folgt $\alpha = \beta \cdot \sigma(\beta)^{-1}$. □

Mit einem ähnlichen Verfahren zeigt man

Satz 7.3.2 (HS90 additiv)
Ist L/K eine Galoiserweiterung mit zyklischer Galoisgruppe $G = \langle \sigma \rangle$ so gilt für jedes $\alpha \in L$:

$$S_{L/K}(\alpha) \;=\; 0 \quad \Leftrightarrow \quad \exists \beta \in L : \; \alpha = \beta - \sigma(\beta) \,.$$

8. Endlichkeit der Klassenzahl

Die Analyse der algebraischen Zahlkörper zergliedert sich in die Analyse der Einheitengruppe (diese wird durch den Einheitensatz von Dirichlet gegeben) und die Idealstruktur in $\mathcal{O}_K$. Das Zielobjekt dieser Analyse ist die Idealklassengruppe $\mathrm{Cl}_K = \mathcal{J}_K/\mathcal{P}_K$. Die zentrale Erkenntnis dieses Aufgabenfeldes ist

Satz 8.0.3
Für jeden Zahlkörper ist die Klassengruppe endlich.

Zum Beweis dieses Satzes ist einige Vorbereitung nötig:

Definition 8.0.1
Die Norm eines ganzen Ideals $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ ist der Gruppenindex $N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$.

Durch Quotientenbildung ist die Norm auch für gebrochene Ideale definiert. Die Namensgebung ist dadurch bedingt, dass für Hauptideale $\mathfrak{a} = (\alpha)$ stets $N(\mathfrak{a}) = |N(\alpha)|$ gilt. Durch diese Definition wird der Normbegriff von $\mathcal{O}_K$ auf den übergeordneten Bereich der Ideale ausgeweitet. Wie für Körperelemente ist auch die Idealnorm multiplikativ.

Lemma 8.0.4
Es gibt eine Konstante c, die nur vom Zahlkörper K abhängt, so dass in jeder Idealklasse mindestens ein ganzes Ideal $\mathfrak{b}$ mit $N(\mathfrak{b}) \leq c$ liegt.

Beweis
Sei $C \in \mathrm{Cl}_K$ eine Idealklasse und $\mathfrak{a}$ ein ganzes Ideal in der dazu inversen Klasse C^{-1}. Satz 6.6.5 besagt, dass es in $\mathfrak{a}$ mindestens ein von Null verschiedenes Element α gibt, dessen Norm die Schranke

$$\left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_k|} \cdot N(\mathfrak{a})$$

nicht übersteigt. Wir setzen $\mathfrak{a}' = (\alpha)$ und $\mathfrak{b} = \mathfrak{a}' \cdot \mathfrak{a}^{-1}$. Dann gilt $N(\mathfrak{b}) \leq N(\mathfrak{a}) \cdot (\frac{2}{\pi})^s \sqrt{|d_K|} \cdot N(\mathfrak{a})^{-1} = c$ mit der Schranke $c = (\frac{2}{\pi})^s \sqrt{|d_K|}$. Das Ideal $\mathfrak{b}$ liegt in der Klasse $[\mathfrak{a}^{-1}] = C$, da es sich von $\mathfrak{a}^{-1}$ nur um das Hauptideal $\mathfrak{a}'$ unterscheidet. Es ist auch ganz, denn es ist wegen $\mathfrak{a}' \subseteq \mathfrak{a}$ eine Teilmenge von $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$. □

Lemma 8.0.5
Für jedes $c > 0$ gibt es nur endlich viele ganze Ideale, deren Norm durch c beschränkt ist.

Beweis
Es ist $N(\mathfrak{P}) = (\mathcal{O}_K : \mathfrak{P})$ für ein Primideal $\mathfrak{P}$ die Elementanzahl des Körpers $\mathcal{O}_K/\mathfrak{P}$, also p^f für ein $f \geq 1$. Für jede Primzahl p ist $(p) = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ für endlich viele Primideale $\mathfrak{P}_j$. Es gibt aber andererseits nur endlich viele Primzahlen, für die p^f unter c liegen kann, woraus folgt, dass nur endlich viele Primideale eine durch c beschränkte Norm besitzen. Für $\mathfrak{P}|\mathfrak{a}$ ist aber $N(\mathfrak{P}) \leq N(\mathfrak{a})$, also gibt es auch nur endlich viele ganze Ideale überhaupt unter der Normschranke c. □

Beweis der Endlichkeit der Klassenzahl
Für die Schranke c aus dem ersten Lemma gibt es für jede Idealklasse ein ganzes Ideal unter dieser Schranke darin, aber nach dem zweiten Lemma kann es insgesamt nur endlich viele solche Ideale geben, also gibt es auch nur endlich viele Idealklassen, da Ideale aus verschiedenen Klassen verschieden sind. □

Definition 8.0.2
Die Zahl $h_K = [\mathcal{J}_K : \mathcal{P}_K] < \infty$ heißt Klassenzahl von K.

Die Klassenzahl ist das Maß für die Zunahme der Komplexität beim Übergang von Zahlen zu Idealen. Für $h_K = 1$ ist $\mathcal{O}_K$ ein Hauptidealring, d. h. es stimmen die Elemente $\alpha \in \mathbb{K}^*$ mit den Idealen $\mathfrak{a} \in \mathcal{J}_K$ bis auf Einheiten überein. Ansonsten besteht $\mathcal{J}_K$ aus h_K Kopien der Hauptidealgruppe.