SKRIPT ZUR VORLESUNG ALGEBRA (ALGEBRA II)

STEFAN GESCHKE

ZUSAMMENFASSUNG. Es handelt sich um die Fortsetzung der Vorlesung "Einführung in die Algebra und Zahlentheorie" nach dem Skript von Prof. V. Schulze. Der Inhalt jener Vorlesung (Kap. 1: Gruppen, Kap. 2: Ringe, Kap. 3: Ideale in kommutativen Ringen, Kap. 4: Elementare Körpertheorie) wird vorausgesetzt.

1. GALOISTHEORIE

1.1. **Körperautomorphismen.** Wir beginnen mit einigen Betrachtungen über Körperautomorphismen.

Definition und Bemerkung 1.1. Für zwei Mengen X und Y bezeichne $\mathrm{Abb}(X,Y)$ die Menge der Abbildungen von X nach Y.

Für einen Körper K lassen sich folgende Verknüpfungen auf $\mathrm{Abb}(X,K)$ definieren: Für $f_1, f_2 \in \mathrm{Abb}(X,K)$ sei

(i) $f_1 + f_2 \in \mathrm{Abb}(X,K)$ definiert durch $(f_1+f_2)(x) := f_1(x) + f_2(x)$ für alle $x \in X$ und
(ii) $f_1 \cdot f_2$ durch $(f_1 \cdot f_2)(x) := f_1(x) \cdot f_2(x)$ für alle $x \in X$.
(iii) Für $\alpha \in K$ und $f \in \mathrm{Abb}(X,K)$ sei $\alpha \cdot f$ definiert durch $(\alpha \cdot f)(x) := \alpha \cdot f(x)$ für alle $x \in X$.

Durch die in (i) und (iii) definierten Verknüpfungen wird $\mathrm{Abb}(X,K)$ zu einem K-Vektorraum.

Satz 1.2. *Sei H Halbgruppe, K^0 die multiplikative Gruppe eines Körpers K und $h_1, \ldots, h_n$ Homomorphismen von H nach K^0. Es gilt:*

$h_1, \ldots, h_n$ sind genau dann paarweise verschieden, wenn sie als Elemente des K-Vektorraums $\mathrm{Abb}(H,K)$ linear unabhängig sind.

Beweis. Offenbar sind linear unabhängige Elemente eines Vektorraums paarweise verschieden. Das zeigt die eine Richtung der Äquivalenz. Die andere Richtung zeigen wir mittels vollständiger Induktion über n.

Seien $n = 1$ und $\alpha \in K$. Ist $\alpha \cdot h_1$ die Nullabbildung, also $\alpha \cdot h_1(x) = 0$ für alle $x \in X$, so folgt $\alpha = 0$ aus der Nullteilerfreiheit von K.

Sei nun $n > 1$ und die Behauptung bereits gezeigt für alle $m < n$. Sind $h_1, \ldots, h_n$ paarweise verschieden, so existiert ein $a \in K$ mit $h_1(a) \neq h_n(a)$. Angenommen $\alpha_1 h_1 + \cdots + \alpha_n h_n$ ist die Nullabbildung für gewisse $\alpha_1, \ldots, \alpha_n \in K$. Wir müssen zeigen, daß alle α_i null sind.

Für alle $x \in H$ gilt $\alpha_1 h_1(x) + \cdots + \alpha_n h_n(x) = 0$. Damit ist auch für alle $x \in H$

$$\alpha_1 h_1(a) h_1(x) + \cdots + \alpha_n h_n(a) h_n(x) = \alpha_1 h_1(ax) + \cdots + \alpha_n h_n(ax) = 0.$$

Dieses Skript basiert weitgehend auf dem handgeschriebenen Skript "Algebra" von Prof. V. Schulze.

Außerdem gilt für alle $x \in H$

$$\alpha_1 h_1(a)h_1(x) + \cdots + \alpha_n h_1(a)h_n(x) = h_1(a) \cdot (\alpha_1 h_1(x) + \cdots + \alpha_n h_n(x)) = 0.$$

Differenzbildung liefert

$$\alpha_2(h_2(a) - h_1(a))h_2(x) + \cdots + \alpha_n(h_n(a) - h_1(a))h_n(x) = 0.$$

Aus der Induktionsvoraussetzung folgt $\alpha_i(h_i(a) - h_1(a)) = 0$ für alle $i \in \{2, \ldots, n\}$. Wegen der Wahl von a ist $h_n(a) - h_1(a) \neq 0$ und damit $\alpha_n = 0$. Also ist bereits $\alpha_1 h_1 + \cdots + \alpha_{n-1} h_{n-1}$ die Nullabbildung. Eine weitere Anwendung der Induktionsvoraussetzung liefert schließlich $\alpha_i = 0$ für alle $i \in \{1, \ldots, n\}$. □

Folgerung 1.3. *Seien L_1 und L_2 Körper und $h_1, \ldots, h_n$ paarweise verschiedene injektive Körperhomomorphismen von L_1 nach L_2. Dann sind $h_1, \ldots, h_n$ linear unabhängig über L_2.*

Beweis. Da die h_i paarweise verschiedene Körperhomomorphismen sind, sind bereits ihre Einschränkungen auf die multiplikative Gruppe L_1^0 von L_1 paarweise verschieden. Da die h_i injektiv sind, sind die Mengen $h_i[L_1^0]$ Teilmengen von L_2^0. Damit sind die Abbildungen $h_i \restriction L_1^0$ Gruppenhomomorphismen von L_1^0 nach L_2^0. Nach Satz 1.2 sind nun die $h_i \restriction L_1^0$ linear unabhängig als Elemente des L_2-Vektorraumes $\mathrm{Abb}(L_1^0, L_2)$. Erst recht sind die h_i linear unabhängig als Elemente des L_2-Vektorraumes $\mathrm{Abb}(L_1, L_2)$. □

Definition und Bemerkung 1.4. Seien L_1 und L_2 endliche Erweiterungen des Körpers K. L_1 und L_2 sind also endlich dimensionale K-Vektorräume. $\mathrm{Hom}_K(L_1, L_2)$ bezeichnet die Menge der K-linearen Abbildungen von L_1 nach L_2. In der üblichen Weise läßt sich $\mathrm{Hom}_K(L_1, L_2)$ als K-Vektorraum auffassen. $\mathrm{Hom}_K(L_1, L_2)$ ist außerdem ein Unterraum des L_2-Vektorraumes $\mathrm{Abb}(L_1, L_2)$.

Lemma 1.5. *Seien K, L_1 und L_2 wie eben. Dann gilt:*

$$\dim_{L_2}(\mathrm{Hom}_K(L_1, L_2)) = [L_1 : K]$$

Beweis. Falls V ein L-Vektorraum ist und K ein Unterkörper von L, so läßt sich V auch als K-Vektorraum auffassen und es gilt $\dim_K(V) = \dim_L(V) \cdot [L : K]$. Letzteres folgt aus dem Beweis der Körpergradformel. Aus der linearen Algebra weiß man

$$\dim_K(\mathrm{Hom}_K(L_1, L_2)) = \dim_K(L_1) \cdot \dim_K(L_2) = [L_1 : K] \cdot [L_2 : K].$$

Zusammen ergibt sich die Behauptung. □

Satz 1.6. *Seien K, L_1 und L_2 wie eben und $h_1, \ldots, h_n$ paarweise verschiedene injektive Körperhomomorphismen von L_1 nach L_2, die K elementweise fest lassen. Dann gilt $n \leq [L_1 : K]$.*

Beweis. Da K elementweise fest bleibt, lassen sich $h_1, \ldots, h_n$ auffassen als Elemente des L_2-Vektorraumes $\mathrm{Hom}_K(L_1, L_2)$. Nach Folgerung 1.3 sind die h_i linear unabhängig über L_2. Andererseits gilt $\dim_{L_2}(\mathrm{Hom}_K(L_1, L_2)) = [L_1 : K]$ nach Lemma 1.5. Zusammen ergibt sich die Behauptung. □

Definition 1.7. Seien K und L Körper mit $K \leq L$. Dann ist $\mathrm{Aut}(L)$ die Gruppe aller Automorphismen von L und $\mathrm{Gal}(L : K)$ die Gruppe aller Automorphismen von L, die K elementweise fest lassen. $\mathrm{Aut}(L)$ ist die *Automorphismengruppe* von L und $\mathrm{Gal}(L : K)$ die *Galoisgruppe* von $L : K$.

Als wichtiger Spezialfall von Satz 1.6 ergibt sich sofort

Satz 1.8. *Sei $L : K$ eine endliche Körpererweiterung. Dann gilt:*

$$|\mathrm{Gal}(L : K)| \leq [L : K]$$

Beispiel 1.9. Nach Satz 1.8 ist $|\,\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})\,| \leq 2$. Die Ordnung der Galoisgruppe von $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ ist in der Tat 2, und das Element φ von $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$, welches nicht die Identität ist, ist eindeutig dadurch bestimmt, daß es $\sqrt{2}$ auf $-\sqrt{2}$ abbildet. Für $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ist $\varphi(a+b\sqrt{2}) = a - b\sqrt{2}$.

Beispiel 1.10. $\sqrt[3]{2}$ bezeichnet die reelle 3-te Wurzel von 2. Die Galoisgruppe von $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ enthält nur die Identität:

Sei nämlich $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$. $\sqrt[3]{2}$ ist Nullstelle von $X^3 - 2$, einem Polynom mit Koeffizienten in $\mathbb{Q}$. Da φ ein Körperhomomorphismus ist, der die Elemente von $\mathbb{Q}$ fest läßt, ist auch $\varphi(\sqrt[3]{2})$ Nullstelle von $X^3 - 2$. $\mathbb{Q}(\sqrt[3]{2})$ enthält aber nur reelle Zahlen und $\sqrt[3]{2}$ ist die einzige reelle Nullstelle von $X^3 - 2$. Damit ist $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. Da φ auf einem Erzeugendensystem von $\mathbb{Q}(\sqrt[3]{2})$ die Identität ist, nämlich auf $\mathbb{Q} \cup \{\sqrt[3]{2}\}$, gilt $\varphi = \mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}$.

Definition und Bemerkung 1.11. Sei G eine Gruppe (oder einfach eine Menge) von Automorphismen des Körpers L. Dann ist

$$\mathrm{Fix}_L(G) := \{x \in L : \forall g \in G(g(x) = x)\}$$

ein Unterkörper von L, der *Fixpunktkörper* von G in L.

Je kleiner die Gruppe G ist, desto größer ist ihr Fixpunktkörper. Das spiegelt sich im nächsten Satz wieder.

Satz 1.12. *Sei G eine endliche Gruppe von Automorphismen des Körpers L. Dann gilt $[L : \mathrm{Fix}_L(G)] = |G|$.*

Bevor wir diesen Satz beweisen, leiten wir eine wichtige Folgerung ab.

Folgerung 1.13. *Sei $L : K$ eine endliche Körpererweiterung. Dann gilt:*

$$|\mathrm{Gal}(L : K)| = [L : K] \Leftrightarrow K = \mathrm{Fix}_L(\mathrm{Gal}(L : K))$$

Beweis. Die Rückrichtung folgt aus Satz 1.12, da $|\mathrm{Gal}(L : K)|$ nach Satz 1.8 endlich ist.

Für die andere Richtung der Äquivalenz beachte, daß nach Satz 1.12

$$|\mathrm{Gal}(L : K)| = [L : \mathrm{Fix}_L(\mathrm{Gal}(L : K))]$$

gilt. Nach Voraussetzung gilt $|\,\mathrm{Gal}(L : K)\,| = [L : K]$. Offenbar ist K ein Unterkörper von $\mathrm{Fix}_L(\mathrm{Gal}(L : K))$. Damit ist $K = F$. □

Diese Folgerung motiviert die nächste Definition.

Definition 1.14. Eine Körpererweiterung $L : K$ heißt *galoissch*, wenn K der Fixpunktkörper von $\mathrm{Gal}(L : K)$ ist.

Zum Beweis von Satz 1.12 benötigen wir

Lemma 1.15. *Sei L ein Körper und U eine endliche Gruppe von Automorphismen von L. Für alle $a \in L$ sei*

$$\mathrm{Spur}_U(a) := \sum_{u \in U} u(a)$$

die Spur *von a bezüglich U. Dann gilt:*

(i) *Für alle $v \in U$ und alle $a \in L$ ist $v(\mathrm{Spur}_U(a)) = \mathrm{Spur}_U(a)$.*
(ii) *Es gibt ein $b \in L$ mit $\mathrm{Spur}_U(b) \neq 0$.*

Beweis. (i) Für alle $v \in U$ und $a \in L$ gilt

$$v(\mathrm{Spur}_U(a)) = v\left(\sum_{u \in U} u(a)\right) = \sum_{u \in U} vu(a) = \sum_{u \in U} u(a) = \mathrm{Spur}_U(a).$$

Das vorletzte Gleichheitszeichen liegt an der Tatsache, daß mit u auch vu alle Elemente von U je einmal durchläuft.

(ii) $\mathrm{Spur}_U(a) = \sum_{u \in U} u(a) = 0$ für alle $a \in L$ ist unmöglich, da sonst die Elemente von U über L linear abhängig wären, im Widerspruch zu Folgerung 1.3. □

Beweis von Satz 1.12. Setze $F := \mathrm{Fix}_L(G)$. Da G nach Voraussetzung endlich ist, gilt $|G| \leq [L : F]$ automatisch falls $L : F$ unendlich ist. Falls $L : F$ endlich ist, so gilt $|G| \leq [L : F]$ nach Satz 1.8, da G eine Teilmenge von $\mathrm{Gal}(L : F)$ ist.

Sei nun $G = \{g_1, \ldots, g_n\}$ und seien $a_1, \ldots, a_{n+1} \in L$ beliebig. Wir zeigen, daß die a_i, $i \in \{1, \ldots, n+1\}$, linear abhängig über F sind.

Betrachte dazu das homogene Gleichungssystem

$$\sum_{i=1}^{n+1} g_j^{-1}(a_i) x_i = 0 \qquad (j \in \{1, \ldots, n\}).$$

Dieses Gleichungssystem besitzt eine nichttriviale Lösung $(z_1, \ldots, z_{n+1}) \in L^{n+1}$, da es mehr Variablen als Gleichungen hat. O.B.d.A. sei $z_1 \neq 0$. Nach Lemma 1.15(ii) existiert ein $b \in L$ mit $\mathrm{Spur}_G(b) \neq 0$. Da mit $(z_1, \ldots, z_{n+1})$ auch der Vektor $(b, bz_1^{-1}z_2, \ldots, bz_1^{-1}z_{n+1})$ Lösung des Gleichungssystems ist, können wir $\mathrm{Spur}_G(z_1) \neq 0$ annehmen.

Anwendung von g_j auf die j-te Gleichung liefert

$$\sum_{i=1}^{n+1} a_i g_j(z_i) = 0$$

für alle $j \in \{1, \ldots, n\}$. Summation über j liefert

$$\sum_{i=1}^{n+1} a_i \,\mathrm{Spur}_G(z_i) = 0.$$

Nach Lemma 1.15(i) ist $\mathrm{Spur}_G(z_i) \in \mathrm{Fix}_L(G) = F$ für alle $i \in \{1, \ldots, n+1\}$. Aus $\mathrm{Spur}_G(z_1) \neq 0$ folgt nun die lineare Abhängigkeit von $a_1, \ldots, a_{n+1}$ über F. Damit haben wir die noch fehlende Ungleichung $[L : F] \leq |G|$ gezeigt. □

1.2. **Galoissche Erweiterungen.** Für jede endliche Körpererweiterung $L : K$ gilt nach Satz 1.8

$$|\mathrm{Gal}(L : K)| \leq [L : K],$$

und nach Folgerung 1.13 ist

$$|\mathrm{Gal}(L : K)| = [L : K]$$

genau dann, wenn K der Fixpunktkörper von $\mathrm{Gal}(L : K)$ ist.

Der nächste Satz charakterisiert galoissche Körpererweiterungen.

Satz 1.16. *Sei $L : K$ endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

(i) *$L : K$ ist galoissche Erweiterung, d.h., $K = \mathrm{Fix}_L(\mathrm{Gal}(L : K))$ (siehe Definition 1.14).*
(ii) *$[L : K] = |\mathrm{Gal}(L : K)|$*
(iii) *$L : K$ ist normale und separable Erweiterung.*
(iv) *L ist der Zerfällungskörper eines separablen Polynoms $f \in K[X]$.*

Beweis. (i) und (ii) sind äquivalent nach Folgerung 1.13.

(i)⇒(iii): Wir zeigen zunächst, daß $L : K$ separabel ist, d.h., daß jedes $a \in L$ Nullstelle eines separablen Polynoms $f \in K[X]$ ist. Man erinnere sich, daß ein Polynom genau dann separabel ist, wenn jeder irreduzible Faktor in seinem Zerfällungskörper nur einfache Nullstellen hat.

Sei $\{\varphi(a) : \varphi \in \mathrm{Gal}(L : K)\} = \{a_1, \ldots, a_n\}$ mit paarweise verschiedenen a_i. Setze

$$f := \prod_{i=1}^{n}(X - a_i) = \sum_{j=0}^{n} b_j X^j.$$

Wegen $\mathrm{id}_L \in \mathrm{Gal}(L : K)$ ist a Nullstelle von f. Zu zeigen ist $f \in K[X]$.

Jedes $\varphi \in \mathrm{Gal}(L : K)$ läßt sich eindeutig zu einem Isomorphismus $\tilde{\varphi} : L[X] \to L[X]$ fortsetzen. $\tilde{\varphi}$ permutiert die a_i und fixiert X. Damit ist $\tilde{\varphi}(f) = f$. Die Koeffizienten b_j von f liegen also im Fixpunktkörper von $\mathrm{Gal}(L : K)$. Nach (i) ist $\mathrm{Fix}_L(\mathrm{Gal}(L : K)) = K$. Also ist f tatsächlich ein Polynom mit Koeffizienten in K.

Es ist auch klar, daß f separabel ist, da f in L zerfällt und nur einfache Nullstellen hat. Es bleibt zu zeigen, daß $L : K$ normal ist. Dazu genügt es zu zeigen, daß L Zerfällungskörper eines Polynoms mit Koeffizienten in K ist (Satz 32.1, Einführung in die Algebra und Zahlentheorie).

Da $L : K$ endlich und separabel ist, existiert nach dem Satz vom primitiven Element (Satz 31.2, Einführung in die Algebra und Zahlentheorie) ein $\vartheta \in L$ mit $L = K(\vartheta)$. Führt man die Konstruktion im ersten Teil des Beweises für ϑ anstelle von a durch, so erhält man ein Polynom $g \in K[X]$ mit $g(\vartheta) = 0$, welches in $L[X]$ in Linearfaktoren zerfällt. L ist also der Zerfällungskörper von g.

(iii)⇒(iv): Nach (iii) ist $L : K$ normal, also Zerfällungskörper eines Polynoms $f \in K[X]$ (Satz 32.1, Einführung in die Algebra und Zahlentheorie). Sei g ein irreduzibler Faktor von f, o.B.d.A. normiert. Es ist zu zeigen, daß g separabel ist. Sei $\alpha \in L$ Nullstelle von g. Da g irreduzibel und normiert ist, ist g das Minimalpolynom von α über K, also $g = \mathrm{Irr}(\alpha, K)$. Nach (iii) ist $L : K$ separabel. Also ist $g = \mathrm{Irr}(\alpha, K)$ separabel.

(iv)⇒(i): Offenbar gilt $K \leq \mathrm{Fix}_L(\mathrm{Gal}(L : K))$. Es bleibt $\mathrm{Fix}_L(\mathrm{Gal}(L : K)) \leq K$ zu zeigen. Sei L der Zerfällungskörper von $f \in K[X]$, f separabel über K.

Wir verwenden eine vollständige Induktion über die Anzahl r der Nullstellen von f, die nicht in K liegen. Ist $r = 0$, so zerfällt f bereits in $K[X]$ und es gilt $K = L = \mathrm{Fix}_L(\mathrm{Gal}(L : K))$.

Für den Induktionsschritt sei $a \in L \setminus K$ eine Nullstelle von f. Betrachte $M := K(a)$ als neuen Grundkörper. Dann ist L der Zerfällungskörper von $f \in M[X]$, und f ist separabel über M. Nach Induktionsvoraussetzung ist $M = \mathrm{Fix}_L(\mathrm{Gal}(L : M))$. Also gilt $\mathrm{Fix}_L(\mathrm{Gal}(L : K)) \leq M$.

Sei $g := \mathrm{Irr}(a, K)$ und $n := \mathrm{grad}(g)$. Dann ist $1, a, \ldots, a^{n-1}$ eine Basis von $M = K(a)$ über K (Satz 27.3, Einführung in die Algebra und Zahlentheorie). Sei nun $\alpha \in \mathrm{Fix}_L(\mathrm{Gal}(L : K))$. Zu zeigen ist $\alpha \in K$.

α ist eine Linearkombination der Basiselemente $1, a, \ldots, a^{n-1}$, z.B.

$$\alpha = k_0 + k_1 a + \cdots + k_{n-1} a^{n-1},$$

$k_i \in K$. $\alpha \in K$ ist gleichbedeutend mit $\alpha = k_0$.

Da g das Minimalpolynom von a ist und a eine Nullstelle von f, wird f von g geteilt. Da f separabel ist, ist auch g separabel. Seien $a_1, \ldots, a_n$ die verschiedenen Nullstellen von g in L. O.B.d.A. sei $a = a_1$.

Für alle $i \in \{1, \ldots, n\}$ existiert ein Isomorphismus $\varphi_i : K(a) \to K(a_i)$ mit $\varphi_i(a) = a_i$ und $\varphi_i \restriction K = \mathrm{id}_K$ (Folgerung 29.2, Einführung in die Algebra und Zahlentheorie). Jedes φ_i laßt sich zu einem Isomorphismus $\Phi_i : L \to L$ fortsetzen (Satz 29.3, Einführung in die Algebra und Zahlentheorie).

Offenbar ist jedes Φ_i ein Element von $\mathrm{Gal}(L : K)$. Wegen $\alpha \in \mathrm{Fix}_L(\mathrm{Gal}(L : K))$ gilt $\Phi_i(\alpha) = \alpha$ für alle $i \in \{1, \ldots, n\}$. Damit ist für alle i

$$\alpha = \Phi_i(k_0 + k_1 a + \cdots + k_{n-1} a^{n-1}) = k_0 + k_1 a_i + \cdots + k_{n-1} a_i^{n-1}.$$

Also hat das Polynom

$$h := (k_0 - \alpha) + k_1 X + \cdots + k_{n-1} X^{n-1} \in \mathrm{Fix}_L(\mathrm{Gal}(L : K))[X]$$

die n verschiedenen Nullstellen $a_1, \ldots, a_n$. Wegen $\mathrm{grad}(h) = n - 1$ muß h das Nullpolynom sein. Es gilt also $\alpha = k_0$, was zu zeigen war. □

Satz 1.16(iv) liefert sofort

Folgerung 1.17. *Sei $L : K$ eine endliche galoissche Köpererweiterung und M eine Körper mit $K \leq M \leq L$. Dann ist auch $L : M$ galoissch.*

Satz 1.18. *Sei $L : K$ eine endliche galoissche Körpererweiterung und M ein Körper mit $K \leq M \leq L$. Dann gilt:*

(i) *$M : K$ ist galoissch genau dann, wenn $M : K$ normal ist.*
(ii) *$M : K$ ist normal genau dann, wenn für alle $\varphi \in \mathrm{Gal}(L : K)$ gilt: $\varphi[M] = M$.*

Beweis. Da $L : K$ galoissch ist, ist $L : K$ auch separabel (Satz 1.16). Mit $L : K$ ist aber auch $M : K$ separabel. Zusammen mit Satz 1.16 zeigt das (i).

Da $M : K$ separabel ist, existiert nach dem Satz vom primitiven Element ein $\vartheta \in M$ mit $M = K(\vartheta)$ (Satz 31.2, Einführung in die Algebra und Zahlentheorie). Ein beliebiges Element $a \in M$ hat nun die Form $a = c_0 + c_1\vartheta + \cdots + c_{n-1}\vartheta^{n-1}$ mit Koeffizienten $c_i \in K$ (Satz 27.3, Einführung in die Algebra und Zahlentheorie).

Angenommen $M : K$ ist normal. Dann liegen alle Nullstellen von $\mathrm{Irr}(\vartheta, K)$ in M (siehe Definition 32.1, Einführung in die Algebra und Zahlentheorie). Sei nun $\varphi \in \mathrm{Gal}(L : K)$. φ bildet ϑ wieder auf eine Nullstelle von $\mathrm{Irr}(\vartheta, K)$ ab, also ist $\varphi(a) \in M$. Es folgt $\varphi[M] \subseteq M$. Da aber auch φ^{-1} ein Element von $\mathrm{Gal}(L : K)$ ist, gilt $\varphi^{-1}[M] \subseteq M$ und somit $\varphi[M] = M$.

Sei nun $\varphi[M] = M$ für alle $\varphi \in \mathrm{Gal}(L : K)$. Es genügt zu zeigen, daß M der Zerfällungskörper eines Polynoms $f \in K[X]$ ist (Satz 32.1, Einführung in die Algebra und Zahlentheorie).

Setze

$$f := \prod_{\varphi \in \mathrm{Gal}(L:K)} (X - \varphi(\vartheta)).$$

Nach Voraussetzung liegen alle Nullstellen von f, nämlich die $\varphi(\vartheta)$, in M. M ist also Zerfällungskörper von f. Es bleibt $f \in K[X]$ zu zeigen.

Wie im Beweis von der Richtung (i)⇒(iii) von Satz 1.16 sieht man, daß die Koeffizienten von f in $\mathrm{Fix}_L(\mathrm{Gal}(L : K))$ liegen. Da $L : K$ endlich und galoissch ist, ist $\mathrm{Fix}_L(\mathrm{Gal}(L : K)) = K$ und somit $f \in K[X]$. □

1.3. **Hauptsätze der Galoistheorie.** Sei $L : K$ endliche, galoissche Körpererweiterung. Das Ziel dieses Abschnittes ist es, eine bijektive Korrespondenz zwischen den Untergruppen der Galoisgruppe von $L : K$ und den Zwischenkörpern von $L : K$ herzuleiten.

Es sei $\mathcal{Z} := \{Z : Z \text{ ist Körper und es gilt } K \leq Z \leq L\}$ die Menge der *Zwischenkörper* von $L : K$ und $\mathcal{U} := \{U : U \text{ ist Untergruppe von } \mathrm{Gal}(L : K)\}$ die Menge der Untergruppen der Galoisgruppe von $L : K$.

Weiter sei $\Phi_{\mathcal{Z},\mathcal{U}} : \mathcal{Z} \to \mathcal{U}$ die Abbildung, die jedem $Z \in \mathcal{Z}$ die Gruppe $\mathrm{Gal}(L : Z)$ zuordnet und $\Phi_{\mathcal{U},\mathcal{Z}} : \mathcal{U} \to \mathcal{Z}$ die Abbildung, die jeder Gruppe $U \in \mathcal{U}$ den Körper $\mathrm{Fix}_L(U)$ zuordnet.

Das Hauptergebnis des nächsten Satzes sagt, daß $\Phi_{\mathcal{Z},\mathcal{U}}$ und $\Phi_{\mathcal{U},\mathcal{Z}}$ bijektiv und invers zueinander sind. Einen Überblick gibt das folgende Schema.

$$\begin{array}{ccc} L & \longmapsto & \{\mathrm{id}_L\} \\ \uparrow & \mapsto & \downarrow \\ Z = \mathrm{Fix}_L(U) & \overset{\Phi_{\mathcal{Z},\mathcal{U}}}{\underset{\Phi_{\mathcal{U},\mathcal{Z}}}{\rightleftarrows}} & U = \mathrm{Gal}(L : Z) \\ \uparrow & \mapsto & \downarrow \\ K & \longmapsto & \mathrm{Gal}(L : K) \end{array}$$

Satz 1.19 (Hauptsatz der Galoistheorie)**.** *Mit den obigen Voraussetzungen und Bezeichnungen gilt:*

(i) *$\Phi_{\mathcal{Z},\mathcal{U}}$ und $\Phi_{\mathcal{U},\mathcal{Z}}$ sind bijektiv und zueinander invers. Mit anderen Worten, für jeden Zwischenkörper Z von $L : K$ ist $Z = \mathrm{Fix}_L(\mathrm{Gal}(L : K))$ und für jede Untergruppe U von $\mathrm{Gal}(L : K)$ ist $U = \mathrm{Gal}(L : \mathrm{Fix}_L(U))$.*

(ii) *Sind U_1 und U_2 Untergruppen von $\mathrm{Gal}(L : K)$ und F_1 und F_2 die zugehörigen Fixpunktkörper, so gilt*

$$U_1 \leq U_2 \Leftrightarrow F_2 \leq F_1.$$

D.h., $\Phi_{\mathcal{Z},\mathcal{U}}$ und $\Phi_{\mathcal{U},\mathcal{Z}}$ sind ordnungsumkehrend (bezüglich $\leq$).

(iii) *Sei U eine Untergruppe von $\mathrm{Gal}(L : K)$ und F der zugehörige Fixpunktkörper. Dann gilt*

$$[L : F] = |U| \text{ sowie } [F : K] = [\mathrm{Gal}(L : K) : U],$$

wobei $[\mathrm{Gal}(L : K) : U]$ der Index von U in $\mathrm{Gal}(L : K)$ ist.

(iv) *Sei U eine Untergruppe von $\mathrm{Gal}(L : K)$, F der zugehörige Fixpunktkörper und $\varphi \in \mathrm{Gal}(L : K)$. Dann ist*

$$\mathrm{Fix}_L(\varphi U \varphi^{-1}) = \varphi[F].$$

(v) *Sei U eine Untergruppe von $\mathrm{Gal}(L : K)$ und F der zugehörige Fixpunktkörper. Dann gilt:*

a) *U ist genau dann Normalteiler in $\mathrm{Gal}(L : K)$, wenn $F : K$ galoissch ist.*

b) *Falls U Normalteiler in $\mathrm{Gal}(L : K)$ ist, so gilt*

$$\mathrm{Gal}(F : K) \cong \mathrm{Gal}(L : K)/\mathrm{Gal}(L : F).$$

Beweis. (i) Wir zeigen

$$\Phi_{\mathcal{U},\mathcal{Z}} \circ \Phi_{\mathcal{Z},\mathcal{U}} = \mathrm{id}_{\mathcal{Z}}$$

und

$$\Phi_{\mathcal{Z},\mathcal{U}} \circ \Phi_{\mathcal{U},\mathcal{Z}} = \mathrm{id}_{\mathcal{U}}\,.$$

Sei $Z \in \mathcal{Z}$, also $K \leq Z \leq L$. Nach Folgerung 1.17 ist $L : Z$ galoissch. Also gilt

$$Z = \mathrm{Fix}_L(\mathrm{Gal}(L : Z)) = (\Phi_{\mathcal{U},\mathcal{Z}} \circ \Phi_{\mathcal{Z},\mathcal{U}})(Z).$$

Sei nun $U \in \mathcal{U}$, also $U \leq \mathrm{Gal}(L : K)$. Nach Folgerung 1.17 ist $L : \mathrm{Fix}_L(U)$ galoissch. Es gilt also $|\mathrm{Gal}(L : \mathrm{Fix}_L(U))| = [L : \mathrm{Fix}_L(U)]$ nach Satz 1.16. Offenbar ist $U \leq \mathrm{Gal}(L : \mathrm{Fix}_L(U))$. Nach Satz 1.12 ist $|U| = [L : \mathrm{Fix}_L(U)]$. Da $L : K$ und damit auch $\mathrm{Gal}(L : \mathrm{Fix}_L(U))$ endlich ist, folgt

$$U = \mathrm{Gal}(L : \mathrm{Fix}_L(U)) = (\Phi_{\mathcal{Z},\mathcal{U}} \circ \Phi_{\mathcal{U},\mathcal{Z}})(U).$$

(ii) folgt unmittelbar aus den Definitionen.

(iii) Wie im Beweis von (i) ist $L : F$ galoissch und es gilt $U = \mathrm{Gal}(L : F)$. Nach Satz 1.16 ist $|U| = [L : F]$. Nach der Körpergradformel ist $[L : K] = [L : F] \cdot [F : K]$. Zusammen mit $[L : K] = |\mathrm{Gal}(L : K)| = |U| \cdot [\mathrm{Gal}(L : K) : U]$ folgt $[F : K] = [\mathrm{Gal}(L : K) : U]$.

(iv) Sei $a \in F$ und $\psi \in U$. Wegen $\psi(a) = a$ ist $(\varphi \circ \psi \circ \varphi^{-1})(\varphi(a)) = \varphi(a)$. Es folgt $\varphi(a) \in \mathrm{Fix}_L(\varphi U \varphi^{-1})$. Das zeigt $\varphi[F] \subseteq \mathrm{Fix}_L(\varphi U \varphi^{-1})$.

Das gleiche Argument liefert

$$\varphi^{-1}[\mathrm{Fix}_L(\varphi U \varphi^{-1})] \subseteq \mathrm{Fix}_L(\varphi^{-1}(\varphi U \varphi^{-1})(\varphi^{-1})^{-1}) = \mathrm{Fix}_L(U) = F.$$

Daraus folgt $\mathrm{Fix}_L(\varphi U \varphi^{-1}) \subseteq \varphi[F]$.

(v) Für a) sei U Normalteiler von $\mathrm{Gal}(L : K)$. Für alle $\varphi \in \mathrm{Gal}(L : K)$ ist also $\varphi U \varphi^{-1} = U$. Wegen (iv) gilt nun $\varphi[F] = F$ für alle $\varphi \in \mathrm{Gal}(L : K)$. Aus Satz 1.18 folgt, daß $F : K$ galoissch ist.

Ist umgekehrt $F : K$ galoissch, so ist wegen Satz 1.18 $\varphi[F] = F$ für alle $\varphi \in \mathrm{Gal}(L : K)$. Wegen (iv) gilt also $F = \mathrm{Fix}_L(\varphi U \varphi^{-1})$ für alle $\varphi \in \mathrm{Gal}(L : K)$. Da $\Phi_{\mathcal{U},\mathcal{Z}}$ nach (i) bijektiv ist, impliziert das $\varphi U \varphi^{-1} = U$ für alle $\varphi \in \mathrm{Gal}(L : K)$. U ist also Normalteiler von $\mathrm{Gal}(L : K)$.

Für b) sei U Normalteiler von $\mathrm{Gal}(L : K)$. Sei $\varphi \in \mathrm{Gal}(L : K)$. Wie im Beweis von a) ist $\varphi[F] = F$. Damit gilt $\varphi \restriction F \in \mathrm{Gal}(F : K)$. Die Abbildung $h : \mathrm{Gal}(L : K) \to \mathrm{Gal}(F : K); \varphi \mapsto \varphi \restriction F$ ist ein Homomorphismus, dessen Kern genau $\mathrm{Gal}(L : F)$ ist. Nach dem Homomorphiesatz für Gruppen ist das Bild von h isomorph zu $\mathrm{Gal}(L : K)/\mathrm{Gal}(L : F)$. $\mathrm{Gal}(L : K)/\mathrm{Gal}(L : F)$ hat die Ordnung $[L : K]/[L : F] = [F : K]$. Nach a) ist $F : K$ galoissch. Damit ist die Ordnung von $\mathrm{Gal}(F : K)$ ebenfalls $[F : K]$ (nach Satz 1.16). h ist also surjektiv. Es folgt $\mathrm{Gal}(L : K)/\mathrm{Gal}(L : F) \cong \mathrm{Gal}(F : K)$.

□

Satz 1.20. *Sei $L : K$ eine endliche, galoissche Körpererweiterung, U_1, U_2 Untergruppen von $\mathrm{Gal}(L : K)$ und F_1, F_2 die zugehörigen Fixpunktkörper. Weiter sei U die kleinste Unetergruppe von $\mathrm{Gal}(L : K)$, die U_1 und U_2 umfaßt, also die von U_1 und U_2 erzeugte Untergruppe. Schließlich sei F der von F_1 und F_2 erzeugte Unterkörper von L. Dann gilt:*

(i) $\mathrm{Fix}_L(U) = F_1 \cap F_2$
(ii) $\mathrm{Fix}_L(U_1 \cap U_2) = F$

Beweis. (i) Die Elemente von U sind endliche Produkte von Elementen von U_1 und U_2. Also lassen die Elemente von U die Elemente von $F_1 \cap F_2$ punktweise fest. Damit gilt $F_1 \cap F_2 \leq \mathrm{Fix}_L(U)$. Aus $U_1, U_2 \leq U$ folgt aber $\mathrm{Fix}_L(U) \leq F_1, F_2$ nach Satz 1.19 (ii). Das zeigt die Behauptung.

(ii) Wegen $U_1 \cap U_2 \leq U_1, U_2$ gilt $F_1, F_2 \leq \mathrm{Fix}_L(U_1 \cap U_2)$ (Satz 1.19 (ii)) und damit auch $F \leq \mathrm{Fix}_L(U_1 \cap U_2)$. Da $L : F$ galoissch ist, gilt $F = \mathrm{Fix}_L(\mathrm{Gal}(L : F))$. Außerdem ist $\mathrm{Gal}(L : F) \leq U_1, U_2$ (Satz 1.19 (ii)), also $\mathrm{Gal}(L : F) \leq U_1 \cap U_2$. Nochmalige Anwendung von Satz 1.19 (ii) liefert nun $\mathrm{Fix}_L(U_1 \cap U_2) \leq F$. □

Sind E und F Unterkörper eines Körpers L, so wird mit $E \cdot F$ der kleinste Unterkörper von L bezeichnet, der E und F umfaßt. Man beachte, daß $E \cdot F$ üblicherweise mehr Elemente enthält als nur die Produkte von Elementen von E und F.

Satz 1.21 (Translationssatz)**.** *Sei $F : K$ eine beliebige Körpererweiterung und $E : K$ eine endliche, galoissche Erweiterung. Dann sind auch $E : E \cap F$ und $E \cdot F : F$ endlich und galoissch und es gilt*

$$\mathrm{Gal}(E \cdot F : F) \cong \mathrm{Gal}(E : E \cap F).$$

Beweis. $E \cap F$ ist ein Zwischenkörper von $E : K$. Nach Folgerung 1.17 ist mit $E : K$ auch $E : E \cap F$ endlich und galoissch. Nach Satz 1.16 ist E Zerfällungskörper eines separablen $f \in K[X]$. Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f in E, also $E = K[\alpha_1, \ldots, \alpha_n]$. Wegen $K \leq F$ gilt $E \cdot F = F[\alpha_1, \ldots, \alpha_n]$. $E \cdot F$ ist also der Zerfällungskörper von f über F, und damit ist $E \cdot F : F$ endlich und galoissch (Satz 1.16).

Sei $\varphi \in \mathrm{Gal}(E \cdot F : F)$. Wegen $K \leq F$ gilt $\varphi \restriction K = \mathrm{id}_K$. Da $E : K$ normal und algebraisch ist, gilt $\varphi[E] = E$, denn für jedes $a \in E$ ist $\varphi(a)$ ja wieder eine Nulstelle von $\mathrm{Irr}(a, K)$, also ein Element von E. (Man erinnere sich an den Beweis von Satz 1.18 (ii).) Insbesondere ist $\varphi \restriction E$ ein Autmorphismus von E, der $E \cap F$ punktweise fest läßt.

Betrachte also die Abbildung

$$h : \mathrm{Gal}(E \cdot F : F) \to \mathrm{Gal}(E : E \cap F); \varphi \mapsto \varphi \restriction E.$$

h ist offenbar ein Homomorphismus. $\varphi \in \mathrm{Gal}(E \cdot F : F)$ liegt genau dann im Kern von h, wenn $\varphi \restriction E = \mathrm{id}_E$ ist. Da φ aber F punktweise festläßt und $E \cdot F$ von E und F erzeugt wird, ist φ genau dann die Identität auf E, wenn φ die Identität auf $E \cdot F$ ist. Der Kern von h besteht somit nur aus $\mathrm{id}_{E \cdot F}$. Also ist h injektiv.

Es bleibt zu zeigen, daß h surjektiv ist. Der Fixpunktkörper von $\mathrm{Gal}(E \cdot F : F)$ ist genau F. Damit ist der Fixpunktkörper von $h[\mathrm{Gal}(E \cdot F : F)]$ genau $F \cap E$. Nach Satz 1.19 kann das nur der Fall sein, wenn $h[\mathrm{Gal}(E \cdot F : F)] = \mathrm{Gal}(E : E \cap F)$ gilt, da $E : E \cap F$ ja galoissch ist. h ist also surjektiv. □

Satz 1.22. *$L : K$ sei eine Körpererweiterung, und L_1 und L_2 seien Zwischenkörper dieser Erweiterung. Die Erweiterungen $L_1 : K$ und $L_2 : K$ seien endlich und galoissch, und es gelte $L_1 \cap L_2 = K$. Dann gilt:*

(i) *$L_1 \cdot L_2 : K$ ist endlich und galoissch.*
(ii) $\mathrm{Gal}(L_1 \cdot L_2 : K) \cong \mathrm{Gal}(L_1 : K) \times \mathrm{Gal}(L_2 : K)$

Beweis. (i) Da $L_1 : K$ und $L_2 : K$ endlich und galoissch sind, existieren separable Polynome $f_1, f_2 \in K[X]$, so daß L_i der Zerfällungskörper von f_i ist für $i = 1, 2$ (Satz 1.16). Offenbar ist $L_1 \cdot L_2$ der Zerfällungskörper (über K) von $f_1 \cdot f_2$. Nach Satz 1.16 ist $L_1 \cdot L_2 : K$ damit endlich und galoissch.

Für (ii) betrachte die Abbildung

$$h : \mathrm{Gal}(L_1 \cdot L_2 : K) \to \mathrm{Gal}(L_1 : K) \times \mathrm{Gal}(L_2, K); \varphi \mapsto (\varphi \restriction L_1, \varphi \restriction L_2).$$

Wie im Beweis von Satz 1.21 sieht man, daß für alle $\varphi \in \mathrm{Gal}(L_1 \cdot L_2 : K)$ und $i = 1, 2$ die Einschränkung $\varphi \restriction L_i$ in der Tat ein Element von $\mathrm{Gal}(L_i : K)$ ist.

Offenbar ist h ein Homomorphismus. Weiterhin ist h injektiv. Ist nämlich $\varphi \restriction L_1 = \mathrm{id}_{L_1}$ und $\varphi \restriction L_2 = \mathrm{id}_{L_2}$, so ist φ selbst die Identität auf $L_1 \cdot L_2$, da $L_1 \cdot L_2$ ja von L_1 und L_2 erzeugt wird.

Es bleibt zu zeigen, daß h surjektiv ist. Da $L_1 \cdot L_2 : K$ endlich und galoissch ist, gilt nach Satz 1.16

$$|\mathrm{Gal}(L_1 \cdot L_2 : K)| = [L_1 \cdot L_2 : K] = [L_1 \cdot L_2 : L_2] \cdot [L_2 : K].$$

Da nach Satz 1.21 auch $L_1 \cdot L_2 : L_2$ endlich und galoissch ist und $\mathrm{Gal}(L_1 \cdot L_2 : L_2) \cong \mathrm{Gal}(L_1 : K)$ gilt, ist

$$\begin{aligned}[L_1 \cdot L_2 : L_2] \cdot [L_2 : K] &= |\mathrm{Gal}(L_1 \cdot L_2 : L_2)| \cdot |\mathrm{Gal}(L_2 : K)| \\ &= |\mathrm{Gal}(L_1 : K)| \cdot |\mathrm{Gal}(L_2 : K)| = |\mathrm{Gal}(L_1 : K) \times \mathrm{Gal}(L_2 : K)| .\end{aligned}$$

Damit ist h surjektiv. □

1.4. **Auflösbare Gruppen.** Auflösbare Gruppen sind ein wichtiges Hilfsmittel beim Studium der Auflösbarkeit von Polynomgleichungen der Form $f(x) = 0$ durch "Wurzelausdrücke".

Definition 1.23. Eine Gruppe G heißt genau dann *auflösbar*, wenn eine (endliche) Folge $N_0, \ldots, N_k$ von Untergruppen von G existiert, so daß gilt:

(i) $\{e\} = N_k \leq \cdots \leq N_0 = G$
(ii) Für jedes $i < k$ ist N_{i+1} Normalteiler in N_i mit abelschem Quotienten N_i/N_{i+1}.

Jede abelsche Gruppe G ist auflösbar. ($N_0 = G$, $N_1 = \{e\}$.) Es sind aber auch viele nicht-abelsche Gruppen auflösbar.

Lemma 1.24. *Jedes homomorphe Bild einer auflösbaren Gruppe ist auflösbar.*

Beweis. Sei G auflösbar, z.B. $G = N_0 \geq \cdots \geq N_k = \{e\}$, wobei die N_i die Auflösbarkeit von G bezeugen. Sei H eine weitere Gruppe und $\varphi : G \to H$ ein Epimorphismus. Man erinnere sich, daß Epimorphismen Normalteiler auf Normalteiler abbilden. Daraus folgt, daß für alle $i < k$ die Gruppe $\varphi[N_{i+1}]$ ein Normalteiler von $\varphi[N_i]$ ist. Offenbar ist $\varphi[N_k]$ einelementig und $\varphi[N_0] = H$.

Um nachzuweisen, daß H auflösbar ist, genügt es nun zu zeigen, daß die Quotienten $\varphi[N_i]/\varphi[N_{i+1}]$ abelsch sind. Sei $i < k$. Betrachte die Abbildung

$$\psi : N_i/N_{i+1} \to \varphi[N_i]/\varphi[N_{i+1}]; aN_i \mapsto \varphi(a)\varphi[N_i].$$

Es ist leicht zu sehen, daß ψ wohldefiniert ist. Außerdem ist ψ ein surjektiver Homomorphismus. Nach Satz 6.1 (iv) aus der Einführung in die Algebra und Zahlentheorie ist jedes homomorphe Bild einer abelschen Gruppe abelsch. Damit ist $\varphi[N_i]/\varphi[N_{i+1}]$ abelsch. □

Lemma 1.25. *Sei G eine Gruppe und N ein Normalteiler von G. Dann ist G auflösbar, falls N und G/N auflösbar sind.*

Beweis. Sei $G/N = M_0 \geq \cdots \geq M_k = \{e_{G/N}\}$, wobei die M_i die Auflösbarkeit von G/N bezeugen, und $N = N_0 \geq \cdots \geq N_l = \{e_N\}$, wobei die N_j die Auflösbarkeit von N bezeugen. $\varphi : G \to G/N; g \mapsto gN$ sei die Quotientenabbildung. Es ist leicht nachzurechnen, daß die Folge

$$G = \varphi^{-1}[M_0] \geq \cdots \geq \varphi^{-1}[M_k] = N = N_0 \geq \cdots \geq N_l$$

die Auflösbarkeit von G bezeugt. Man beachte nämlich, daß aus den Homomorphiesätzen für Gruppen folgt, daß für jedes $i < k$ der Quotient $\varphi^{-1}[M_i]/\varphi^{-1}[M_{i+1}]$ isomorph zu M_i/M_{i+1} ist. □

Lemma 1.26. *Sei G eine p-Gruppe, also $|G| = p^n$ für eine Primzahl p und ein $n > 0$. Dann ist G auflösbar.*

Beweis. Wir beweisen die Aussage durch induktion über n. Die Aussage gilt für $n = 1$, da Gruppen von Primzahlordnung zyklisch und damit abelsch (also auch auflösbar) sind.

Sei $n > 1$. Setze $Z := \{x \in G : \forall g \in G(xg = gx)\}$. Z ist das *Zentrum* von G. Es folgt unmittelbar aus der Definition, daß Z ein abelscher Normalteiler von G ist. Außerdem ist $Z \neq \{e\}$. Z besteht nämlich genau aus den

Elementen von G, die nur zu sich selbst konjugiert sind, wie zum Beispiel das neutrale Element.

Für jedes $g \in G$ ist die Anzahl der zu g konjugierten Elemente (einschließlich g selbst) ein Teiler von $|G|$. (Siehe Einführung in die Algebra und Zahlentheorie, Satz 8.1.) Falls die Anzahl der zu g konjugierten Elemente größer als 1 ist, ist sie also ein Vielfaches von p. Da $|G|$ ein Vielfaches von p ist, muß es mehr als ein Element geben, daß nur zu sich selbst konjugiert ist. Es folgt, daß Z mehr als ein Element hat.

Da Z abelsch ist, ist Z auflösbar. $|G/Z|$ ist eine p-Potenz, deren Exponent echt kleiner als n ist. Nach Induktionvoraussetzung ist G/Z also auflösbar. Nach Lemma 1.25 ist G auflösbar. □

Bemerkung 1.27. S_n sei die symmetrische Gruppe über n Elementen, also die Gruppe der Permutationen einer n-elementigen Menge. A_n sei die Untergruppe der *geraden* Permutationen, also der Produkte einer geraden Anzahl von Transpositionen. A_n ist ein Normalteiler von S_n vom Index 2.

S_2 ist abelsch, also auflösbar. A_3 ist nicht-trivialer Normalteiler von S_3. A_3 hat die Ordnung 3, ist also auflösbar. S_3/A_3 hat die Ordnung 2 und ist damit abelsch. Also ist S_3 auflösbar.

S_4 hat den Normalteiler A_4, und A_4 hat einen Normalteiler N der Ordnung 4. N ist als p-Gruppe auflösbar. Die Quotienten S_4/A_4 und A_4/N haben die Ordnung 2, beziehungsweise 3, sind also abelsch. Damit ist S_4 auflösbar.

Etwas schwieriger zu zeigen ist

Satz 1.28. *S_n ist genau dann auflösbar, wenn $n \leq 4$ gilt.*

Dieser Satz folgt unmittelbar aus den beiden folgenden Lemmata zusammen mit der obigen Bemerkung.

Lemma 1.29. *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*

Beweis. Sei G auflösbar und $U \leq G$. $G = N_0 \geq \cdots \geq N_k = \{e\}$ bezeuge die Auflösbarkeit von G. Für $i \leq k$ setze $M_i := U \cap N_i$. Für jedes $i \leq k$ ist M_{i+1} Normalteiler in M_i. Der Quotient M_i/M_{i+1} ist isomorph zu einer Untergruppe von N_i/N_{i+1}, nämlich zu $\{uN_{i+1} : u \in U\}$, also abelsch. Die Folge der M_i bezeugt also die Auflösbarkeit von U. □

Lemma 1.30. *Die alternierende Gruppe A_n besitzt für $n \geq 5$ keinen Normalteiler $N \neq A_n$, für den A_n/N abelsch ist.*

Beweis. Sei $n \geq 5$. Angenommen N ist Normalteiler von A_n mit abelschem Quotienten A_n/N. Sei (abc) ein beliebiger Zyklus der Länge 3. Setze $x := (abd)$ und $y := (ace)$. Verschiedene Buchstaben stehen hierbei für verschiedene Elemente der Menge auf der S_n operiert. Dann ist $xyx^{-1}y^{-1} = (abc)$. Da A_n/N abelsch ist, ist $xyx^{-1}y^{-1} \in N$. Also ist $(abc) \in N$. N enthält also jeden Zyklus der Länge 3.

Um nun $N = A_n$ zu zeigen, genügt es zu beweisen, daß A_n von den Zyklen der Länge 3 erzeugt wird. Offenbar wird A_n von Elementen der Form $\sigma \circ \tau$, σ und τ Transpositionen, erzeugt. Sind σ und τ nicht disjunkt, so ist $\sigma \circ \tau$ ein Zyklus der Länge 3 oder die Identität. Seien nun σ und τ disjunkte Transpositionen, also zum Beispiel $\sigma = (ab)$ und $\tau = (cd)$.

Dann gilt $(ab) \circ (cd) = (cbd) \circ (acb)$. $\sigma \circ \tau$ ist also Produkt von Zyklen der Länge 3. Damit erzeugen die Zyklen der Länge 3 die Gruppe A_n und es gilt $N = A_n$. □

Beweis von Satz 1.28. Nach Bemerkung 1.27 ist S_n auflösbar für $n \leq 4$. Sei nun $n \geq 5$. Dann hat S_n eine Untergruppe, die zu S_5 isomorph ist. Damit hat S_n auch eine Untergruppe, die zu A_5 isomorph ist. A_5 ist aber nicht auflösbar, da A_5 nach Lemma 1.30 keinen nicht-trivialen Normalteiler mit abelschem Quotienten besitzt. Nach Lemma 1.29 ist S_n also nicht auflösbar. □

Definition und Bemerkung 1.31. Sei G eine Gruppe und N ein Normalteiler von G. Die von $\{xyx^{-1}y^{-1} : x, y \in G\}$ erzeugte Untergruppe $K(G)$ von G, die *Kommutatoruntergruppe* von G, ist ein Normalteiler von G. G/N ist genau dann abelsch, wenn $K(G)$ eine Teilmenge von N ist.

Beweis. Die Elemente von $K(G)$ sind endliche Produkte von Elementen der Form $xyx^{-1}y^{-1}$. Um zu zeigen, daß $K(G)$ ein Normalteiler von G ist, genügt es nachzurechnen, daß die Elemente der Form $xyx^{-1}y^{-1}$ unter Konjugation abgeschlossen sind. Seien $x, y, z \in G$. Dann ist

$$z(xyx^{-1}y^{-1})z^{-1} = zxz^{-1}zyz^{-1}(zxz^{-1})^{-1}(zyz^{-}1)^{-1}.$$

Das zeigt, daß $K(G)$ Normalteiler ist.

G/N ist genau dann abelsch, wenn für alle $x, y \in G$ gilt: $xyN = yxN$. Das gilt aber genau dann, wenn für alle $x, y \in G$ gilt: $xyx^{-1}y^{-1} \in N$. Letzteres ist äquivalent dazu, daß die von den Elementen der Form $xyx^{-1}y^{-1}$ erzeugte Untergruppe von G, nämlich $K(G)$, eine Untergruppe von N ist. □

1.5. **Auflösbarkeit von Polynomen durch Radikale.** In diesem Abschnitt wird die Frage untersucht, wann sich die Nullstellen eines Polynoms durch "Wurzelausdrücke" darstellen lassen. Für quadratische Polynome ist das möglich mit den bekannten Formeln (p,q-Formel für normierte Polynome und a,b,c-Formel im allgemeinen Fall).

Für kubische Polynome gibt es die Formel von Cardano, und seit Mitte des 16. Jahrhunderts kennt man auch Formeln für Polynome 4. Grades. 1826 bewies Abel, daß es entsprechende Formeln für Polynome höheren Grades nicht geben kann.

Mit Hilfe der Galoistheorie werden wir im folgenden diejenigen Polynome charakterisieren, für die eine entsprechende Formel existiert. Wir beschränken uns dabei auf Körper der Charakteristik 0.

Zunächst eine Vorbemerkung über Einheitswurzeln.

Bemerkung 1.32. Sei K ein Körper der Charakteristik 0. Dann ist jedes Polynom $f \in K[X]$ separabel über K (Bemerkung 32.4, Einführung in die Algebra und Zahlentheorie). Sei $n > 0$ und E der Zerfällungskörper von $X^n - 1$ über K. Dann ist $E : K$ endlich und galoissch.

$X^n - 1$ besitzt in E nur einfache Nullstellen, da $(X^n - 1)' = n \cdot X^{n-1}$ nur die Nullstelle 0 hat. (Siehe Bemerkung 16.5, Einführung in die Algebra und Zahlentheorie.) Die Nullstellen von $X^n - 1$ bilden wegen

$$a^n = 1 \wedge b^n = 1 \Rightarrow (ab)^n = 1$$

und

$$a^n = 1 \Rightarrow (a^{-1})^n = (a^n)^{-1} = 1$$

eine Gruppe E_n bezüglich der Multiplikation. E_n ist zyklisch und hat die Ordnung n. (Man erinnere sich, daß nach Satz 30.2, Einführung in die Algebra und Zahlentheorie, jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist.)

Die Elemente von E_n heißen *n-te Einheitswurzeln.* Ein erzeugendes Element ζ von E_n heißt *primitive* n-te Einheitswurzel. Es gilt $E = K(\zeta)$.

$\mathrm{Gal}(E : K)$ ist abelsch. Sei nämlich ζ primitive n-te Einheitswurzel. Jedes $\varphi \in \mathrm{Gal}(E : K)$ ist dann festgelegt durch $\varphi(\zeta)$. Falls $\varphi \in \mathrm{Gal}(E : K)$ die primitive Einheitswurzel ζ auf $\zeta^i \in E_n$ abbildet, so bezeichne φ mit φ_i. Jedes $\varphi \in \mathrm{Gal}(E : K)$ hat die Form φ_i. Es gilt

$$(\varphi_i \circ \varphi_j)(\zeta) = \zeta^{i \cdot j} = (\varphi_j \circ \varphi_i)(\zeta).$$

Satz 1.33. *Sei K ein Körper der Charakteristik 0, der alle n-ten Einheitswurzeln enthält. (D.h., $X^n - 1$ zerfällt über K in Linearfaktoren.) Dann gilt:*

(i) *Sei b eine Nullstelle von $X^n - a \in K[X]$ in einem Erweiterungskörper von K. Dann ist $K(b)$ endlich und galoissch und $\mathrm{Gal}(K(b) : K)$ ist zyklisch.*

(ii) *Sei $L : K$ endlich und galoissch, so daß $\mathrm{Gal}(L : K)$ zyklisch ist mit Ordnung n. Dann existiert $b \in L$ mit $L = K(b)$, wobei b Nullstelle eines Polynoms $X^n - a \in K[X]$ ist, also n-te Wurzel eines Elementes von K.*

Beweis. (i) Sei ζ primitive n-te Einheitswurzel in K, also

$$E_n = \{1, \zeta, \ldots, \zeta^{n-1}\}.$$

Die Nullstellen von $X^n - a$ sind dann $b, b\zeta, \ldots, b\zeta^{n-1}$. $K(b)$ ist also der Zerfällungskörper von $X^n - a$ über K. Damit ist $K(b) : K$ endlich und galoissch.

$\varphi \in \mathrm{Gal}(K(b) : K)$ ist eindeutig bestimmt durch $\varphi(b)$; und $\varphi(b)$ hat die Form $b\zeta^i$. Bezeichne $\varphi \in \mathrm{Gal}(K(b) : K)$ mit φ_i, falls $\varphi(b) = b\zeta^i$ gilt. Definiere $h : \mathrm{Gal}(K(b) : K) \to \mathbb{Z}_n$ durch $h(\varphi_i) := i + n\mathbb{Z}$.

Da für jedes $\varphi \in \mathrm{Gal}(K(b) : K)$ die Restklasse $i + n\mathbb{Z}$ durch $\varphi(b) = b\zeta^i$ eindeutig bestimmt ist, ist h wohldefiniert. Außerdem ist h injektiv. Wegen $(\varphi_i \circ \varphi_j)(b) = b\zeta^{i+j} = \varphi_{i+j}(b)$ ist h ein Gruppenhomomorphismus. Nach dem Homomorphiesatz für Gruppen ist $\mathrm{Gal}(K(b) : K)$ also isomorph zu einer Untergruppe von $\mathbb{Z}_n$ und damit zyklisch.

(ii) Sei $\mathrm{Gal}(L : K) = \{\mathrm{id}, \varphi, \ldots, \varphi^{n-1}\}$. Nach Folgerung 1.3 sind die Elemente von $\mathrm{Gal}(L : K)$ linear unabhängig als Elemente des L-Vektorraumes $\mathrm{Abb}(L, L)$. Für jede n-te Einheitswurzel ζ ist also

$$\psi := \mathrm{id} + \zeta\varphi + \cdots + \zeta^{n-1}\varphi^{n-1}$$

verschieden von der Nullabbildung. Also existiert ein $c \in L$ mit $b := \psi(c) \neq 0$. ($\mathrm{id} + \zeta\varphi + \cdots + \zeta^{n-1}\varphi^{n-1}$ heißt die *Lagrangesche Resolvente*.)

Wegen $\varphi^n = \mathrm{id}$ und $\zeta^n = 1$ gilt

$$\varphi(b) = \varphi(c) + \zeta\varphi^2(c) + \cdots + \zeta^{n-1}\varphi^n(c) = \\ \zeta^{-1}(\zeta\varphi(c) + \cdots + \zeta^{n-1}\varphi^{n-1}(c) + c) = \zeta^{-1}b.$$

Also ist $\varphi(b^n) = \zeta^{-n}b^n = b^n$. Damit liegt b^n im Fixpunktkörper von $\mathrm{Gal}(L : K)$, d.h., $b^n \in K$.

Nach (i) ist $K(b) : K$ endlich und galoissch. Wir zeigen: ist ζ primitive n-te Einheitswurzel, so gilt $L = K(b)$.

Klar ist $K \leq K(b) \leq L$. Aufgrund der Voraussetzungen des Satzes gilt $[L : K] = n$. Es genügt daher $[K(b) : K] \geq n$ zu zeigen. Für $i \in \{0, \ldots, n-1\}$ gilt $\varphi^i(b) = \zeta^{-i}b$. Andereseits ist $\varphi^i(b)$ Nullstelle von $\mathrm{Irr}(b, K)$. Also hat $\mathrm{Irr}(b, K)$ mindestens die n Nullstellen $\zeta^{-i}b$, $i \in \{0, \ldots, n-1\}$. Es folgt $[K(b) : K] \geq n$. □

Definition 1.34. Sei $E : K$ eine Körpererweiterung.

(i) $E : K$ heißt *reine Radikalerweiterung*, falls E die Form $K(b)$ hat, wobei b Nullstelle eines Polynoms $X^n - a$ mit $a \in K$ ist (d.h., falls L aus K durch Adjunktion einer n-ten Wurzel eines Elementes von K entsteht).

(ii) $E : K$ heißt *Radikalerweiterung*, falls eine endliche Körperkette $K = K_0 \leq K_1 \leq \cdots \leq K_n = L$ existiert, in der jede Erweiterung $K_{i+1} : K_i$ eine reine Radikalerweiterung ist.

Definition 1.35. Sei K ein Körper und $f \in K[X]$. f heißt *über K durch Radikale auflösbar*, falls der Zerfällungskörper von f in einer Radikalerweiterung von K enthalten ist (d.h., falls sich die Nullstellen von f als "verschachtelte Wurzelausdrücke" von Elementen in K schreiben lassen).

Lemma 1.36. *Sei $f \in K[X]$ irreduzibel, E der Zerfällungskörper von f über K und $\alpha \in E$ Nullstelle von f. Dann ist f genau dann über K durch Radikale auflösbar, wenn $K(\alpha)$ in einer Radikalerweiterung von K enthalten ist.*

Beweis. Falls f durch Radikale auflösbar ist, so ist nach Definition E in einer Radikalerweiterung von K enthalten. Insbesondere ist $K(\alpha)$ als Teilmenge von E in einer Radikalerweiterung von K enthalten.

Sei nun $K(\alpha)$ in einer Radikalerweiterung von K enthalten. Wir zeigen, daß auch E in einer Radikalerweiterung von K enthalten ist.

Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f in E. O.B.d.A. sei $\alpha = \alpha_1$. Da f irreduzibel ist, gilt $K(\alpha) \cong K[X]/(f) \cong K(\alpha_i)$ für alle $i \in \{1, \ldots, n\}$. Also ist jedes $K(\alpha_i)$ in einer Radikalerweiterung von K enthalten. Eine Radikalerweiterung entsteht durch Adjunktion von Wurzeln. Adjungiert man alle Wurzeln, die man braucht, um die verschiedenen $K(\alpha_i)$ zu erzeugen, so erhält man eine Radikalerweiterung von K, die $K(\alpha_1, \ldots, \alpha_n)$ umfaßt. □

Satz 1.37. *Sei K ein Körper der Charakteristik 0 und $E : K$ endlich und galoissch. Dann ist E genau dann in einer Radikalerweiterung von K enthalten, wenn $\mathrm{Gal}(E : K)$ auflösbar ist.*

Aus diesem Satz ergibt sich sofort ein Kriterium für die Auflösbarkeit von Polynomen durch Radikale.

Folgerung 1.38. *Sei K ein Körper der Charakteristik 0. Dann ist $f \in K[X]$ genau dann durch Radikale auflösbar, wenn die Galoisgruppe des Zerfällungskörpers E von f über K auflösbar ist.*

Für den Beweis des Satzes stellen wir zunächst folgendes fest:

Lemma 1.39. *Falls G eine auflösbare Gruppe ist, so existieren ein $k \in \mathbb{N}$ und eine Folge $N_0, \ldots, N_k$ von Untergruppen von G, so daß gilt:*

(i) *$N_0 = G$ und $N_k = \{e\}$*
(ii) *Für alle $i \in \{0, \ldots, k-1\}$ ist N_{i+1} Normalteiler von N_i mit zyklischem Quotienten N_i/N_{i+1}.*

Beweis. $G = N_0 \geq \cdots \geq N_k = \{e\}$ bezeuge die Auflösbarkeit von G. So eine Folge $N_0, \ldots, N_k$ nennen wir eine *Auflösung von G*. Wir können annehmen, daß die N_i paarweise verschieden sind. Da wir nur endlichen Gruppen G betrachten, können wir außerdem annehmen, daß k maximal ist in dem Sinne, daß es keine längere Auflösung von G gibt, in der die auftretenden Untergruppen paarweise verschieden sind.

Wir zeigen, daß N_i/N_{i+1} für alle $i \in \{0, \ldots, k-1\}$ zyklisch ist. Angenommen für ein i ist das nicht der Fall.

Wähle ein $a \in N_i/N_{i+1}$, das von $e_{N_i/N_{i+1}}$ verschieden ist. Die von a in N_i/N_{i+1} erzeugte Untergruppe M ist ein Normalteiler, da N_i/N_{i+1} abelsch ist. Außerdem ist $M \neq N_i/N_{i+1}$, da N_i/N_{i+1} nicht zyklisch ist. Sei $h : N_i \to N_i/N_{i+1}$ die Quotientenabbildung. Dann ist $h^{-1}[M]$ ein Normalteiler von N_i, und N_{i+1} ist ein Normalteiler von $h^{-1}[M]$. Der Quotient $h^{-1}[M]/N_{i+1}$ ist eine Untergruppe von N_i/N_{i+1}, also abelsch. Der Quotient $N_i/h^{-1}[M]$ ist isomorph zu $(N_i/N_{i+1})/M$, also homomorphes Bild einer abelschen Gruppe und damit auch abelsch.

Insgesamt ist $N_0, \dots, N_i, h^{-1}[M], N_{i+1}, \dots, N_k$ eine Auflösung von G mit paarweise verschiedenen Untergruppen. Ein Widerspruch zur Maximalität von k. □

Beweis von Satz 1.37. Sei auflösbar und $G_0, \dots, G_k$ eine Auflösung der Galoisgruppe $\mathrm{Gal}(E : K)$. Nach Lemma 1.39 können wir annehmen, daß alle Quotienten G_i/G_{i+1} zyklisch sind.

Für jedes $i \in \{0, \dots, k\}$ sei K_i der Fixpunktkörper von G_i. Für alle $i \in \{0, \dots, k-1\}$ ist $K_{i+1} : K_i$ also endlich und galoissch mit zyklischer Galoisgruppe, z.B. mit der Ordnung n_i. Sei n das kleinste gemeinsame Vielfache der n_i und ζ primitive n-te Einheitswurzel.

Für jedes $i \in \{0, \dots, k\}$ sei $K_i^* := K_i(\zeta)$. Offenbar ist $K_0^* : K_0$ eine reine Radikalerweiterung. Für alle $i \in \{0, \dots, k-1\}$ ist $K_{i+1} : K_{i+1} \cap K_i^*$ galoissch. Wegen $K_i \leq K_{i+1} \cap K_i^*$ ist $\mathrm{Gal}(K_{i+1} : K_{i+1} \cap K_i^*)$ eine Untergruppe von $\mathrm{Gal}(K_{i+1} : K_i)$, also zyklisch.

Nach Satz 1.21 ist $\mathrm{Gal}(K_{i+1} : K_{i+1} \cap K_i^*)$ isomorph zu $\mathrm{Gal}(K_{i+1}^* : K_i^*)$. Nach Satz 1.33 (ii) ist $K_{i+1}^* : K_i^*$ eine reine Radikalerweiterung. Insgesamt ist $K_k^* : K$ also eine Radikalerweiterung. Offenbar gilt $E = K_k \leq K_k^*$.

Für die andere Richtung des Satzes sei $L : K$ eine Radikalerweiterung mit $E \leq L$. Da K die Charakteristik 0 hat, ist $L : K$ separabel. Da $L : K$ endlich ist, existiert nach dem Satz vom primitiven Element ein $\vartheta \in L$ mit $L = K(\vartheta)$. Nach Lemma 1.36 ist der Zerfällungskörper von $\mathrm{Irr}(\vartheta, K)$ eine Radikalerweiterung von K. Indem wir L eventuell vergrößern, können wir also annehmen, daß L bereits Zerfällungskörper eines Polynoms über K ist. Damit ist die Erweiterung $L : K$ galoissch.

$K = K_0 \leq \cdots \leq K_l = L$ sei eine Körperkette, so daß für jedes $i \in \{0, \dots, l-1\}$ die Erweiterung $K_{i+1} : K_i$ eine reine Radikalerweiterung ist, etwa $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ mit $a_i \in K_i$ und $n_i > 0$. Sei n das kleinste gemeinsame Vielfache der n_i und ζ primitive n-te Einheitswurzel über K.

Für jedes $i \in \{0, \dots, l\}$ sei $K_i^* := K_i(\zeta)$. Nach der Bemerkung über n-te Einheitswurzeln ist $K_0^* : K_0$ galoissch mit abelscher Galoisgruppe $\mathrm{Gal}(K_0^* : K_0)$. Nach Satz 1.19 (v) ist $\mathrm{Gal}(L : K_0^*)$ Normalteiler in $\mathrm{Gal}(L : K_0)$ und $\mathrm{Gal}(L : K_0)/\mathrm{Gal}(L : K_0^*)$ isomorph zu $\mathrm{Gal}(K_0^* : K_0)$, also abelsch.

Nach Satz 1.33 (i) ist für alle $i \in \{0, \dots, l-1\}$ die Körpererweiterung $K_{i+1}^* : K_i^*$ galoissch mit zyklischer Galoisgruppe $\mathrm{Gal}(K_{i+1}^* : K_i^*)$. Nach Satz 1.19 (v) ist $\mathrm{Gal}(L : K_{i+1}^*)$ Normalteiler von $\mathrm{Gal}(L : K_i^*)$ und $\mathrm{Gal}(L : K_i^*)/\mathrm{Gal}(L : K_{i+1}^*)$ isomorph zu $\mathrm{Gal}(K_{i+1}^* : K_i^*)$, also abelsch.

Damit ist $\mathrm{Gal}(L : K_0), \mathrm{Gal}(L : K_0^*), \dots, \mathrm{Gal}(L : K_l^*) = \{\mathrm{id}_L\}$ eine Auflösung von $\mathrm{Gal}(L : K)$. $E : K$ ist galoissch, und damit ist, wieder nach Satz 1.19 (v), $\mathrm{Gal}(L : E)$ Normalteiler von $\mathrm{Gal}(L : K)$ mit $\mathrm{Gal}(L : K)/\mathrm{Gal}(L : E) \cong \mathrm{Gal}(E : K)$. Also ist $\mathrm{Gal}(E : K)$ homomorphes Bild einer auflösbaren Gruppe und damit selber auflösbar. □

Bemerkung 1.40 (Die Galoisgruppe als Permutationsgruppe)**.** Sei E der Zerfällungskörper von $f \in K[X]$, und seien $\alpha_1, \ldots, \alpha_n \in E$ die Nullstellen von f. Es gilt also $E = K(\alpha_1, \ldots, \alpha_n)$. Jedes $\varphi \in \mathrm{Gal}(E : K)$ bildet die Nullstellen von f wieder auf Nullstellen von f ab. Da mit φ auch φ^{-1} ein Element von $\mathrm{Gal}(E : K)$ ist, ist $\varphi \restriction \{\alpha_1, \ldots, \alpha_n\}$ eine Permutation der Nullstellen von f. Da E über K von den α_i erzeugt wird, ist φ bereits durch diese Permutation von $\{\alpha_1, \ldots, \alpha_n\}$ eindeutig bestimmt. Also ist $\mathrm{Gal}(E : K)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

Ist f irreduzibel, so operiert $\mathrm{Gal}(E : K)$ *transitiv* auf den Nullstellen von f, d.h., für alle $i, j \in \{1, \ldots, n\}$ existiert ein $\varphi \in \mathrm{Gal}(E : K)$ mit $\varphi(\alpha_i) = \alpha_j$. Für alle i und j existiert nämlich ein Isomorphismus $\psi : K(\alpha_i) \to K(\alpha_j)$, der K punktweise festläßt und α_i auf α_j abbildet. (ψ existert, da $K(\alpha_i)$ und $K(\alpha_j)$ beide über K zu $K[X]/(f)$ isomorph sind.) Der Isomorphismus ψ läßt sich, wie im Beweis für die Eindeutigkeit des Zerfällungskörpers, zu einem Automorphismus von ganz E fortsetzen.

Bemerkung 1.41. Nach Lemma 1.29 ist jede Untergruppe einer auflösbaren Gruppe auflösbar. Nach Bemerkung 1.27 ist die symmetrische Gruppe S_n auflösbar für $n \leq 4$. Sei K ein Körper der Charakteristik 0 und $f \in K[X]$ ein Polynom mit Grad ≤ 4. Weiter sei E der Zerfällungskörper von f über K. f habe n Nullstellen. Da der Grad von f höchstens 4 ist, ist $n \leq 4$. Nach Bemerkung 1.40 ist $\mathrm{Gal}(E : K)$ isomorph zu einer Untergruppe von S_n und damit auflösbar. Nach Satz 1.37 ist f also durch Radikale auflösbar.

In den Übungen wird gezeigt, daß die Galoisgruppe des Zerfällungskörpers von $X^5 - 6X^3 + 3$ über $\mathbb{Q}$ isomorph zu S_5 ist. Da S_5 nach Satz 1.28 nicht auflösbar ist, ist $X^5 - 6X^3 + 3$ nach Satz 1.37 über $\mathbb{Q}$ nicht durch Radikale auflösbar.

1.6. **Die Galoisgruppe der allgemeinen Gleichung.** Sei K ein Körper, $K[X_1, \ldots, X_n]$ der Polynomring über K in den Unbestimmten $X_1, \ldots, X_n$ und $L := K(X_1, \ldots, X_n)$ der Quotientenkörper von $K[X_1, \ldots, X_n]$ (der Körper der rationalen Funktionen in den Unbestimmten $X_1, \ldots, X_n$). $g \in L$ heißt *symmetrisch*, wenn g bei jeder Permutation der $X_1, \ldots, X_n$ unverändert bleibt. (Jede Permutation der X_i induziert einen Automorphismus von L. g ist symmetrisch, falls g im Fixpunktkörper der Gruppe dieser Automorphismen liegt.)

Betrachte das Polynom

$$f(X) := (X - X_1) \cdot \cdots \cdot (X - X_n) = s_0 X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n X^0.$$

f heißt *allgemeine Gleichung über K*. Die Koeffizienten $s_0, \ldots, s_n$ heißen die *elementarsymmetrischen Polynome von $K[X_1 \ldots, X_n]$*.

Sei $M := K(s_0, \ldots, s_n)$. Dann ist L der Zerfällungskörper von $f \in M[X]$. f ist separabel. Damit ist $L : M$ ein galoissche Körpererweiterung.

Satz 1.42. $\mathrm{Gal}(L : M) \cong S_n$

Beweis. Nach Bemerkung 1.40 permutiert jedes $\varphi \in \mathrm{Gal}(L : M)$ die Nullstellen $X_1, \ldots, X_n$ von f. Jede Permutation π von $\{X_1, \ldots, X_n\}$ induziert einen Automorphismus

$$\overline{\pi} : L \to L; \frac{g(X_1, \ldots, X_n)}{h(X_1, \ldots, X_n)} \mapsto \frac{g(\pi(X_1), \ldots, \pi(X_n))}{h(\pi(X_1), \ldots, \pi(X_n))}.$$

Wie man leicht sieht, läßt $\overline{\pi}$ die Polynome $s_0, \ldots, s_n$ fest (und natürlich auch die Elemente von K). Damit ist $\overline{\pi} \in \mathrm{Gal}(L : M)$. Das zeigt $\mathrm{Gal}(L : M) \cong S_n$. □

Bemerkung 1.43. K habe die Charakteristik 0. Da S_n nach Satz 1.28 nur für $n \leq 4$ auflösbar ist, ist die allgemeine Gleichung über K für $n \geq 5$ nicht durch Radikale auflösbar.

Jedes symmetrische Polynom $g \in K[X_1, \ldots, X_n]$ liegt offenbar im Fixpunktkörper von $\mathrm{Gal}(L : M)$, also in M. Das liefert sofort

Satz 1.44 (Hauptsatz über symmetrische Polynome)**.** *Sei K ein Körper der Charakteristik 0. Dann läßt sich jedes symmetrische $g \in K(X_1, \ldots, X_n)$ darstellen als Quotient von Polynomen in den elementarsymmetrischen Polynomen $s_0, \ldots, s_n$ mit Koeffizienten in K.*

Es gibt auch eine allgemeinere Formulierung dieses Satzes für symmetrische Polynome über kommutativen Ringen R mit 1.

Bemerkung 1.45. Sei G eine Gruppe der Ordnung n. Dann ist G isomorph zu einer Untergruppe von S_n (Satz 5.1, Einführung in die Algebra und Zahlentheorie). Nach dem Hauptsatz der Galoistheorie besitzt $L : M$ einen Zwischenkörper F mit $\mathrm{Gal}(L : F) \cong G$, nämlich den Fixpunktkörper einer zu G isomorphen Untergruppe von $\mathrm{Gal}(L : M) \cong S_n$.

Also tritt jede endliche Gruppe auf als Galoisgruppe einer endlichen, galoisschen Körpererweiterung. Es ist nicht bekannt, ob jede endliche Gruppe auch als Galoisgruppe einer endlichen, galoisschen Körpererweiterung mit dem Grundkörper $\mathbb{Q}$ auftritt. Safarevic hat gezeigt, daß zumindest jede auflösbare endliche Gruppe als Galoisgruppe einer endlichen, galoisschen Körpererweiterung der Form $E : \mathbb{Q}$ auftritt.

2. Kreisteilung und Konstruktion regelmässiger n-Ecke

In diesem Abschnitt werden wir diejenigen n bestimmen, für die sich das regelmäßige n-Eck mit Zirkel und Lineal aus der Einheitsstrecke konstruieren läßt. Legt man ein regelmäßiges n-Eck so auf die Gaußsche Zahlenebene $\mathbb{C}$, daß sich der Mittelpunkt im Nullpunkt befindet und eine Ecke der Punkt $1 \in \mathbb{R}$ ist, so sind die Ecken des n-Ecks genau die n-ten Einheitswurzeln.

Wir beginnen mit einigen Betrachtungen zu n-ten Einheitswurzeln. Im folgenden sei K ein Körper der Charakteristik 0. In Bemerkung 1.32 wurde festgestellt, daß die n-ten Einheitswurzeln bezüglich der Multiplikation eine zyklische Gruppe E_n im Zerfällungskörper L von $X^n - 1$ über K bilden. L heißt der *n-te Kreisteilungskörper über K*.

Die Ordnung von E_n ist n. Die Elemente von E_n der Ordnung n sind die primitiven n-ten Einheitswurzeln. Ist ζ primitive n-te Einheitswurzel, so ist ζ^i genau dann ebenfalls primitive n-te Einheitswurzel, wenn i und n teilerfremd sind. Es gibt also genau $\varphi(n)$ primitive n-te Einheitswurzeln. (φ ist die Eulersche φ-Funktion, die zu jedem $n \in \mathbb{N}$ die Anzahl der zu n teilerfremden $m \in \{1, \ldots, n\}$ liefert.)

Definition 2.1. Seien $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln über K. Das Polynom $\Phi_{n,K} := \prod_{i=1}^{\varphi(n)}(X - \zeta_i)$ heißt *n-tes Kreisteilungspolynom über K*. Falls sich K aus dem Zusammenhang ergibt, schreiben wir Φ_n anstelle von $\Phi_{n,K}$.

Lemma 2.2. $\Phi_{n,K} \in K[X]$

Beweis. Sei L der Zerfällungskörper von $X^n - 1$ über K. Dann ist $L : K$ endlich und galoissch. Die Elemente von $\mathrm{Gal}(L : K)$ permutieren die n-ten Einheitswurzeln, und ihre Einschränkungen auf E_n sind Automorphismen von E_n. Damit bilden die Elemente von $\mathrm{Gal}(L : K)$ primitive n-te Einheitswurzeln wieder auf primitive n-te Einheitswurzeln ab. Die Elemente von $\mathrm{Gal}(L : K)$ induzieren also Automorphismen von $L[X]$, die $\Phi_{n,K}$ wieder auf $\Phi_{n,K}$ abbilden. Damit liegen die Koeffizienten von $\Phi_{n,K}$ im Fixpunktkörper von $\mathrm{Gal}(L : K)$, also in K. □

Satz 2.3. $X^n - 1 = \prod_{d|n} \Phi_d$

Beweis. Sei d ein Teiler von n. Dann ist jede Nullstelle von $X^d - 1$ auch Nullstelle von $X^n - 1$. Eine n-te Einheitswurzel ζ ist genau dann primitive d-te Einheitswurzel, wenn d die Ordnung von ζ in E_n ist. Jede n-te Einheitswurzel ist also Nullstelle genau eines Φ_d. Da $X^n - 1$ und $\prod_{d|n} \Phi_d$ keine mehrfachen Nullstellen besitzen, gilt $X^n - 1 = \prod_{d|n} \Phi_d$. □

Satz 2.4. $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$

Beweis. Wir beweisen den Satz durch vollständige Induktion über n. Für $n = 1$ ist $\Phi_n = X - 1$.

Sei L der n-te Kreisteilungskörper. Angenommen für alle $d < n$ ist $\Phi_d \in \mathbb{Z}[X]$. Nach Satz 2.3 ist der Rest bei Polynomdivision von $X^n - 1$ durch $\prod_{d|n \wedge d \neq n} \Phi_d$ null. Die Division erfolgt aber in $\mathbb{Z}[X]$, da $\prod_{d|n \wedge d \neq n} \Phi_d$ normiert ist und nach der Induktionsvoraussetzung ganzzahlige Koeffizienten

hat. Also liegt

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n \wedge d \neq n} \Phi_d}$$

in $\mathbb{Z}[X]$. □

Satz 2.5. *Φ_n ist irreduzibel in $\mathbb{Z}[X]$ (und damit auch in $\mathbb{Q}[X]$, siehe Bemerkung 24.1, Einführung in die Algebra und Zahlentheorie).*

Beweis. Seien $g, f \in \mathbb{Z}[X]$ mit $\Phi_n = f \cdot g$, f irreduzibel. Da Φ_n normiert ist, sind auch f und g normiert. Sei ζ Nullstelle von f in $\mathbb{C}$, also ζ primitive n-te Einheitswurzel.

Wir zeigen: Ist p Primzahl und teilerfremd zu n, so ist auch ζ^p Nullstelle von f. Wiederholte Anwendung zeigt dann, daß alle primitiven n-ten Einheitswurzeln Nullstellen von f sind. Es folgt, daß g konstant ist.

Angenommen, p ist eine zu n teilerfremde Primzahl, für die $f(\zeta^p) \neq 0$ ist. Dann ist ζ^p primitive n-te Einheitswurzel, also Nullstelle von Φ_n. Wegen $f(\zeta^p) \neq 0$ ist ζ^p Nullstelle von g. $g(X^p)$ ist also ein Polynom mit der Nullstelle ζ. Wegen $f = \mathrm{Irr}(\zeta, \mathbb{Q})$ ist $g(X^p)$ ein Vielfaches (in $\mathbb{Q}[X]$) von f.

f und $g(X^p)$ sind normiert und damit primitiv (der größte gemeinsame Teiler der Koeffizienten ist jeweils 1). Nach dem Lemma von Gauß (Satz 21.4, Einführung in die Algebra und Zahlentheorie) existiert ein $h \in \mathbb{Z}[X]$ mit $f(X) \cdot h(X) = g(X^p)$.

Wir betrachten die Situation modulo p. Sei $\bar{\cdot} : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ die von der Quotientenabbildung $\mathbb{Z} \to \mathbb{Z}_p; a \mapsto a + p\mathbb{Z}$ induzierte Abbildung. Man erinnere sich, daß für Körper der Charakteristik p die Abbildung $a \mapsto a^p$ ein Homomorphismus ist. In $\mathbb{Z}_p[X]$ gilt also

$$\overline{f}(X) \cdot \overline{h}(X) = \overline{g(X^p)} = \overline{g(X)}^p.$$

Sei $f_0 \in \mathbb{Z}_p[X]$ ein irreduzibler Teiler von $\overline{f}$. Dann teilt f_0 auch $\overline{g}$. Damit ist f_0^2 ein Teiler von $\overline{f} \cdot \overline{g}$. Es gilt aber $\overline{f} \cdot \overline{g} = \overline{\Phi}_n$. $\overline{\Phi}_n$ ist ein Teiler von $X^n - 1 \in \mathbb{Z}_p[X]$.

Die Ableitung von $X^n - 1 \in \mathbb{Z}_p[X]$ ist $(n + p\mathbb{Z})X^{n-1}$. Da Da n und p teilerfremd sind, hat diese Ableitung im n-ten Kreisteilungskörper über $\mathbb{Z}_p$ nur die Nullstelle 0. Also hat $X^n - 1$ im n-ten Kreisteilungskörper über $\mathbb{Z}_p$ nur einfache Nullstellen. (Siehe Bemerkung 18.5, Einführung in die Algebra und Zahlentheorie.) $X^n - 1$ wird in $\mathbb{Z}_p[X]$ aber von f_0^2 geteilt und hat damit eine doppelte Nullstelle in seinem Zerfällungskörper. Ein Widerspruch. □

Satz 2.6. *Sei L der n-te Kreisteilungskörper über $\mathbb{Q}$. Dann ist* $\mathrm{Gal}(L : \mathbb{Q})$ *isomorph zur primen Restklassengruppe $\mathbb{Z}_n^*$.*

Beweis. Sei $\zeta \in L$ primitive n-te Einheitswurzel und $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$. Dann ist $\sigma(\zeta)$ wieder primitive n-te Einheitswurzel, z.B. $\sigma(\zeta) = \zeta^i$ für ein zu n teilerfremdes i, und σ ist eindeutig bestimmt durch $\sigma(\zeta)$. In Bemerkung 1.32 haben wir gesehen, daß die Abbildung $h : \mathrm{Gal}(L : K) \to (\mathbb{Z}_n^*, \cdot); \sigma \mapsto i + n\mathbb{Z}$ ein injektiver Homomorphismus ist.

Da Φ_n irreduzibel ist, ist $\Phi_n = \mathrm{Irr}(\zeta, \mathbb{Q})$. Da Φ_n den Grad $\varphi(n)$ hat, $L : \mathbb{Q}$ endlich und galoissch ist und L aus $\mathbb{Q}$ durch Adjunktion einer Nullstelle von Φ_n entsteht, gilt $|\mathrm{Gal}(L : K)| = \varphi(n)$. Also ist h surjektiv und damit ein Isomorphismus. □

2.1. **Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal.** Wir setzen den folgenden Satz als bekannt voraus. (Siehe Satz 28.1, Einführung in die Algebra und Zahlentheorie.)

Satz 2.7. *$\alpha \in \mathbb{R}$ läßt sich genau dann mit Zirkel und Lineal aus den Punkten 0 und 1 konstruieren, wenn eine Körperkette $\mathbb{Q} = K_0 \leq \cdots \leq K_m$ mit $\alpha \in K_m$ existiert, so daß für alle $i < m$ der Grad der Erweiterung $[K_{i+1} : K_i]$ genau 2 ist (wenn also K_{i+1} aus K_i durch Adjunktion einer Quadratwurzel eines Elementes von K_i entsteht). Insbesondere ist für konstruierbare $\alpha \in \mathbb{R}$ der Grad der Erweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$ eine Zweierpotenz.*

Wir benötigen eine Variation dieses Satzes für n-Einheitswurzeln. Um ein regelmäßiges n-Eck zu konstruieren, genügt es in der Zahlenebene $\mathbb{C}$ den Punkt $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ zu konstruieren.

Lemma 2.8. *ζ ist genau dann konstruierbar, wenn eine Körperkette $\mathbb{Q} = K_0 \leq \cdots \leq K_m$ existiert mit $[K_{i+1} : K_i] = 2$ für alle $i \in \{0, \ldots, m-1\}$ und $\zeta \in K_m$.*

Beweis. Angenommen, $\mathbb{Q} = K_0 \leq \cdots \leq K_m$ ist eine Körperkette wie oben. Mit ζ ist auch $\zeta + \overline{\zeta}$ ein Element von K_m. Damit ist $\zeta + \overline{\zeta} \in \mathbb{R}$ konstruierbar nach Satz 2.7. Also ist auch ζ konstruierbar.

Sei nun ζ konstruierbar. Dann ist auch $\zeta + \overline{\zeta}$ konstruierbar, und es existiert eine Körperkette $\mathbb{Q} = K_0 \leq \cdots \leq K_m$ mit $[K_{i+1} : K_i] = 2$ für alle $i \in \{0, \ldots, m-1\}$ und $\zeta + \overline{\zeta} \in K_m$. Setze $K_{m+1} := K_m(\zeta)$. Wegen $i\sin\frac{2\pi}{n} = \sqrt{-(1 - (\frac{\zeta+\overline{\zeta}}{2})^2)}$ ist $[K_{m+1} : K_m] = 2$, falls $K_{m+1} \neq K_m$. Das zeigt die Existenz der gewünschten Körperkette. □

Bei der Konstruktion regelmäßiger n-Ecke spielen die Fermatschen Primzahlen eine wesentliche Rolle.

Definition 2.9. Eine Primzahl $p \neq 2$ der Form $2^m + 1$ heißt *Fermatsche Primzahl*.

Lemma 2.10. *Ist $p = 2^m + 1$ eine Primzahl mit $p \neq 2$, so ist m eine Zweierpotenz (also p von der Form $2^{2^k} + 1$).*

Beweis. Sei $m = r \cdot s$ und $r \neq 1$ ungerade. Dann gilt

$$2^m + 1 = (2^s + 1)(2^{s(r-1)} - 2^{s(r-2)} + \cdots - 2^s + 1).$$

Also ist $2^m + 1$ keine Primzahl. □

$2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ und $2^{2^4} + 1 = 65537$ sind Fermatsche Primzahlen. $2^{2^5} + 1$ ist keine Primzahl. Man vermutet, daß es nur endlich viele Fermatsche Primzahlen gibt.

Wir sammeln ein paar einfache Feststellungen über die Konstruierbarkeit regelmäßiger n-Ecke. Offenbar gilt

Lemma 2.11. *Ist das regelmäßige n-Eck konstruierbar und $m|n$, so ist auch das regelmäßige m-Eck konstruierbar.*

Lemma 2.12. *Seien k und l teilerfremde natürliche Zahlen. Sind sowohl das regelmäßige k-Eck als auch das regelmässige l-Eck konstruierbar, so ist auch das regelmäßige $k \cdot l$-Eck konstruierbar.*

Beweis. Nach dem Euklidischen Algorithmus existieren $\lambda, \mu \in \mathbb{Z}$ mit $\lambda k + \mu l = 1$. Es gilt $\frac{2\pi\mu}{k} + \frac{2\pi\lambda}{l} = \frac{2\pi}{k \cdot l}$. Geeignete Addition bzw. Subtraktion der Winkel $\frac{2\pi}{k}$ und $\frac{2\pi}{l}$ liefert also den Winkel $\frac{2\pi}{k \cdot l}$. □

Da sich Winkel mit Zirkel und Lineal halbieren lassen, gilt schließlich

Lemma 2.13. *Für $l > 0$ ist das regelmäßige 2^l-Eck mit Zirkel und Lineal konstruierbar.*

Die wesentliche Information zur Berechnung derjenigen n, für die das regelmäßige n-Eck konstruierbar ist, liefert

Lemma 2.14. *Für eine Primzahl $p > 2$ ist das regelmäßige p-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn p Fermatsche Primzahl ist.*

Beweis. Sei $\zeta_p := \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$, also ζ_p primitive p-te Einheitswurzel.

Angenommen das regelmäßige p-Eck ist konstruierbar. Nach Lemma 2.8 ist dann $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ eine Zweierpotenz.

Andererseits ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ nach Satz 2.6. Also ist p Fermatsche Primzahl.

Für die andere Richtung sei p Fermatsche Primzahl. Nach Satz 2.6 ist die Erweiterung $\mathbb{Q}(\zeta_p) : \mathbb{Q}$ ist endlich und galoissch mit $\mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q}) \cong \mathbb{Z}_p^*$. Die prime Restklassengruppe $\mathbb{Z}_p^*$ ist zyklisch von der Ordnung $p - 1$. Da p eine Fermatsche Primzahl ist, existiert ein m mit $p = 2^m + 1$.

Es ist leicht zu sehen, daß eine Folge $U_0, \ldots, U_m$ von Untergruppen von $\mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ existiert mit

$$\{\mathrm{id}\} = U_0 \leq \cdots \leq U_m = \mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$$

und $|U_i| = 2^i$ für alle i. Offenbar gilt $[U_{i+1} : U_i] = 2$ für alle $i \in \{0, \ldots, m-1\}$. Der Hauptsatz der Galoistheorie liefert eine Körperkette

$$\mathbb{Q} = K_0 \leq \cdots \leq K_m = \mathbb{Q}(\zeta_p)$$

mit $[K_{i+1} : K_i] = 2$ für alle $i \in \{0, \ldots, m-1\}$. Die Konstruierbarkeit des regelmäßigen p-Ecks folgt nun aus Lemma 2.8. □

Mit diesen Vorbereitungen können wir diejenigen n, für die das regelmäßige n-Eck konstruierbar ist, bestimmen.

Satz 2.15. *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n die Form $2^m \cdot p_1 \ldots p_r$ hat, wobei die p_i paarweise verschiedene Fermatsche Primzahlen sind.*

Beweis. Hat n die oben angebene Form, so ist das regelmäßige n-Eck konstruierbar nach Lemma 2.12, Lemma 2.13 und Lemma 2.14.

Ist das n-Eck konstruierbar und $p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ die Primfaktorzerlegung von n mit paarweise verschiedenen p_i, so ist jedes $p_i \neq 2$ Fermatsche Primzahl nach Lemma 2.11 und Lemma 2.14.

Angenommen für ein i ist $\alpha_i > 1$. Dann ist auch das regelmäßige p_i^2-Eck konstruierbar. Nach Lemma 2.8 ist also $[\mathbb{Q}(\zeta_{p_i}) : \mathbb{Q}]$ eine Zweierpotenz. Nach Satz 2.6 ist aber $[\mathbb{Q}(\zeta_{p_i^2}) : \mathbb{Q}] = \varphi(p_i^2) = p_i \cdot (p_i - 1)$. Letzteres ist aber nur für $p_i = 2$ eine Zweierpotenz. Daraus folgt, daß n die oben angegebene Form hat. □

3. Die Sylow-Sätze

In diesem Abschnitt werden wichtige Sätze über die Struktur endlicher Gruppen bewiesen.

3.1. **Operationen von Gruppen auf Mengen.**

Definition 3.1. Sei G eine Gruppe und X eine Menge. Eine Abbildung $G \times X \to X; (g,x) \mapsto g \cdot x$ heißt *Gruppenoperation* (G operiert auf X), wenn für alle $g, h \in G$, alle $x \in X$ und das neutrale Element e von G gilt:

(i) $(gh) \cdot x = g \cdot (h \cdot x)$
(ii) $e \cdot x = x$

Für $x \in X$ heißt $G \cdot x := \{g \cdot x : g \in G\}$ der *G-Orbit* (oder einfach *Orbit*) *von x*. $G_x := \{g \in G : g \cdot x = x\}$ heißt der *Stabilisator von x*.

Wie man leicht nachrechnet, induziert jede Gruppenoperation $G \times X \to X; (g,x) \mapsto g \cdot x$ einen Homomorphismus von G in die Gruppen S_X der Permutationen der Menge X, indem man jedes $g \in G$ auf die Permutation $x \mapsto g \cdot x$ abbildet. Umgekehrt liefert jeder Homomorphismus $\varphi : G \to S_X$ eine Gruppenoperation $(g,x) \mapsto \varphi(g)(x)$. In gewissem Sinne sind Gruppenoperationen also das gleiche wie Homomorphismen von Gruppen in Permutationsgruppen.

Im folgenden sei $G \times X \to X; (g,x) \mapsto g \cdot x$ immer eine Gruppenoperation.

Lemma 3.2. *Für jedes $x \in X$ gilt:*

(i) *G_x ist eine Untergruppe von G.*
(ii) $|G \cdot x| = [G : G_x]$

Beweis. Für (i) seien $g, h \in G_x$. Dann ist $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, also $gh \in G_x$. Außerdem ist für $g \in G_x$ auch $g^{-1} \in G_x$, da $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = e \cdot x = x$, wobei e das neutrale Element von G ist.

Für (ii) seien $g, h \in G$. Dann gilt

$$g^{-1}h \in G_x \Leftrightarrow g^{-1} \cdot (h \cdot x) = x \Leftrightarrow h \cdot x = g \cdot x.$$

g und h liegen also genau dann in derselben Linksnebenklasse von G_x, wenn $g \cdot x = h \cdot x$ gilt. Die Abbildung $gG_x \mapsto g \cdot x$ ist also eine Bijektion zwischen der Menge der Linksnebenklassen von G_x und $G \cdot x$. □

Lemma 3.3. *Für $x, y \in X$ sind die Orbits $G \cdot x$ und $G \cdot y$ entweder gleich oder disjunkt. Die Relation $\{(x,y) : \exists g, h \in G(g \cdot x = h \cdot y)\}$ ist also eine Äquivalenzrelation (die* Orbit-Äquivalenzrelation*).*

Beweis. Angenommen $g \cdot x = h \cdot y$. Dann gilt $x = (g^{-1}h) \cdot y$. Also ist $x \in G \cdot y$ und damit $G \cdot x \subseteq G \cdot y$. Vertauscht man x und y, so ergibt sich $G \cdot y \subseteq G \cdot x$. Also gilt $G \cdot x = G \cdot y$. Daraus folgt die Behauptung. □

Satz 3.4. *Sei $V \subseteq X$ eine Menge, die jeden Orbit in genau einem Punkt schneidet. (Man nennt V ein* Vertretersystem für die Orbits*.) Dann gilt:*

$$|X| = \sum_{x \in V} [G : G_x]$$

Beweis. Nach Lemma 3.3 ist X die disjunkte Vereinigung der Orbits. Nach Lemma 3.2 ist die Mächtigkeit eines Orbits $G \cdot x$ genau $[G : G_x]$. Das liefert die Behauptung. □

Definiert man die Menge der *Fixpunkte der Gruppenoperation* als

$$\mathrm{Fix}_X(G) := \{x \in X : \forall g \in G(g \cdot x = x)\},$$

so läßt sich Satz 3.4 auch schreiben als

Folgerung 3.5. *Sei $V \subseteq X$ ein Vertretersystem für die Orbits. Dann gilt:*

$$|X| = |\mathrm{Fix}_X(G)| + \sum_{x \in V \wedge [G:G_x] > 1} [G : G_x]$$

Mit Hilfe dieser Folgerung können wir folgenden Fixpunktsatz beweisen:

Satz 3.6. *Ist p eine Primzahl und G ein Gruppe der Ordnung p^r, die auf einer endlichen Menge X operiert, so ist $|X| \equiv |\mathrm{Fix}_X(G)| \pmod p$. Insbesondere gibt es mindestens einen Fixpunkt, falls $|X|$ und p teilerfremd sind.*

Beweis. Sei $V \subseteq X$ ein Vertretersystem für die Orbits. Nach Folgerung 3.5 ist

$$|X| - |\mathrm{Fix}_X(G)| = \sum_{x \in V \wedge [G:G_x] > 1} [G : G_x].$$

Jeder Summand auf der rechten Seite dieser Gleichung ist ein von 1 verschiedener Teiler von p^r, also ein Vielfaches von p. Damit ist die Summe durch p teilbar. Sind $|X|$ und p teilerfremd, so muß $|\mathrm{Fix}_X(G)|$ also von 0 verschieden sein. □

Wichtig ist folgendes Beispiel einer Gruppenoperation: $\mathcal{U}$ sei die Menge aller Untergruppen der Gruppe G. Dann operiert G auf $\mathcal{U}$ durch Konjugation, d.h., mittels der Abbildung $G \times \mathcal{U} \to \mathcal{U}; (g, U) \mapsto gUg^{-1}$.

Für $U \in \mathcal{U}$ schreibt man $N(U)$ anstelle von G_U. $N(U)$ ist der *Normalisator von U in G*. $N(U)$ ist die größte Untergruppe von G, in der U Normalteiler ist.

Für jedes $U \in \mathcal{U}$ ist der Orbit von U genau die Menge der zu U konjugierten Untergruppen von G. Lemma 3.2 liefert sofort

Satz 3.7. *Die Anzahl der verschiedenen zu einer Untergruppe U von G konjugierten Untergruppen ist $[G : N(U)]$.*

G operiert auch auf sich selber durch Konjugation, also durch $(g, h) \mapsto ghg^{-1}$. Der Stabilisator G_g eines Elementes $g \in G$ bzgl. Konjugation heißt, wie im Falle der Konjugation von Untergruppen, der *Normalisator von g* und wird mit $N(g)$ bezeichnet. Wie man leicht sieht, ist $\mathrm{Fix}_G(G)$ genau das Zentrum $Z(G) = \{h \in G : \forall g \in G(gh = hg)\}$ von G. Im Beweis von Lemma 1.26 wurde gezeigt, daß jede p-Gruppe, also jede Gruppe, deren Ordnung eine (von 1 verschiedene) Potenz der Primzahl p ist, ein nichttriviales Zentrum hat.

Das läßt sich mühelos aus Satz 3.6 ableiten: Ist G eine p-Gruppe, so ist $|Z(G)| = |\mathrm{Fix}_G(G)| \equiv |G| \equiv 0 \pmod p$. Da $Z(G)$ mindestens das neutrale Element enthält, ist $|Z(G)| \neq 0$. Damit ist $|Z(G)| > 1$.

3.2. **Sylow-Untergruppen.**

Definition 3.8. Sei G eine endliche Gruppe und p eine Primzahl. Eine Untergruppe U von G heißt *p-Sylow-Untergruppe von G*, falls die Ordnung von U die höchste p-Potenz ist, die die Ordnung von G teilt.

Wir zeigen, daß p-Sylow-Untergruppen immer existieren. Dazu benötigen wir ein Lemma über abelsche Gruppen.

Lemma 3.9. *Sei G eine endliche abelsche Gruppe und p eine Primzahl, die die Ordnung von G teilt. Dann hat G eine Untergruppe der Ordnung p.*

Beweis. Sei $n \neq 0$ ein gemeinsames Vielfaches aller Ordnungen von Elementen von G. Man nennt solch ein n einen *Exponenten von G*. Wir zeigen induktiv, daß die Ordnung von G eine Potenz von n teilt. Für $|G|= 1$ ist das klar.

Sei $|G|> 1$. Dann existiert ein $g \in G$ mit $g \neq e_G$. Sei H die von g erzeugte zyklische Gruppe. Wegen $g^n = e_G$ ist n ein Vielfaches von $|H|$. Wie man leicht sieht, ist n ein Exponent von G/H. Nach Induktionsannahme teilt $|G/H|$ eine Potenz von n. Wegen $|G|= [G : H]\cdot |H|$ teilt damit auch $|G|$ eine Potenz von n.

Angenommen p teilt $|G|$. Nach dem eben Gezeigten teilt p jeden Exponenten von G. Also enthält G ein Element g, dessen Ordnung ein Vielfaches von p ist. Sei m die Ordnung von g. Dann hat $g^{\frac{m}{p}}$ die Ordnung p. Die von g erzeugte zyklische Gruppe ist die gesuchte Untergruppe von G. □

Satz 3.10. *Sei G eine endliche Gruppe und p eine Primzahl. Dann hat G eine p-Sylow-Untergruppe.*

Beweis. Wir beweisen den Satz durch Induktion über die Ordnung von G. Der Fall $|G|= 1$ ist klar. Sei also $|G|> 1$.

Angenommen G hat eine echte Untergruppe H, so daß $[G : H]$ teilerfremd zu p ist. Nach Induktionsannahme hat H eine p-Sylow-Untergruppe P. Da p den Index von H in G nicht teilt, ist die höchste p-Potenz, die $|H|$ teilt, auch die höchste p-Potenz, die $|G|$ teilt. Also ist P auch p-Sylow-Untergruppe von G.

Wir können also annehmen, daß der Index jeder echten Untergruppe von G ein Vielfaches von p ist. G operiert auf sich selber durch Konjugation. Das Zentrum $Z(G)$ von G ist genau die Menge der Fixpunkte bezüglich dieser Gruppenoperation. Nach Folgerung 3.5 teilt p die Ordnung von $Z(G)$. Nach Lemma 3.9 hat $Z(G)$ eine Untergruppe H der Ordnung p. Da die Elemente von H mit allen Elementen von G kommutieren, ist H ein Normalteiler von G.

Sei $h : G \to G/H; g \mapsto gH$ die Quotientenabbildung. Nach Induktionsannahme hat G/H eine p-Sylow-Untergruppe P. Sei p^r die höchste p-Potenz, die $|G|$ teilt. Dann ist p^{r-1} die höchste p-Potenz, die $|G/H|$ teilt. Also hat P die Ordnung p^{r-1}. $h^{-1}[P]$ hat die Ordnung $p \cdot p^{r-1} = p^r$. Also ist $h^{-1}[P]$ p-Sylow-Untergruppe von G. □

Satz 3.11. *Sei G eine endliche Gruppe. Dann gilt:*

(i) *Jede p-Gruppe $H \leq G$ ist in einer p-Sylow-Untergruppe von G enthalten.*

(ii) *Für jede p-Gruppe $H \leq G$ und jede p-Sylow-Untergruppe $P \leq G$ existiert ein $g \in G$ mit $gHg^{-1} \leq P$. Insbesondere sind alle p-Sylow-Untergruppen von G konjugiert.*
(iii) *Die Anzahl der p-Sylow-Untergruppen von G ist kongruent zu* 1 *modulo p und teilt $|G|$.*

Beweis. Sei S die Menge der p-Sylow-Untergruppen von G. G operiert auf S durch Konjugation. Sei P ein Element von S. P ist eine Untergruppe des Stabilisators G_P von P bezüglich Konjugation. Da die Ordnung von P bereits die höchste p-Potenz ist, die $|G|$ teilt, ist $[G : G_P]$ teilerfremd zu p. Also ist die Mächtigkeit des Orbits S_P von P teilerfremd zu p.

Angenommen $H \leq G$ ist eine p-Gruppe mit $|H| > 1$. Dann operiert H auf S_P durch Konjugation und S_P zerfällt in paarweise disjunkte Orbits bezüglich der Operation von H. Nach Satz 3.6 hat die Operation von H auf S_P einen Fixpunkt P'. H ist eine Untergruppe von $G_{P'}$, dem Normalisator von P'.

Da jede Untergruppe einer Gruppe Normalteiler ihres Normalisators ist, gilt $gP' = P'g$ für alle $g \in H$. Damit ist HP' Untergruppe von G und P' Normalteiler von HP'. Da HP'/P' zu $H/(H \cap P')$ isomorph ist, ist $|HP'/P'|$ eine Potenz von p. Also ist auch $|HP'|$ eine Potenz von p. Da P' aber p-Sylow-Untergruppe ist, folgt daraus $HP' = P'$. Insbesondere ist $H \leq P'$. Das zeigt (i). Ist H selbst p-Sylow-Untergruppe, so gilt sogar $H = P'$. Das zeigt (ii). Aus (ii) folgt sofort $S_P = S$.

Sei schließlich $H = P$. Dann gibt es genau einen einelementigen Orbit der Operation von H auf S, nämlich $\{P\}$. (Wir haben nämlich oben gezeigt, daß $H \leq P'$ für jeden Fixpunkt P' der Operation von H auf S gilt.) Die Mächtigkeiten aller anderen Orbits sind von der Form $[P : U]$ für echte Untergruppen U von P, also Vielfache von p. Damit ist $|S|$ kongruent zu 1 modulo p. Wegen $|S| = |S_P| = [G : G_P]$ ist die Anzahl der p-Sylow-Untergruppen ein Teiler von $|G|$. □

Man kann sogar zeigen, daß für alle p-Potenzen p^s, die $|G|$ teilen, die Anzahl der Untergruppen von G der Ordnung p^s kongruent zu 1 modulo p ist. (Siehe zum Beispiel Meyberg: Algebra.) Wir begnügen uns mit

Folgerung 3.12. *Sei G eine endliche Gruppe, p eine Primzahl und p^s ein Teiler von $|G|$. Dann hat G eine Untergruppe der Ordnung p^s.*

Beweis. Nach Satz 3.10 hat G eine p-Sylow-Untergruppe P. Offenbar teilt p^s die Ordnung von P. Es genügt zu zeigen, daß P eine Untergruppe der Ordnung p^s hat.

Nach Lemma 1.26 ist P auflösbar. Sei $P = P_0, P_1, \ldots, P_k = \{e_G\}$ eine Auflösung von P maximaler Länge mit paarweise verschiedenen P_i. Wie man leicht sieht, haben alle Quotienten P_i/P_{i+1} die Ordnung p. Damit ist $s \leq k$ und P_s hat die Ordnung p^s. □

4. Körpertheorie

4.1. Algebraisch abgeschlossene Körper.

Definition 4.1. Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes nichtkonstante Polynom $f \in K[X]$ über K in Linearfaktoren zerfällt.

Lemma 4.2. *Sei K ein Körper. Dann sind folgende Aussagen äquivalent:*

(i) *K ist algebraisch abgeschlossen.*
(ii) *Jedes nichtkonstante Polynom $f \in K[X]$ hat eine Nullstelle in K.*
(iii) *K hat keine echte algebraische Erweiterung.*

Beweis. (i)⇒(ii) ist klar. Angenommen K erfüllt (ii). Dann haben alle irreduziblen Polynome über K höchstens den Grad 1. Damit hat jede einfache algebraische Erweiterung von K, also jede algebraische Erweiterung, die über K von einem Element erzeugt wird, den Grad 1 und ist damit nicht echt. Daraus folgt (iii).

Wenn K (iii) erfüllt, so haben alle irreduziblen Polynome über K einen Grad ≤ 1. Da jedes Polynom in irreduzible Faktoren zerfällt, zerfällt jedes Polynom über K in Linearfaktoren. Das zeigt (iii)⇒(i). □

Wir zeigen nun den *Fundamentalsatz der Algebra*, der zuerst von Gauß bewiesen wurde.

Satz 4.3. *$\mathbb{C}$ ist algebraisch abgeschlossen.*

Beweis. Wir benötigen zwei Tatsachen aus der reellen Analysis:

1. Jedes $f \in \mathbb{R}[X]$ ungeraden Grades hat eine reelle Nullstelle.
2. Für jedes $a > 0$ hat $x^2 - a$ eine reelle Nullstelle.

Beide Tatsachen folgen aus dem Zwischenwertsatz für stetige reelle Funktionen.

Zum Beweis des Satzes: Es genügt zu zeigen, daß kein Polynom $f \in \mathbb{C}[X]$ mit Grad > 1 irreduzibel ist.

Angenommen $f \in \mathbb{C}[X]$ hat Grad > 1 und ist irreduzibel. Sei E der Zerfällungskörper von f über $\mathbb{C}$. Dann ist E eine echte Erweiterung von $\mathbb{C}$. Da $E : \mathbb{C}$ endlich ist, ist auch $E : \mathbb{R}$ endlich. Nach dem Satz vom primitiven Element existiert ein $\alpha \in E$ mit $E = \mathbb{R}(\alpha)$. Sei F der Zerfällungskörper von $\mathrm{Irr}(\alpha, \mathbb{R})$. Dann ist $F : \mathbb{R}$ endlich und galoissch und es gilt $E \leq F$.

Betrachte $\mathrm{Gal}(F : \mathbb{R})$. Angenommen $|\mathrm{Gal}(F : \mathbb{R})|$ hat einen ungeraden Teiler $t > 1$. Nach Satz 3.10 hat $\mathrm{Gal}(F : \mathbb{R})$ eine 2-Sylow-Untergruppe P. Da t die Ordnung von $\mathrm{Gal}(F : \mathbb{R})$ teilt, ist $P \neq \mathrm{Gal}(F : \mathbb{R})$. $\mathrm{Fix}_F(P)$ ist damit eine echte Erweiterung von $\mathbb{R}$ von ungeradem Grad. Das widerspricht aber 1.

$|\mathrm{Gal}(F : \mathbb{R})|$ ist also eine Zweierpotenz. Damit ist auch $|\mathrm{Gal}(F : \mathbb{C})|$ eine Zweierpotenz. Nach Folgerung 3.12 hat $\mathrm{Gal}(F : \mathbb{C})$ eine Untergruppe H vom Index 2. $\mathrm{Fix}_F(H)$ ist eine Erweiterung von $\mathbb{C}$ vom Grad 2. Also ist $\mathrm{Fix}_F(H) = \mathbb{C}(\sqrt{z})$ für ein geeignetes $z \in \mathbb{C}$. Sei $\varphi \in \mathbb{R}$ mit $Z = |z| (\cos\varphi + i \sin\varphi)$. Nach 2 ist $\sqrt{|z|} \in \mathbb{R}$. Also gilt

$$\sqrt{z} = \pm\sqrt{|z|}(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}) \in \mathbb{C}.$$

Ein Widerspruch. □

Lemma 4.4. *Sei $E : K$ eine Körpererweiterung und $F := \{\alpha \in E : \alpha$ ist algebraisch über $K\}$. Dann gilt:*

(i) *F ist ein Körper, nämlich der* algebraische Abschluß von K in E.
(ii) *F ist der algebraische Abschluß von F in E.*

Beweis. Für (i) seien $a, b \in F$, $b \neq 0$. Dann ist $K(a, b) : K$ algebraisch und damit auch endlich. Also sind $a \cdot b$ und $\frac{a}{b}$ algebraisch über K und damit in F.

Für (ii) sei $a \in E$ algebraisch über F, zum Beispiel a Nullstelle von $b_0 + b_1X + \cdots + b_kX^k \in F[X]$. Dann ist $K[a, b_0, \ldots, b_k] : K$ endlich und damit auch algebraisch. Also ist $a \in F$. □

Satz 4.5. *Sei $E : K$ eine Körpererweiterung und E algebraisch abgeschlossen. Weiter sei F der algebraische Abschluß von K in E. Dann ist F algebraisch abgeschlossen.*

Beweis. Sei $f \in F[X]$. Da E algebraisch abgeschlossen ist, hat f eine Nullstelle $a \in E$. Da a algebraisch über F ist, ist $a \in F$ nach Lemma 4.4. Es folgt die Behauptung. □

Definition 4.6. Sei $E : K$ eine Körpererweiterung. E heißt der *algebraische Abschluß von K* (oder auch die *algebraische Hülle von K*), falls $E : K$ algebraisch ist und E algebraisch abgeschlossen.

Satz 4.7. *Jeder Körper K besitzt einen algebraischen Abschluß.*

Beweis. Wir benötigen einige elementare Tatsachen aus der Mengenlehre. Zwei Mengen A und B heißen *gleichmächtig*, falls es eine Bijektion zwischen ihnen gibt. Man schreibt in diesem Fall $|A|=|B|$. Wir schreiben $|A|\leq|B|$, falls es eine Injektion von A nach B gibt. Man kann zeigen, daß $|A|=|B|$ zu $|A|\leq|B| \wedge |B|\leq|A|$ äquivalent ist. B ist *echt größer als* A, wenn $|A|\leq|B|$ gilt, jedoch nicht $|A|=|B|$. Es läßt sich zeigen, daß je zwei Mengen bezüglich $\leq$ vergleichbar sind.

Folgende mengentheoretische Tatsachen werden gebraucht:

1. Für jede Menge A existiert eine Menge B, die echt größer ist als A.
2. Sei K ein unendlicher Ring. Dann ist $|K[X]|=|K|$.
3. Ist $\mathcal{F}$ eine unendliche Familie endlicher Mengen und $|A|=|\mathcal{F}|$, so ist $|\bigcup \mathcal{F}|\leq|A|$.
4. Sei $A \subseteq B$ und B unendlich und echt größer als A. Dann ist $B \setminus A$ gleichmächtig mit B.

Um zu zeigen, daß K einen algebraischen Abschluß hat, genügt es nach Satz 4.5 zu zeigen, daß K überhaupt einen algebraisch abgeschlossenen Erweiterungkörper besitzt. Wir können annehmen, daß K unendlich ist, indem wir gegebenenfalls von K zu $K(X)$ übergehen. Wie man leicht sieht, ist $K(X)$ immer unendlich. Wegen 1. existiert eine Menge M, die echt größer ist als K. Wir können annehmen, daß K eine Teilmenge von M ist.

Betrachte die Menge

$$P := \{(E, \oplus, \odot) : E \subseteq M \wedge (E, \oplus, \odot) \text{ ist ein Körper } \wedge \\ (K, +, \cdot) \leq (E, \oplus, \odot) \wedge E : K \text{ ist algebraisch}\}.$$

P ist durch die Relation $\leq$ (die Teilkörperrelation) halbgeordnet.

Jede Kette in P besitzt eine obere Schranke. Sei nämlich

$$\{(E_i, \oplus_i, \odot_i) : i \in I\}$$

eine Kette in P. Wie man leicht nachrechnet, ist

$$\left(\bigcup_{i\in I} E_i, \bigcup_{i\in I} \oplus_i, \bigcup_{i\in I} \odot_i\right)$$

ein Element von P und eine obere Schranke der Kette. Nach dem Zornschen Lemma besitzt P also ein maximales Element E.

Wir zeigen, daß E algebraisch abgeschlossen ist. Da $E : K$ algebraisch ist, gibt es für jedes $a \in E$ ein Polynom $f \in K[X]$ mit $f(a) = 0$. Wegen 2. ist $|K[X]|=|K|$. Jedes nichtkonstante Polynom hat nur endlich viele Nullstellen. Nach 3. ist damit $|E|\leq|K|$, also $|E|=|K|$. Da M echt größer ist als K, und damit auch als E, ist $M \setminus E$ gleichmächtig mit M gemäß 4.

Falls E nicht algebraisch abgeschlossen ist, so existiert ein irreduzibles Polynom $f \in E[X]$, welches einen Grad > 1 hat. Sei F ein Erweiterungskörper von E, in dem f eine Nullstelle a hat. Dann ist $E(a)$ isomorph zu $E[X]/(f)$. Wegen 2. ist $|E(a)|=|E[X]/(f)|\leq|E|=|K|$. Damit ist in M genügend Platz, um eine zu $E(a)$ isomorphe Körpererweiterung von E unterzubringen. Ein Widerspruch zur Maximalität von E. □

Im Folgenden wird gezeigt, daß die algebraische Hülle eines Körpers bis auf Isomorphie eindeutig bestimmt ist. Wir beweisen einen etwas stärkeren Satz, der den Satz über die Eindeutigkeit des Zerfällungskörpers eines Polynoms verallgemeinert.

Definition 4.8. Sei K ein Körper und $M \subseteq K[X]$. Ein Erweiterungskörper E von K heißt *Zerfällungskörper von M über K*, falls jedes Polynom $f \in M$ über E in Linearfaktoren zerfällt und E aus K durch Adjunktion der Nullstellen der $f \in M$ entsteht.

Bemerkung 4.9. Ist E der Zerfällungskörper von $M \subseteq K[X]$ über K, so ist die Erweiterung $E : K$ algebraisch, da alle Elemente von E in einer endlichen Erweiterung von K enthalten sind. Außerdem existiert für alle $M \subseteq K[X]$ der Zerfällungskörper E von M über K. Wähle nämlich einen algebraischen Abschluß F von K und setze

$$E := K(\{\alpha \in F : \alpha \text{ ist Nullstelle eines } f \in M\}).$$

Lemma 4.10. *Sei K ein Körper. Der Zerfällungskörper E von $K[X]$ über K ist ein algebraischer Abschluß von K.*

Beweis. Nach Bemerkung 4.9 ist $E : K$ algebraisch. Außerdem zerfällt jedes Polynom $f \in K[X]$ über E in Linearfaktoren. Sei $g \in E[X]$ und α eine Nullstelle von g in einem Erweiterungskörper von E. Dann ist α algebraisch über E und damit auch über K. Also existiert ein Polynom $f \in K[X]$, dessen Nullstelle α ist. Nach Wahl von E gilt dann $\alpha \in E$. Also ist E algebraisch abgeschlossen. □

Satz 4.11. *Seien K und K' Körper und $\varphi : K \to K'$ ein Körperisomorphismus. $\overline{\varphi} : K[X] \to K'[X]$ sei der von φ induzierte Isomorphismus zwischen $K[X]$ und $K'[X]$. Weiter sei $M \subseteq K[X]$ und $M' := \overline{\varphi}[M]$.*

Sind E und E' Zerfällungskörper von M beziehungsweise M' über K beziehungweise K', so läßt sich φ zu einem Isomorphismus $\psi : E \to E'$ fortsetzen.

Aus diesem Satz erhält man sofort

Folgerung 4.12. *Sei K ein Körper und $M \subseteq K[X]$. Dann ist der Zerfällungskörper von M über K bis auf Isomorphie eindeutig bestimmt. Insbesondere ist der algebraische Abschluß von K als Zerfällungskörper von $K[X]$ über K bis auf Isomorphie eindeutig bestimmt.*

Beweis von Satz 4.11. Sei H die Menge aller injektiven Homomorphismen von einem Zwischenkörper von $E : K$ nach E', die φ fortsetzen. H ist geordnet durch $\subseteq$. (Beachte, daß für $\sigma, \tau \in H$ genau dann $\sigma \subseteq \tau$ gilt, wenn τ eine Fortsetzung von σ ist.)

Wie man leicht nachrechnet ist für jede Kette $(\sigma_i)_{i\in I}$ in H die Vereinigung $\bigcup_{i\in I} \sigma_i$ ein injektiver Homomorphismus von einem Zwischenkörper von $E : K$ nach E', der φ fortsetzt, also ein Element von H. Nach dem Zornschen Lemma hat H ein maximales Element $\psi : L \to E'$, wobei L ein Zwischenkörper von $E : K$ ist.

Wir zeigen $L = E$. Angenommen $L \neq E$. Dann existiert ein $\alpha \in E \setminus L$, das Nullstelle eines $f \in M$ ist. Offenbar ist α algebraisch über L. Sei $\overline{\psi}$ die Fortsetzung von ψ auf $L[X]$. (Die Funktionswerte von $\overline{\psi}$ liegen also in $E'[X]$.) Wie man leicht sieht, ist

$$L(\alpha) \cong L[X]/(\mathrm{Irr}(\alpha, L)) \cong \overline{\psi}[L[X]]/(\overline{\psi}(\mathrm{Irr}(\alpha, L))) \cong \psi[L](\alpha'),$$

wobei α' eine Nullstelle von $\overline{\psi}(\mathrm{Irr}(\alpha, L))$ in einem Erweiterungskörper von $\psi[L]$ ist. Der kanonische Isomorphismus, den man dabei zwischen $L(\alpha)$ und $\psi[L](\alpha')$ erhält, ist eine Fortsetzung von ψ.

Wegen $\mathrm{Irr}(\alpha, L)|f$ in $L[X]$ gilt $\overline{\psi}(\mathrm{Irr}(\alpha, L))|\overline{\psi}(f) = \overline{\varphi}(f)$ in $\overline{\psi}[L[X]] = \psi[L][X]$. Wegen $\overline{\varphi}(f) \in M'$ ist $\alpha' \in E'$ und damit $\psi[L](\alpha') \subseteq E'$. Also hat ψ eine echte Fortsetzung in H. Ein Widerspruch zur Maximalität von ψ.

Schließlich ist ψ auch surjektiv: Da E alle Nullstellen aller $f \in M$ enthält, enthält $\psi[E]$ alle Nullstellen aller $f' \in M'$. Da aber E' durch Adjunktion der Nullstellen der $f' \in M'$ zu K' entsteht, folgt daraus $\psi[E] = E'$. □

4.2. **Separable und inseparable Körpererweiterungen.**

Definition 4.13. Sei $E : K$ eine Körpererweiterung.

(i) $\alpha \in E$ heißt *inseparabel über* K, falls α algebraisch über K ist, aber nicht separabel.
(ii) $E : K$ heißt *inseparabel*, falls $E : K$ algebraisch ist, aber nicht separabel.
(iii) $E : K$ heißt *rein inseparabel*, falls jedes $\alpha \in E \setminus K$ inseparabel über K ist.
(iv) $\alpha \in E$ heißt *rein inseparabel über* K, falls $K(\alpha)$ rein inseparabel ist.

Satz 4.14. *Sei $E : K$ eine Körpererweiterung. Dann ist*

$$H_s(E : K) := \{\alpha \in E : \alpha \text{ ist separabel über } K\}$$

ein Zwischenkörper von $E : K$, nämlich die separable Hülle von K in E. *Inbesondere ist für jedes $M \subseteq E$ die Erweiterung $K(M) : K$ genau dann separabel, wenn jedes Element von M separabel über K ist.*

Beweis. Seien $\alpha, \beta \in H_s(E : K)$, $\beta \neq 0$. Dann sind $\mathrm{Irr}(\alpha, K)$ und $\mathrm{Irr}(\beta, K)$ separabel. Also ist der Zerfällungskörper von $\mathrm{Irr}(\alpha, K) \cdot \mathrm{Irr}(\beta, K)$ galoissch über K und damit auch separabel über K. Also sind $\alpha \cdot \beta$, $\alpha + \beta$, $\frac{\alpha}{\beta}$ und $\alpha - \beta$ separabel über K. Damit ist $H_s(E : K)$ ein Körper. □

Satz 4.15. *Sei $E : K$ eine Körpererweiterung und $p \neq 0$ die Charakteristik von K. Weiter sei $\alpha \in E$ algebraisch über K und $f := \mathrm{Irr}(\alpha, K)$. Angenommen f ist ein Polynom in X^{p^e}, aber nicht in $X^{p^{e+1}}$, etwa $f(X) = g(X^{p^e})$. Dann gilt:*

(i) *e ist die kleinste Zahl derart, daß α^{p^e} separabel über K ist. Insbesondere ist α genau dann separabel über K, wenn $e = 0$ ist.*
(ii) *g ist irreduzibel und separabel. Sind $\beta_1, \ldots, \beta_r$ die paarweise verschiedenen Nullstellen von g im Zerfällungskörper von g, so gilt im Zerfällungskörper von f die Gleichung $f = (X - \alpha_1)^{p^e} \ldots (X - \alpha_r)^{p^e}$ für eindeutig bestimmte α_i mit $\alpha_i^{p^e} = \beta_i$. Insbesondere haben alle Nullstellen von f dieselbe Vielfachheit.*
(iii) *Ist K endlich, so gilt stets $e = 0$.*

Beweis. (i) Mit f ist auch g irreduzibel in $K[X]$, da

$$\varphi : K[X] \to K[X]; h(X) \mapsto h(X^{p^e})$$

ein Homomorphismus ist und eine Zerlegung von g somit auch eine Zerlegung von f liefert. Nach Definition von e ist $g' \neq 0$. Damit ist g separabel. Offenbar ist α^{p^e} eine Nullstelle von g. Also ist α^{p^e} separabel über K.

Für alle $i < e$ ist α^{p^i} eine Nullstelle von h, falls $h(X^{p^i}) = f(X)$ ist. Mit dem gleichen Argument wie für die Irreduzibilität von g sieht man, daß h irreduzibel ist. Wegen $i < e$ ist h ein Polynom in X^p. Damit gilt $h' = 0$. Also ist h nicht separabel. Es folgt, daß α^{p^i} nicht separabel ist.

(ii) Es gilt

$$f(X) = g(X^{p^e}) = (X^{p^e} - \beta_1) \ldots (X^{p^e} - \beta_r).$$

Sei α_i Nullstelle von $X^{p^e} - \beta_i$. Dann ist

$$X^{p^e} - \beta_i = X^{p^e} - \alpha_i^{p^e} = (X - \alpha_i)^{p^e}$$

nach den binomischen Regeln in kommutativen Ringen der Charakteristik p. □

Im Folgenden wird gezeigt, daß mit den Körpererweiterungen $E : L$ und $L : K$ auch $E : K$ separabel ist. Wir benötigen dazu

Lemma 4.16. *Sei $E : K$ eine algebraische Körpererweiterung und $\alpha \in E$. Sei $p \neq 0$ die Charakteristik von K. Dann gilt:*

(i) *α ist genau dann separabel über K, wenn $K(\alpha) = K(\alpha^p)$ gilt.*
(ii) *Ist $E : K$ separabel, so ist $E = K(E^p)$ mit $E^p := \{\alpha^p : \alpha \in E\}$. Ist $E : K$ endlich und $E = K(E^p)$, so ist $E : K$ separabel.*

Beweis. (i) Sei α nicht separabel über K. Dann ist nach Satz 4.15 $\mathrm{Irr}(\alpha, K)$ ein Polynom in X^p, etwa $\mathrm{Irr}(\alpha, K) = g(X^p)$. α^p ist Nullstelle von g. Damit gilt

$$[K(\alpha^p) : K] \leq \mathrm{grad}(g) < \mathrm{grad}(\mathrm{Irr}(\alpha, K)) = [K(\alpha) : K].$$

Sei nun α separabel über K. Dann ist α separabel über $K(\alpha^p)$. Also besitzt $\mathrm{Irr}(\alpha, K(\alpha^p))$ keine mehrfachen Nullstellen. Andererseits ist α Nullstelle von $X^p - \alpha^p \in K(\alpha^p)[X]$. Es gilt $X^p - \alpha^p = (X - \alpha)^p$. Also ist $\mathrm{Irr}(\alpha, K(\alpha^p)) = X - \alpha$ und damit $\alpha \in K(\alpha^p)$, also $K(\alpha) = K(\alpha^p)$.

(ii) Sei $E : K$ separabel. Offenbar gilt $K(E^p) \leq E$. Wir zeigen $E \leq K(E^p)$. Sei $\alpha \in E$. Wegen (i) ist $K(\alpha) = K(\alpha^p) \leq K(E^p)$. Also gilt $E \leq K(E^p)$.

Sei nun $E = K(E^p)$ und $E : K$ endlich. Es ist zu zeigen, daß $E : K$ separabel ist. Dazu zeigen wir zunächst

($*$) Sind $\alpha_1, \ldots, \alpha_m \in E$ linear unabhängig über K, so auch $\alpha_1^p, \ldots, \alpha_m^p$.

Da $E : K$ endlich ist, können wir annehmen, daß die α_i bereits eine Basis von E über K bilden. Es genügt nun zu zeigen, daß die α_i^p den K-Vektorraum E erzeugen. Es ist klar, daß die α_i^p den K^p-Vektorraum E^p erzeugen. $E = K(E^p)$ enthält aber nur K-Linearkombinationen von Elementen aus E^p. Also erzeugen die α_i den K-Vektorraum E. Das zeigt ($*$).

Angenommen es gibt ein $\alpha \in E$, welches nicht separabel über K ist. Nach Satz 4.15 ist $\mathrm{Irr}(\alpha, K)$ ein Polynom in X^p, etwa $\mathrm{Irr}(\alpha, K) = a_0 + a_1 X^p + \cdots + a_n X^{pn}$. Dann sind $1, \alpha^p, \ldots, \alpha^{pn}$ linear abhängig über K. Nach ($*$) sind auch $1, \alpha, \ldots, \alpha^n$ linear abhängig über K. Das ist aber nicht möglich, da $\mathrm{grad}(\mathrm{Irr}(\alpha, K)) = pn > n$ ist. □

Satz 4.17. *Seien $K \leq L \leq E$ Körper, $L : K$ separabel und $\alpha \in E$ separabel über L. Dann ist α auch separabel über K.*

Beweis. Hat K die Charakteristik 0, so ist jede Körpererweiterung von K separabel. Wir können also annehmen, daß K die Charakteristik $p \neq 0$ hat. Sei $\mathrm{Irr}(\alpha, L) = a_0 + a_1 X + \cdots + a_n X^n \in L[X]$. Nach Voraussetzung ist $\mathrm{Irr}(\alpha, L)$ separabel. Betrachte $L_0 := K(a_0, \ldots, a_n)$. Wegen $L_0 \leq L$ ist $L_0 : K$ separabel. Nach Lemma 4.16 ist $L_0 = K(L_0^p)$. Betrachte $L_1 := L_0(\alpha)$.

Dann ist $L_1 : L_0$ separabel, da $\mathrm{Irr}(\alpha, L_0) = \mathrm{Irr}(\alpha, L)$ separabel ist. Nach Lemma 4.16 ist damit $L_1 = L_0(L_1^p)$. Wegen $L_0 \leq L_1$ folgt

$$L_1 = K(L_0^p)(L_1^p) = K(L_1^p).$$

Da $L_1 : K$ endlich ist, liefert eine weitere Anwendung von Lemma 4.16, daß $L_1 : K$ separabel ist. Damit ist α separabel über K. □

Definition und Bemerkung 4.18. Sei $E : K$ eine Körpererweiterung, $H_s(E : K)$ die separable Hülle von K in E und $H_a(E : K)$ der algebraische Abschluß von K in E. Dann gilt

$$K \leq H_s(E : K) \leq H_a(E : K) \leq E.$$

$[E : K]_s := [H_s(E : K) : K]$ heißt *Separabilitätsgrad von* $E : K$. $[E : K]_i := [H_a(E : K) : H_s(E : K)]$ heißt *Inseparabilitätsgrad von* $E : K$. $H_s(E : K)$ ist eine separable Erweiterung von K. $H_a(E : K) : H_s(E : K)$ ist eine rein inseparable Erweiterung. Jedes $\alpha \in E \setminus H_a(E : K)$ ist transzendent über K.

Satz 4.19. *Sei K ein Körper der Charakteristik $p \neq 0$, E ein Erweiterungskörper von K und $\alpha \in E$. Dann gilt:*

(i) *Falls α rein inseparabel über K ist, so hat* $\mathrm{Irr}(\alpha, K)$ *die Form $X^{p^e} - b$.*
(ii) *Ist α Nullstelle von $X^{p^e} - b \in K[X]$, so ist α rein inseparabel über K.*

Beweis. (i) Wir können annehmen, daß α kein Element von K ist. Sei e so gewählt, daß $\mathrm{Irr}(\alpha, K)$ ein Polynom in X^{p^e} ist, etwa $\mathrm{Irr}(\alpha, K) = g(X^{p^e})$, aber nicht in $X^{p^{e+1}}$. Wir zeigen, daß g den Grad 1 hat.

Angenommen nicht. Nach Satz 4.15 ist α^{p^e} separabel über K. Offenbar gilt $\alpha^{p^e} \in K(\alpha)$. Da g aber kein lineares Polynom ist, gilt $\alpha^{p^e} \notin K$. Das ist ein Widerspruch zu der Vorausetzung, daß α rein inseparabel über K ist.

(ii) Sei $c \in K(\alpha) \setminus K$, etwa $c = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ mit $a_i \in K$ für alle i. Wir zeigen, daß c nicht separabel über K ist. Wegen $\alpha^{p^e} = b \in K$ gilt

$$d := c^{p^e} = a_0^{p^e} + a_1^{p^e}\alpha^{p^e} + \cdots + a_n^{p^e}\alpha^{p^e \cdot n} \in K.$$

Also ist c Nullstelle von $X^{p^e} - d \in K[X]$. Wegen $X^{p^e} - d = (X - c)^{p^e}$ hat $X^{p^e} - d$ nur die Nullstelle c. Damit ist c inseparabel über K. □

Folgerung 4.20. *Sei K ein Körper der Charakteristik $p \neq 0$, E Erweiterungskörper von K und $\alpha \in E$. Dann gilt:*

(i) *α ist genau dann rein inseparabel über K, wenn α p^e-te Wurzel (für geeignetes $e \in \mathbb{N}$) eines Elementes von K ist.*
(ii) *$E : K$ ist genau dann rein inseparabel, wenn E nur p^e-te Wurzeln (für geeignete $e \in \mathbb{N}$) von Elementen aus K enthält.*

Folgerung 4.21. *Seien $K \leq M \leq E$ Körper und $\alpha \in E$. Dann gilt:*

(i) *Falls α rein inseparabel über K ist, so auch über M.*
(ii) *Sind $E : M$ und $M : K$ rein inseparabel, so auch $E : K$.*

Beweis. Hat K die Charakteristik 0, so ist K vollkommen und die Behauptungen sind trivialer Weise erfüllt. Wir können also annehmen, daß K die Charakteristik $p \neq 0$ hat. (i) und (ii) folgen nun unmittelbar aus den entsprechenden Teilen von Folgerung 4.20. □

Definition und Bemerkung 4.22. Sei $E : K$ eine Körpererweiterung. Dann ist

$$H_r(E : K) := \{\alpha \in E : \alpha \text{ ist rein inseparabel über } K\}$$

ein Körper, nämlich der *rein inseparable* oder auch *perfekte Abschluß von K in E*.

Beweis. Übung. □

Satz 4.23. *Sei K ein Körper der Charakteristik $p \neq 0$ und $E : K$ normale Körpererweiterung. Dann gilt:*

(i) *$E : H_r(E : K)$ ist normal und separabel.*
(ii) *$E = H_r(E : K) \cdot H_s(E : K)$ und $K = H_r(E : K) \cap H_s(E : K)$.*
(iii) *$H_s(E : K) : K$ ist normal und separabel.*
(iv) *Es ist*

$$\mathrm{Gal}(E : H_r(E : K)) = \mathrm{Gal}(E : K) \cong \mathrm{Gal}(H_s(E : K) : K).$$

Insbesondere ist $[E : H_r(E : K)] = [H_s(E : K) : K]$, falls $E : K$ endlich ist.

Beweis. (i) und (ii): Übung. (iii) Sei $\alpha \in H_s(E : K)$. Da $E : K$ normal ist, liegen alle Nullstellen von $\mathrm{Irr}(\alpha, K)$ in E. Wegen $\alpha \in H_s(E : K)$ besitzt $\mathrm{Irr}(\alpha, K)$ nur einfache Nullstellen. Also liegen alle Nullstellen von $\mathrm{Irr}(\alpha, K)$ in $H_s(E : K)$.

(iv) Sei $\varphi \in \mathrm{Gal}(E : K)$ und $\alpha \in H_r(E : K)$. Nach Satz 4.19 hat $\mathrm{Irr}(\alpha, K)$ die Form $X^{p^e} - b = (X - \alpha)^{p^e}$. Da $\varphi(\alpha)$ Nullstelle von $\mathrm{Irr}(\alpha, K)$ ist und $\mathrm{Irr}(\alpha, K)$ nur die eine Nullstelle α hat, ist $\varphi(\alpha) = \alpha$. Also liegen alle Elemente von $H_r(E : K)$ im Fixpunktkörper von $\mathrm{Gal}(E : K)$. Also ist $\mathrm{Gal}(E : K) = \mathrm{Gal}(E : H_r(E : K))$. Das Übrige liefert der Translationssatz zusammen mit (ii). □

Lemma 4.24. *Sei $E : K$ eine endliche und normale Körpererweiterung und M ein Zwischenkörper. Weiter sei $M_s := H_s(M : K)$. Dann existieren genau $[M_s : K]$ injektive Körperhomomorphismen von M nach E, die K elementweise festlassen.*

Beweis. Nach Satz 4.23 ist $H_s(E : K) : K$ normal und separabel. Da $E : K$ endlich ist, ist auch $M_s : K$ endlich. Nach dem Satz vom primitiven Element existiert ein $\alpha \in M_s$ mit $M_s = K(\alpha)$. $\mathrm{Irr}(\alpha, K)$ hat genau $[M_s : K]$ Nullstellen in $H_s(E : K)$. Sei $\beta \in H_s(E : K)$ eine Nullstelle von $\mathrm{Irr}(\alpha, K)$. Wegen $K(\alpha) \cong K[X]/(\mathrm{Irr}(\alpha, K)) \cong K(\beta)$ existiert genau ein injektiver Homomorphismus $\varphi : M_s \to H_s(E : K)$ mit $\varphi(\alpha) = \beta$, der K elementweise festläßt. Da alle Nullstellen β von $\mathrm{Irr}(\alpha, K)$ in $H_s(E : K)$ liegen, ist das Bild eines jeden injektiven Homomorphismus' von $M_s = K(\alpha)$ nach E ein Unterkörper von $H_s(E : K)$. Also gibt es genau $[M_s : K]$ injektive Homomorphismen von M_s nach E.

Sei φ injektiver Homomorphismus von M_s nach E. Da $E : K$ endlich und normal ist, ist E Zerfällungskörper über K. Nach Satz 4.11 läßt sich φ zu einem Automorphismus von E fortsetzen. Insbesondere läßt φ sich zu einem injektiven Homomorphismus $\overline{\varphi} : M \to E$ fortsetzen. $\overline{\varphi}$ ist dabei eindeutig bestimmt.

Sei nämlich $\alpha \in M \setminus M_s$. Da $M : M_s$ rein inseparabel ist, hat $\mathrm{Irr}(\alpha, M_s)$ nur die Nullstelle α. Also ist die Fortsetzung der Identität von M_s auf M eindeutig bestimmt. Daraus ergibt sich die Eindeutigkeit von $\overline{\varphi}$.

Insgesamt ergibt sich, daß es genau $[M_s : K]$ injektive Homomorphismen von M nach E gibt. □

Analog zu Lemma 4.24 erhält man

Lemma 4.25. *Seien $K \leq M_1 \leq M_2 \leq E$ Körper und $E : K$ endlich und normal. Ist $\varphi : M_1 \to E$ ein injektiver Homomorphismus, der K elementweise festläßt, so läßt sich φ auf genau $[H_s(M_2 : M_1) : M_1]$ Arten zu einem injektivem Homomorphismus von M_2 nach E fortsetzen.*

Satz 4.26. *Seien $K \leq L \leq E$ Körper und $E : K$ endlich. Dann gilt:*

(i) $[E : K]_s = [E : L]_s \cdot [L : K]_s$
(ii) $[E : K]_i = [E : L]_i \cdot [L : K]_i$

Beweis. Nach der Körpergradformel genügt es, (i) zu zeigen. Sei $\overline{E}$ eine endliche Erweiterung von E, die normal über K ist. Wegen der Endlichkeit von $E : K$ existiert eine solche Erweiterung. Nach Lemma 4.24 existieren genau $[E : K]_s = [H_s(E : K) : K]$ injektive Homomorphismen von E nach $\overline{E}$, die K elementweise festlassen. Ebenso existieren genau $[L : K]_s$ injektive Homomorphismen von L nach $\overline{E}$, die K elementweise festlassen. Nach Lemma 4.25 läßt sich jeder dieser Homomorphismen auf genau $[E : L]_s$ Arten zu einem injektiven Homomorphismus von E nach $\overline{E}$ fortsetzen. Es gibt also genau $[E : L]_s \cdot [L : K]_s$ injektive Homomorphismen von E nach $\overline{E}$, die K elementweise festlassen. Lemma 4.24 liefert nun (i). □

4.3. **Transzendente Körpererweiterungen.**

Definition 4.27. Sei $L : K$ eine Körpererweiterung, $a_1, \ldots, a_n \in L$ und $S \subseteq L$.

(i) $a_1, \ldots, a_n$ sind *algebraisch unabhängig* (oder auch *transzendent*) *über* K, falls $f(a_1, \ldots, a_n) \neq 0$ für alle $f \in K[X_1, \ldots, X_n]$ mit $f \neq 0$ gilt. (Sonst sind $a_1, \ldots, a_n$ *algebraisch abhängig über* K.)
(ii) S ist *algebraisch unabhängig* (oder auch *transzendent*) *über* K, falls jede endliche Teilmenge von S transzendent über K ist.
(iii) S ist eine *Transzendenzbasis von* $L : K$, falls S über K transzendent ist und $L : K(S)$ algebraisch.
(iv) $L : K$ ist *rein transzendent*, falls es eine Transzendenzbasis B von $L : K$ gibt, für die $L = K(B)$ gilt.
(v) Eine Transzendenzbasis B von $L : K$ heißt separierend, falls $L : K(B)$ separabel ist.

Bemerkung 4.28. Sei K ein Körper. Dann ist $\{X\}$ eine separierende Transzendenzbasis von $K(X) : K$. Für alle $n > 0$ ist $\{X^n\}$ ebenfalls Transzendenzbasis von $K(X) : K$, da $K(X) : K(X^n)$ algebraisch ist. Hat K die Charakteristik $p \neq 0$ und ist n ein Vielfaches von p, so ist $\{X^n\}$ keine separierende Transzendenzbasis von $K(X) : K$, da $K(X) : K(X^n)$ nicht separabel ist.

Lemma 4.29. *Sei $L : K$ eine rein transzendente Körpererweiterung und B eine Transzendenzbasis von $L : K$ mit $L = K(B)$. Dann gilt:*

(i) *Seien $b_1, \ldots, b_n$ paarweise verschiedene Elemente von B. Dann ist die Abbildung*

$$\varphi : K(X_1, \ldots, X_n) \to K(b_1, \ldots, b_n); \frac{f}{g} \mapsto \frac{f(b_1, \ldots, b_n)}{g(b_1, \ldots, b_n)}$$

ein Isomorphismus.
(ii) *Die Elemente von L haben die Form $f(b_1, \ldots, b_n)/g(b_1, \ldots, b_n)$, wobei f und g Polynome aus $K(X_1, \ldots, X_n)$ sind, $g \neq 0$ und $b_1, \ldots, b_n \in B$ paarweise verschieden.*
(iii) *Jedes $\alpha \in L \setminus K$ ist transzendent über K.*

Beweis. (i) Wegen der algebraischen Unabhängigkeit der b_i über K ist für jedes $g \neq 0$ auch $g(b_1, \ldots, b_n) \neq 0$. Damit ist φ wohldefiniert. Es ist klar, daß φ ein surjektiver Homomorphismus ist. Wegen der algebraischen Unabhängigkeit der b_i über K enthält der Kern von φ nur 0. Damit ist φ ein Isomorphismus.

(ii) Für jedes $\alpha \in L$ existieren paarweise verschiedene $b_1, \ldots, b_n \in B$ mit $\alpha \in K(b_1, \ldots, b_n)$. Die Behauptung folgt nun aus (i).

(iii) Sei

$$\alpha = \frac{f(b_1, \ldots, b_n)}{g(b_1, \ldots, b_n)} \in L \setminus K$$

mit $f, g \in K[X_1, \ldots, X_n]$, $g \neq 0$ und $b_1, \ldots, b_n \in B$ paarweise verschieden. Nach Satz 21.6, Einführung in die Algebra und Zahlentheorie, ist der Polynomring $K[X_1, \ldots, X_n]$ ein ZPE-Ring. Nach eventuellem Kürzen können wir annehmen, daß f und g teilerfremd sind.

Angenommen,

$$a_0 + a_1 \frac{f(b_1, \ldots, b_n)}{g(b_1, \ldots, b_n)} + \cdots + a_m \frac{f^m(b_1, \ldots, b_n)}{g^m(b_1, \ldots, b_n)} = 0$$

für gewisse $a_0, \ldots, a_m \in K$. Nach (i) ist das äquivalent dazu, daß in in dem Körper $K(X_1, \ldots, X_n)$ die Gleichung

$$a_0 + a_1 \frac{f}{g} + \cdots + a_m \frac{f^m}{g^m} = 0$$

gilt. Multiplikation mit g^m liefert, daß g ein Teiler von f^m ist. Da 1 der größte gemeinsame Teiler von f und g in $K[X_1, \ldots, X_n]$ ist, folgt $g \in K$. Wir können daher $g = 1$ annehmen. Also ist $a_0 + a_1 f + \cdots + a_m f^m = 0$. Wegen $\alpha \notin K$ ist f aber nicht konstant. Ein Widerspruch. □

Lemma 4.30. *Sei $L : K$ eine Körpererweiterung und $B \subseteq L$ transzendent über K. Dann ist B genau dann Transzendenzbasis von $L : K$, wenn B eine maximal transzendente Menge über K ist.*

Beweis. Sei B eine Transzendenzbasis von $L : K$ und $\alpha \in L \setminus B$. Dann ist α algebraisch über $K(B)$. Also existiert ein von 0 verschiedenes Polynom $f \in K(B)[X]$ mit $f(\alpha) = 0$, etwa $f = a_0 + \cdots + a_n X^n$. Nach Lemma 4.29 hat a_i die Form $f_i(b_1, \ldots, b_n)/g_i(b_1, \ldots, b_n)$ für gewisse $f_i, g_i \in K[X_1, \ldots, X_n]$ mit $g_i \neq 0$ und gewisse paarweise verschiedene $b_1, \ldots, b_n \in B$. Wir können annehmen, daß m und die b_j nicht von i abhängen. Multipliziert man die Gleichung $f(\alpha) = 0$ mit dem Produkt der Nenner der a_i, so erhält man eine Gleichung, die zeigt, daß α und $b_1, \ldots, b_n$ algebraisch abhängig über K sind. Also ist B eine maximale transzendente Menge über K.

Sei nun B eine maximale transzendente Menge über K und $\alpha \in L$. Ist $\alpha \in B$, so ist α algebraisch über $K(B)$. Ist $\alpha \notin B$, so ist $B \cup \{\alpha\}$ wegen der Maximalität von B algebraisch abhängig über K. Also existieren $b_1, \ldots, b_n \in B$ und ein Polynom $f \in K[X_1, \ldots, X_{n+1}]$ mit $f \neq 0$ und $f(b_1, \ldots, b_n, \alpha) = 0$. Nun ist $g(X) := f(b_1, \ldots, b_n, X) \in K(B)[X]$ und $g(\alpha) = 0$. Wegen der algebraischen Unabhängigkeit der b_i über K ist $g \neq 0$. Also ist α algebraisch über $K(B)$. Das zeigt, daß B eine Transzendenzbasis von $L : K$ ist. □

Satz 4.31. *Sei $L : K$ eine Körpererweiterung und $A \subseteq L$ transzendent über K. Dann hat $L : K$ eine Transzendenzbasis B mit $A \subseteq B$. Insbesondere hat jede Körpererweiterung eine Transzendenzbasis.*

Beweis. Betrachte die Menge

$$H := \{B \subseteq L : A \subseteq B \text{ und } B \text{ ist transzendent über } K\}.$$

H ist durch $\subseteq$ halbgeordnet. Wegen $A \in H$ ist $H \neq \emptyset$. Wie man leicht sieht, ist die Vereinigung einer Kette in H wieder ein Element von H. Jede Kette in H hat also eine obere Schranke in H. Nach dem Zornschen Lemma existiert ein maximales Element B von H. Nach Lemma 4.30 ist B eine Transzendenzbasis von $L : K$. Nach Definition von H ist $A \subseteq B$. □

Folgerung 4.32. *Für jede Körpererweiterung $L : K$ existiert ein Zwischenkörper M, so daß $L : M$ algebraisch ist und $M : K$ rein transzendent.*

Satz 4.33. *Sei $\{b_1, \ldots, b_n\}$ eine Transzendenzbasis der Körpererweiterung $L : K$ mit paarweise verschiedenen b_i. Dann hat jede Transzendenzbasis von $L : K$ die Mächtigkeit n.*

Der Satz gilt auch im Unendlichen: Alle Transzendenzbasen einer festen Körpererweiterung haben dieselbe Mächtigkeit.

Beweis von Satz 4.33. Wir benutzen ein Analogon zum Steinitzschen Austauschsatz in der linearen Algebra:

Behauptung 4.34. Seien $a_1, \ldots, a_r \in L$ algebraisch unabhängig über K und $r \leq n$. Bei geeigneter Numerierung der b_i ist dann

$$\{a_1, \ldots, a_r, b_{r+1}, \ldots, b_n\}$$

eine Transzendenzbasis von $L : K$.

Aus dieser Behauptung folgt sofort der Satz: Wir können annehmen, daß n die minimale Mächtigkeit einer Transzendenzbasis von $L : K$ ist. Sei B eine weitere Transzendenzbasis von $L : K$. Wegen der Minimalität von n existieren paarweise verschiedene $a_1, \ldots, a_n \in B$. Die a_i sind algebraisch unabhängig, da B eine Transzendenzbasis ist. Gemäß der Behauptung ist $\{a_1, \ldots, a_n\}$ bereits eine Transzendenzbasis von $L : K$. Da Transzendenzbasen maximal algebraisch unabhängig sind, folgt $B = \{a_1, \ldots, a_n\}$.

Wir beweisen die Behauptung durch Induktion über r. Für $r = 0$ ist nichts zu zeigen. Sei also $r > 0$ und die Behauptung bereits gezeigt für $r - 1$. Seien $a_1, \ldots, a_r \in L$ algebraisch unabhängig über K. Nach Induktionsannahme ist bei geeigneter Numerierung der b_i die Menge $\{a_1, \ldots, a_{r-1}, b_r, \ldots, b_n\}$ eine Transzendenzbasis von $L : K$. Also ist a_r algebraisch über

$$K(a_1, \ldots, a_{r-1}, b_r, \ldots, b_n).$$

Insbesondere sind $a_r, b_r, \ldots, b_n$ algebraisch abhängig über $K(a_1, \ldots, a_{r-1})$. Also existiert ein nichtkonstantes Polynom

$$f \in K(a_1, \ldots, a_{r-1})[X, Y_r, \ldots, Y_n]$$

mit $f(a_r, b_r, \ldots, b_n) = 0$.

Wegen der algebraischen Unabhängigkeit von $a_1, \ldots, a_{r-1}, b_r, \ldots, b_n$ sind $b_r, \ldots, b_n$ algebraisch unabhängig über $K(a_1, \ldots, a_{r-1})$. Daher kommt X echt in f vor. Da a_r über K transzendent ist, kommt auch ein Y_i, $r \leq i \leq n$, echt in f vor. O.B.d.A. komme Y_r in f echt vor.

Wir zeigen, daß $L : K(a_1, \ldots, a_r, b_{r+1}, \ldots, b_n)$ algebraisch ist. Wegen $f(a_r, b_r, \ldots, b_n) = 0$ ist b_r algebraisch über $K(a_1, \ldots, a_r, b_{r+1}, \ldots, b_n)$. Also ist

$$K(a_1, \ldots, a_r, b_r, \ldots, b_n) : K(a_1, \ldots, a_r, b_{r+1}, \ldots, b_n)$$

algebraisch. Da $L : K(a_1, \ldots, a_{r-1}, b_r, \ldots, b_n)$ algebraisch ist, ist auch

$$L : K(a_1, \ldots, a_r, b_r, \ldots, b_n)$$

algebraisch. Also ist $L : K(a_1, \ldots, a_r, b_{r+1}, \ldots, b_n)$ algebraisch.

Schließlich sind $a_1, \ldots, a_r, b_{r+1}, \ldots, b_n$ algebraisch unabhängig über K: Angenommen nicht. Dann existiert ein nichtkonstantes Polynom

$$g \in K[X_1, \ldots, X_n]$$

mit $g(a_1, \ldots, a_r, b_{r+1}, \ldots, b_n) = 0$. Wegen der algebraischen Unabhängigkeit von $a_1, \ldots, a_{r-1}, b_{r+1}, \ldots, b_n$ über K kommt X_r echt in g vor. Also ist a_r algebraisch über $K(a_1, \ldots, a_{r-1}, b_{r+1}, \ldots, b_n)$. Damit ist aber

$$L : K(a_1, \ldots, a_{r-1}, b_{r+1}, \ldots, b_n)$$

algebraisch. Also ist auch b_r algebraisch über $K(a_1, \ldots, a_{r-1}, b_{r+1}, \ldots, b_n)$, im Widerspruch dazu, daß $\{a_1, \ldots, a_{r-1}, b_r, \ldots, b_n\}$ eine Transzendenzbasis von $L : K$ ist. □

Nach Satz 4.33 ist folgende Definition sinnvoll:

Definition 4.35. Sei $L : K$ eine Körpererweiterung und B eine Transzendenzbasis von $L : K$. Dann heißt $\mathrm{Trg}(L : K) := |B|$ der *Transzendenzgrad von* $L : K$.

Satz 4.36. *Seien $K \leq M \leq L$ Körper, A eine Transzendenzbasis von $L : M$ und B eine Transzendenzbasis von $M : K$. Dann ist $A \cup B$ eine Transzendenzbasis von $L : K$ und es gilt $A \cap B = \emptyset$. Insbesondere ist* $\mathrm{Trg}(L : K) = \mathrm{Trg}(L : M) + \mathrm{Trg}(M : K)$.

Beweis. Da zwar jedes $b \in B$ algebraisch über M ist, aber kein $a \in A$, gilt $A \cap B = \emptyset$. Wir zeigen, daß $A \cup B$ über K transzendent ist.

Angenommen, es gibt paarweise verschiedene $a_1, \ldots, a_n \in A$ und paarweise verschiedene $b_1, \ldots, b_m \in B$, so daß $a_1, \ldots, a_n, b_1, \ldots, b_m$ über K algebraisch abhängig sind. Dann existiert ein nichtkonstantes Polynom

$$f \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$$

mit $f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0$. Wegen der algebraischen Unabhängigkeit der b_j kommt mindestens ein X_i echt in f vor. Damit ist aber

$$g(X_1, \ldots, X_n) := f(X_1, \ldots, X_n, b_1, \ldots, b_m)$$

ein nichtkonstantes Polynom über M mit $g(a_1, \ldots, a_n) = 0$, im Widerspruch zur algebraischen Unabhängigkeit der a_i über M.

Es bleibt zu zeigen, daß $L : K(A \cup B)$ algebraisch ist. Sei $\alpha \in L$. Da A Transzendenzbasis von $L : M$ ist, ist α algebraisch über $M(A)$. Gelte etwa

$$c_0 + c_1\alpha + \cdots + c_r\alpha^r = 0$$

für gewisse $c_i \in M(A)$, die nicht alle 0 sind. Indem wir die c_i mit ihrem Hauptnenner multiplizieren, können wir annehmen, daß alle c_i bereits in $M[A]$ liegen.

Offenbar ist α algebraisch über $K(c_0, \ldots, c_r)$. Insbesondere ist α algebraisch über $K(c_0, \ldots, c_r, A \cup B)$. Um zu zeigen, daß α über $K(A \cup B)$ algebraisch ist, genügt es nun, die Algebraizität aller c_i über $K(A \cup B)$ zu zeigen.

Jedes c_i ist aber ein Polynom in endlich vielen Elementen von A mit Koeffizienten in einer Menge $\{m_1 \ldots, m_s\} \subseteq M$. Wir können annehmen, daß s und die m_j dabei nicht von i abhängen. Jedes m_j ist algebraisch über $K(B)$, da B eine Transzendenzbasis von $M : K$ ist. Damit ist die Körpererweiterung $K(m_1, \ldots, m_s, B) : K(B)$ algebraisch. Also ist auch

$$K(m_1, \ldots, m_s, A \cup B) : K(A \cup B)$$

algebraisch. Da aber alle c_i in $K(m_1, \ldots, m_s, A \cup B)$ liegen, ist schließlich auch $K(c_1, \ldots, c_r, A \cup B) : K(A \cup B)$ algebraisch. □

4.4. **Transzendente Zahlen.** *Transzendente Zahlen* sind diejenigen Elemente von $\mathbb{C}$, die transzendent über $\mathbb{Q}$ sind. Die komplexen Zahlen, die algebraisch über $\mathbb{Q}$ sind, heißen *algebraische Zahlen*. Beispiele reeller transzendenter Zahlen sind e und π.

Zunächst stellen wir fest, daß es unendlich viele reelle transzendente Zahlen gibt. Das wurde zuerst von Cantor gezeigt.

Satz 4.37. *Es gibt unendlich viele reelle transzendente Zahlen.*

Beweis. Bekanntlich ist $\mathbb{Q}$ abzählbar und $\mathbb{R}$ nicht. Es gibt auch nur abzählbar viele Polynome über $\mathbb{Q}$. Jedes Polynom über $\mathbb{Q}$ hat nur endlich viele Nullstellen. Also gibt es nur abzählbar viele Nullstellen von Polynomen über $\mathbb{Q}$. Jede algebraische Zahl ist aber Nullstelle eines Polynoms über $\mathbb{Q}$. Daher gibt es nur abzählbar viele algebraische Zahlen. Also sind überabzählbar viele reelle Zahlen transzendent. □

Der folgende Satz von Liouville liefert eine Möglichkeit, transzendente Zahlen zu erkennen.

Satz 4.38. *Ist $a \in \mathbb{R}$ irrational und algebraisch vom Grad m über $\mathbb{Q}$, so gibt es eine Konstante $c = c(a) \in \mathbb{R}$, so daß für alle $p, q \in \mathbb{Z}$ mit $q > 0$ gilt:*

$$\left| a - \frac{p}{q} \right| > \frac{c}{q^m}$$

Beweis. Sei $f \in \mathbb{Z}[X]$ ein irreduzibles Polynom mit $f(a) = 0$. Dann hat f den Grad m. Da $\mathbb{Q}$ die Charakteristik 0 hat, ist f separabel. Also ist a einfache Nullstelle von f. Damit gilt $f'(a) \neq 0$. Die Ableitung von f im Sinne der Algebra stimmt mit der Ableitung im Sinne der Analysis überein. Damit gibt es zu $\varepsilon := |f'(a)| > 0$ ein $\delta > 0$ mit

$$\left| \frac{f\left(\frac{p}{q}\right) - f(a)}{\frac{p}{q} - a} - f'(a) \right| < \varepsilon = |f'(a)| \tag{1}$$

für alle $p, q \in \mathbb{Z}$ mit $q \neq 0$ und $\left| \frac{p}{q} - a \right| \leq \delta$. Aus (1) folgt

$$\frac{1}{q^m} \leq \left| f\left(\frac{p}{q}\right) \right| < 2 \cdot |f'(a)| \cdot \left| \frac{p}{q} - a \right|.$$

Für alle $p, q \in \mathbb{Z}$ mit $q > 0$ und $\left| \frac{p}{q} - a \right| \leq \delta$ gilt nun

$$\left| \frac{p}{q} - a \right| > \frac{1}{2 \cdot |f'(a)|} \cdot \frac{1}{q^m}.$$

Für $p, q \in \mathbb{Z}$ mit $q > 0$ und $\left| \frac{p}{q} - a \right| > \delta$ gilt offenbar $\left| \frac{p}{q} - a \right| > \frac{\delta}{q^m}$. Also leistet $c := \min\left\{ \frac{1}{2 \cdot |f'(a)|}, \delta \right\}$ das Gewünschte. □

Folgerung 4.39. *Sei $a \in \mathbb{R}$. Gibt es zu jedem $n \in \mathbb{N}$ ganze Zahlen p und q mit $q \geq 2$, so daß $0 < \left| \frac{p}{q} - a \right| < \frac{1}{q^n}$ gilt, so ist a transzendent.*

Beweis. Sei $c > 0$ und $m > 0$. Wähle s so, daß $\frac{1}{2^s} < c$ gilt. Zu $n := m + s$ existieren $p, q \in \mathbb{Z}$ mit $q \geq 2$ und

$$0 < \left| a - \frac{p}{q} \right| < \frac{1}{2^s \cdot q^m} < \frac{c}{q^m}.$$

Damit folgt die Transzendenz von a aus Satz 4.38, falls a irrational ist.

Angenommen, a ist rational. Dann gibt es $r, s \in \mathbb{Z}$ mit $s > 0$ und $a = \frac{r}{s}$. Dann gilt für m mit $2^{m-1} > s$ und alle $p, q \in \mathbb{Z}$ mit $q \geq 2$

$$\left| a - \frac{p}{q} \right| = \left| \frac{rq - sp}{sq} \right| \geq \frac{1}{sq} \geq \frac{1}{2^{m-1} \cdot q} \geq \frac{1}{q^m}.$$

Das widerspricht aber der Voraussetzung. Damit ist a irrational und somit auch transzendent. □

Beispiel 4.40. Für $b \in \mathbb{Z}$ mit $b \geq 2$ erfüllt

$$a := \sum_{i=1}^{\infty} \frac{1}{b^{i!}} = \frac{1}{b} + \frac{1}{b^2} + \frac{1}{b^6} + \frac{1}{b^{24}} + \dots$$

die Voraussetzungen von Folgerung 4.39 und ist damit transzendent.

Ohne Beweis zitieren wir den folgenden Satz von Thue, Siegel und Roth:

Satz 4.41. *Ist $a \in \mathbb{C}$ algebraisch und $\varepsilon > 0$, so gilt $\left| \frac{p}{q} - a \right| > \frac{1}{q^{2+\varepsilon}}$ für alle bis auf endlich viele rationale Zahlen $\frac{p}{q}$ mit $p, q \in \mathbb{Z}$ und $q > 0$.*

Folgerung 4.42. *Gibt es zu $a \in \mathbb{C}$ ein $\varepsilon > 0$, so daß $\left| \frac{p}{q} - a \right| \leq \frac{1}{q^{2+\varepsilon}}$ für unendlich viele rationale Zahen $\frac{p}{q}$ mit $p, q \in \mathbb{Z}$ und $q > 0$ gilt, so ist a transzendent.*

Besonders interessant ist es natürlich, die Transzendenz konkret gegebener Zahlen wie zum Beispiel e und π nachzuweisen. Das gelang Hermite 1873 für e und Lindemann 1882 für π. Wir werden nur die Transzendenz von e nachweisen.

Satz 4.43. *e ist transzendent.*

Beweis. Für ein Polynom $f \in \mathbb{R}[x]$ betrachte die Summe $F(x) := f(x) + f'(x) + f''(x) + \dots$ der Ableitungen von f. Da f ein Polynom ist, ist diese Summe endlich. Es gilt

$$\frac{d}{dx} e^{-x} F(x) = -e^{-x} F(x) + e^{-x} F'(x) = -e^{-x} f(x).$$

Durch integrieren erhält man

$$e^{-x} F(x) - F(0) = -\int_0^x e^{-t} f(t) dt$$

beziehungsweise

$$e^x F(0) - F(x) = e^x \int_0^x e^{-t} f(t) dt \tag{2}$$

Angenommen, e ist algebraisch. Dann gibt es $a_0, \dots, a_n \in \mathbb{Z}$ mit

$$a_0 + a_1 e + \dots + a_n e^n = 0 \tag{3}$$

In (2) setzen wir $x = k$ und multiplizieren mit a_k. Das liefert $a_k e^k F(0) - a_k F(k) = -a_k c_k$ mit $c_k = -e^k \int_0^k e^{-t} f(t)dt$. Summation über k liefert nun, unter Verwendung von (3),

$$\sum_{k=0}^{n} a_k F(k) = \sum_{k=0}^{n} a_k c_k. \tag{4}$$

Wir betrachten nun diese Gleichung für das Polynom

$$f(x) := \frac{1}{(p-1)!} x^{p-1}(x-1)^p \dots (x-n)^p,$$

wobei p eine Primzahl $p > \max\{a_0, n\}$ sei.

Wie man leicht sieht, ist $F(k)$ für $k \in \{0, \dots, n\}$ eine ganze Zahl. Für $k \in \{1, \dots, n\}$ ist p ein Teiler von $F(k)$. p ist aber kein Teiler von $F(0)$. Damit ist p kein Teiler von $\sum_{k=0}^n a_k F(k)$ und $\sum_{k=0}^n a_k F(k)$ eine ganze, von 0 verschiedene Zahl, also vom Betrag her ≥ 1. Für die c_k in (4) gilt nach dem Mittelwertsatz

$$\begin{aligned} -c_k = e^k \int_0^k e^{-t} f(t)dt &= e^{k-\xi_k} f(\xi_k) k \\ &= e^{k-\xi_k} \frac{1}{(p-1)!} \xi_k^{p-1} (\xi_k - 1)^p \dots (\xi_k - n)^p k \end{aligned}$$

für ein $\xi_k \in [0, k]$. Also gilt

$$|c_k| \leq \frac{e^n (n^{n+1})^p}{(p-1)!} \to 0 \text{ für } p \to \infty.$$

Damit ist $|\sum_{k=0}^n a_k c_k| < 1$ für genügend große p. Zusammen mit (4) ergibt sich ein Widerspruch zu $|\sum_{k=0}^n a_k F(k)| \geq 1$. □

4.5. **Einfache transzendente Erweiterungen.**

Definition 4.44. Eine Körpererweiterung $L : K$ heißt *einfach*, falls es ein $\alpha \in L \setminus K$ mit $L = K(\alpha)$ gibt.

Satz 4.45. *Sei $K(X) : K$ eine einfache transzendente Körpererweiterung und $u \in K(X) \setminus K$. Dann hat u die Form $\frac{f(X)}{g(X)}$ für gewisse teilerfremde Polynome $f, g \in K[X]$ mit $g \neq 0$. Der* Grad von u *sei* $\deg(u) := \max\{\deg(f), \deg(g)\}$. *Dann gilt:*

(i) *u ist transzendent über K.*
(ii) *X ist Nullstelle von $f(Y) - u \cdot g(Y) \in K(u)[Y]$ und $f(Y) - u \cdot g(Y)$ ist irreduzibel in $K(u)[Y]$.*
(iii) *X ist algebraisch über $K(u)$ und $[K(X) : K(u)] = \deg(u)$.*

Beweis. (i) folgt aus Lemma 4.29 (iii).

(ii) Offenbar ist X Nullstelle von $f(Y) - u \cdot g(Y)$. Um zu zeigen, daß $f(Y) - u \cdot g(Y)$ über $K(u)$ irreduzibel ist, genügt es, die Irreduzibilität über $K[u]$ zu zeigen. Angenommen $f(Y) - u \cdot g(Y)$ ist reduzibel in $K[u][Y]$, etwa

$$f(Y) - u \cdot g(Y) = (f_1(Y) + u \cdot f_2(Y)) \cdot f_3(Y).$$

(Da $f(Y) - u \cdot g(Y)$ in u linear ist, tritt in der Zerlegung nur ein Faktor auf, der u enthält.) Dann ist $f(Y) = f_1(Y) \cdot f_3(Y)$ und $g(Y) = f_2(Y) \cdot f_3(Y)$. Also ist $f_3(Y)$ gemeinsamer Teiler von $f(Y)$ und $g(Y)$. Wegen der angenommenen

Teilerfremdheit von f und g folgt daraus $f_3 \in K$. Also ist $f(Y) - u \cdot g(Y)$ unzerlegbar über $K[u]$.

(iii) folgt aus (ii) zusammen mit der Feststellung, daß der Grad von $f(Y) - u \cdot g(Y)$ genau $\max\{\deg(f), \deg(g)\}$ ist. Letzteres folgt aus der Transzendenz von u über K. □

Folgerung 4.46. *Sei $u \in K(X)$. Dann gilt $K(u) = K(X)$ genau dann, wenn u die Form $\frac{aX+b}{cX+d}$ für gewisse $a, b, c, d \in K$ mit $ad - bc \neq 0$ hat.*

Beweis. Gilt $K(u) = K(X)$, so ist X algebraisch über $K(u)$ vom Grad 1. Daraus folgt $u = \frac{aX+b}{cX+d}$ gemäß Satz 4.45. Dabei ist $aX + b$ kein Vielfaches von $cX + d$ und $cX + d$ kein Vielfaches von $aX + b$. Daraus folgt $ad - bc \neq 0$.

Ist $ad - bc \neq 0$ und $u = \frac{aX+b}{cX+d}$, so ist $u \notin K$, da $aX + b$ und $cX + d$ dann teilerfremd sind. Außerdem ist X algebraisch über $K(u)$ vom Grad 1 nach Satz 4.45. Also gilt $X \in K(u)$ und damit auch $K(X) = K(u)$. □

Als nächstes bestimmen wir die Galoisgruppe einer einfachen transzendenten Körpererweiterung $K(X) : K$. Sei $\varphi \in \mathrm{Gal}(K(X) : K)$. Dann gilt $K(X) = K(\varphi(X))$, also $\varphi(X) = \frac{aX+b}{cX+d}$ für gewisse $a, b, c, d \in K$ mit $ad + bc \neq 0$.

Sei umgekehrt $u = \frac{aX+b}{cX+d} \in K(X)$ gegeben mit $a, b, c, d \in K$ und $ad + bc \neq 0$. Dann ist $\varphi : K(X) \to K(u); \frac{g(X)}{h(X)} \mapsto \frac{g(u)}{h(u)}$ ein Isomorphismus, der K elementweise festläßt. Wegen $K(u) = K(X)$ ist φ ein Automorphismus von $K(X)$.

Die Elemente von $\mathrm{Gal}(K(X) : K)$ entsprechen also den 2×2 Matrizen über K mit nicht verschwindener Determinante. Zwei invertierbare Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ entsprechen genau dann demselben Automorphismus von $K(X)$, wenn $\frac{aX+b}{cX+d} = \frac{a'X+b'}{c'X+d'}$ gilt, wenn also ein $e \in K$ mit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = e \cdot \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ existiert.

Das zeigt

Definition und Bemerkung 4.47. Sei $\mathrm{Gl}_2(K)$ die Gruppe der invertierbaren 2×2-Matrizen über K. Dann ist

$$U := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in K \wedge a \neq 0 \right\}$$

ein Normalteiler in $\mathrm{Gl}_2(K)$, und $\mathrm{PGl}_2(K) := \mathrm{Gl}_2(K)/U$ ist isomorph zu $\mathrm{Gal}(K(X) : K)$

Zum Abschluß der Körpertheorie beweisen wir noch den *Satz von Lüroth*.

Satz 4.48. *Sei $K(X) : K$ eine transzendente Körpererweiterung und L ein Zwischenkörper mit $K \subsetneq L \leq K(X)$. Dann hat L die Form $K(u)$ für ein geeignetes $u \in K(X)$.*

Beweis. Sei $v \in L \setminus K$. Nach Satz 4.45 ist X algebraisch über $K(v)$. Also ist X algebraisch über L. Sei $f(Y) = Y^n + a_1 Y^{n-1} + \cdots + a_n := \mathrm{Irr}(X, L)$. Da X nicht über K algebraisch ist, existiert ein $j \in \{1, \ldots, n\}$ mit $a_j \notin K$. Wir zeigen $L = K(u)$ für $u := a_j$.

Nach Satz 4.45 ist $u = \frac{g(X)}{h(X)}$ für gewisse teilerfremde Polynome $g, h \in K[X]$ mit $h \neq 0$. Sei $m := \deg(u)$. Nach Satz 4.45 ist $[K(X) : K(u)] = m$.

Wegen $K(u) \leq L$ und $[K(X) : L] = n$ ist $m \geq n$ und $m = n$ gilt genau dann, wenn $L = K(u)$ ist.

X ist Nullstelle des Polynoms $g(Y) - u \cdot h(Y) \in L[Y]$. Also gibt es ein $q(Y) \in L[Y]$ mit

$$(*) \qquad g(Y) - u \cdot h(Y) = q(Y)f(Y).$$

Sei $c_0(X) \in K[X]$ ein normiertes Polynom von minimalem Grad, so daß $c_i(X) := c_0(X) \cdot a_i$ für alle $i \in \{1, \ldots, n\}$ ein Element von $K[X]$ ist. Dann ist

$$F(X, Y) := c_0(X) \cdot f(Y) = c_0(X)Y^n + \cdots + c_n(X) \in K[X, Y],$$

und $F(X, Y)$ ist primitiv als Polynom in Y, d.h., die $c_i(X)$ sind teilerfremd.

Der Y-Grad von $F(X, Y)$ ist n. Wegen $u = a_j = \frac{g(X)}{h(X)}$ und da $g(X)$ und $h(X)$ teilerfremd sind, hat $F(X, Y)$ einen X-Grad $\geq m$. Ersetzt man u in $(*)$ durch $\frac{g(X)}{h(X)}$ und die Koeffizienten von q durch die entsprechenden Ausdrücke in X, so sieht man, daß $F(X, Y)$ ein Teiler von $g(Y)h(X) - g(X)h(Y)$ in $K(X)[Y]$ ist. Wegen $g(Y)h(X) - g(X)h(Y), F(X, Y) \in K[X, Y]$ und da $F(X, Y)$ als Polynom in Y primitiv ist, existiert ein Polynom $Q(X, Y) \in K[X, Y]$ mit

$$(**) \qquad g(Y)h(X) - g(X)h(Y) = Q(X, Y)F(X, Y).$$

Da der X-Grad der linken Seite von $(**)$ nicht größer als m ist und der von $F(X, Y)$ nicht kleiner als m, sind beide Grade $= m$ und es gilt $Q(X, Y) = Q(Y) \in K[Y]$. Da $Q(Y)$ als Polynom in Y über $K[X]$ nur invertierbare Koeffizienten hat, ist $Q(Y)$ primitiv. Da auch $F(X, Y)$ als Polynom in Y primitiv ist, ist $Q(Y)F(X, Y)$ als Polynom in Y über $K(X)$ primitv. Aus Symmetriegründen ist die linke Seite von $(**)$ auch als Polynom in X über $K[Y]$ primitiv. Damit ist $Q(Y) = Q \in K$. Also ist der X-Grad von $F(X, Y)$ gleich dem Y-Grad von $F(X, Y)$ und es gilt $n = m$, was zu zeigen war. □

5. Moduln

Moduln gehören zu den wichtigsten algebraischen Strukturen. Die Theorie der Moduln ist eine Verallgemeinerung der linearen Algebra und hat viele Anwendungen in verschiedenen Bereichen der Mathematik, zum Beispiel in der Darstellungstheorie von Gruppen.

5.1. **Linksmoduln.**

Definition 5.1. Sei $R = (R, +, \cdot)$ ein Ring und $M = (M, +)$ eine abelsche Gruppe. M zusammen mit einer äußeren Verknüpfung (Skalarmultiplikation)

$$R \times M \to M; (r, m) \mapsto r \cdot m$$

heißt ein *R-Linksmodul* (oder *Linksmodul über R*), wenn für alle $r, r_1, r_2 \in R$ und alle $m, m_1, m_2 \in M$ gilt:

(i) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$
(ii) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$
(iii) $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$

Hat R eine 1, so heißt der Modul *unitär*, wenn zusätzlich $1 \cdot m = m$ für alle $m \in M$ gilt. Zur Abkürzung schreiben wir für $r \cdot m$ meistens rm.

Rechtsmoduln werden analog zu den Linksmoduln definiert. Die äußere Verknüpfung ist dabei eine Abbildung $M \times R \to M; (m, r) \mapsto m \cdot r$. Aus den Axiomen (i)-(iii) für Linksmoduln erhält man durch Spiegelung die entsprechenden Axiome für Rechtsmoduln. Man beachte, daß ein R-Rechtsmodul nicht genau dasselbe (bis auf die Schreibweise) sein muß, wie ein R-Linksmodul. Wenn R nicht kommutativ ist, muß man beim Übergang vom Links- zum Rechtsmodul auch die Multiplikation auf R "umdrehen", um äquivalente Strukturen zu erhalten.

Wir werden R-Linksmoduln M mit ${}_R M$ bezeichnen und R-Rechtsmoduln N mit N_R. Ist M sowohl R-Linksmodul als auch S-Rechtsmodul, so bezeichnet man M als (R, S)-Bimodul (und schreibt ${}_R M_S$).

Beispiel 5.2. a) Sei $(G, +)$ eine abelsche Gruppe. Für $n \in \mathbb{N}$ und $g \in G$ wird $n \cdot g$ rekursiv definiert durch

$$0 \cdot g := 0 \text{ und } (n + 1) \cdot x := n \cdot x + x.$$

Außerdem sei $(-n) \cdot x := -(n \cdot x)$ für alle $n \in \mathbb{N}$. Mit der äußeren Verknüpfung $\mathbb{Z} \times G \to G; (n, g) \mapsto n \cdot g$ ist G ein unitärer $\mathbb{Z}$-Linksmodul.

b) Ist R ein Ring, so ist R mit der Multiplikation auf R als äußerer Verknüpfung ein R-Linksmodul. Dieser Modul ist genau dann unitär, wenn R eine 1 hat.

c) Ist K ein Schiefkörper, so sind die unitären K-Linksmoduln genau die Linksvektorräume (ein Begriff, der hoffentlich selbsterklärend ist) über K.

d) Ist M eine abelsche Gruppe, R ein Ring und definiert man die äußere Verknüpfung $R \times M \to M$ durch $(r, m) \mapsto r \cdot m := 0$, so wird M ein R-Linksmodul. Moduln dieser Art nennt man *trivial*.

e) Ist G eine abelsche Gruppe und R der Endomorphismenring von G, so ist G zusammen mit $R \times G \to G; (r, g) \mapsto r(g)$ ein R-Linksmodul.

Definition 5.3. Sei ${}_R M$ ein Modul. Eine nichtleere Menge $U \subseteq M$ heißt *Untermodul* von M, wenn gilt:

(i) U ist eine Untergruppe von M und
(ii) für alle $u \in U$ und alle $r \in R$ ist $ru \in U$

Für (ii) kann man auch kürzer $RU \subseteq U$ schreiben.

Beispiel 5.4. a) Sei G eine abelsche Gruppe. Betrachtet man G als $\mathbb{Z}$-Modul ${}_{\mathbb{Z}}G$, so sind die Untermoduln genau die Untergruppen.

b) Ist R ein Ring, so sind die Untermoduln von ${}_RR$ genau die Linksideale von R.

c) Ist K ein Körper und ${}_KV$ unitärer K-Modul, also K-Vektorraum, so sind die Untermoduln von ${}_KV$ genau die linearen Unterräume von V.

d) Ist ${}_RM$ ein Modul, dann ist für jedes $m \in M$ die Menge $Rm := \{rm : r \in R\}$ ein Untermodul von ${}_RM$. (Man beachte, daß m selbst nicht in Rm liegen muß.)

Definition 5.5. Sei ${}_RM$ ein R-Modul. Ein Untermodul U von M heißt *zyklisch*, falls U die Form Rm für ein $m \in M$ hat.

Bemerkung 5.6. Mit den üblichen Beweisen für Gruppen, Ringe und Vektorräume beweist man auch für Moduln folgende Aussagen:

a) Ist ${}_RM$ ein R-Modul und $(U_i)_{i\in I}$ eine Familie von Untermoduln, so ist $\bigcap_{i\in I} U_i$ ein Untermodul von ${}_RM$. Ist $A \subseteq M$, so ist

$$ {}_R\langle A\rangle := \bigcap \{U : U \text{ ist ein Untermodul von } M \text{ mit } A \subseteq U\}$$

der *von A erzeugte Untermodul von M*. Ist M unitär, so besteht $R\langle A\rangle$ genau aus den (endlichen) R-Linearkombinationen von Elementen von A.

Anstelle von ${}_R\langle\{a_1, \dots, a_n\}\rangle$ schreibt man meist ${}_R\langle a_1, \dots, a_n\rangle$. Außerdem wird das R bei ${}_R\langle\cdot\rangle$ oft weggelassen.

Im unitären Fall gilt $\langle a\rangle = Ra$ für alle $a \in M$. Allgemein gilt nur

$$\langle a\rangle = \mathbb{Z}a + Ra = \{na + ra : n \in \mathbb{Z}, r \in R\}.$$

$A \subseteq M$ heißt ein *Erzeugendensystem* von M, falls $M = \langle A\rangle$ ist. M heißt *endlich erzeugt*, wenn M ein endliches Erzeugendensystem hat.

Ist $(U_i)_{i\in I}$ eine Familie von Untermoduln von M, so setzt man $\sum_{i\in I} U_i := \langle\bigcup_{i\in I} U_i\rangle$ und bezeichnet $\sum_{i\in I} U_i$ als die *innere Summe der U_i*. Eine Summe $\sum_{i\in I} U_i$ heißt *direkt*, wenn sich die 0 nur auf triviale Weise als Summe von Elementen der U_i darstellen läßt. Für direkte Summen schreibt man $\bigoplus_{i\in I} U_i$ beziehungweise $U_1 \oplus U_2 \oplus \cdots \oplus U_n$.

Ist U ein Untermodul von ${}_RM$, so wird auf der Faktorgruppe M/U eine äußere Verknüpfung $R \times M/U \to M/U$ durch $r \cdot (m + U) := r \cdot m + U$ definiert. Wegen $rU \subseteq U$ ist diese Verknüpfung wohldefiniert. M/U wird dadurch zu einem R-Linksmodul.

Definition 5.7. Seien R ein Ring und ${}_RM$ und ${}_RN$ R-Moduln. Eine Abbildung $f : M \to N$ heißt *R-Modulhomomorphismus* (oder auch *R-linear*), falls f ein Gruppenhomomorphismus ist und zusätzlich $f(rm) = r \cdot f(m)$ für alle $r \in R$ und alle $m \in M$ gilt.

Kern und Bild von R-Modulhomomorphismen sind wie üblich definiert und sind Untermoduln der entsprechenden R-Moduln. Wie auch bei Gruppen und Ringen gelten folgende Sätze:

Satz 5.8. *Ist $f : {}_RM \to {}_RN$ ein Modulhomomorphismus, so gilt $f[M] \cong M/\operatorname{Ker} f$.*

Satz 5.9. *Sind U und V Untermoduln eines Moduls ${}_RM$, so gilt $(U + V)/V \cong U/(U \cap V)$.*

Satz 5.10. *Sind U und V Untermoduln eines Moduls ${}_RM$ mit $U \subseteq V$, so gilt $(M/U)/(V/U) \cong M/V$.*

Definition 5.11. Sei ${}_RM$ ein Modul und $a \in M$. Dann heißt $\operatorname{Ann}(a) := \{r \in R : ra = 0\}$ der *Annullator von A*. $\operatorname{Ann}(a)$ ist ein Linksideal von R (also ein Untermodul von ${}_RR$). Es gilt $Ra \cong R/\operatorname{Ann}(a)$.

Für einen Untermodul U von ${}_RM$ definiert man

$$\operatorname{Ann}(U) := \{r \in R : ru = 0 \text{ für alle } u \in U\}.$$

Es gilt $\operatorname{Ann}(U) = \bigcap_{u \in U} \operatorname{Ann}(u)$. $\operatorname{Ann}(U)$ ist ebenfalls ein Linksideal von R.

$a \in M$ heißt *Torsionselement*, falls $\operatorname{Ann}(a) \neq \{0\}$ ist. Ein Modul ohne Torsionselemente $\neq 0$ heißt *torsionsfrei*. Ist ${}_RM \neq \{0\}$ torsionsfrei, so hat R keine Nullteiler.

Satz 5.12. *Sei R ein Integritätsring und M ein R-Linksmodul. Weiter sei $\operatorname{Tor}(M) := \{a \in M : a \text{ ist Torsionselement}\}$. Dann ist $\operatorname{Tor}(M)$ ein Untermodul von M, und $M/\operatorname{Tor}(M)$ ist torsionsfrei.*

Beweis. Sei $a \in \operatorname{Tor}(M)$ und $r \in R$. Dann existiert ein $s \in R$ mit $s \neq 0$ und $sa = 0$. Es ist $s(ra) = (sr)a = (rs)a = r(sa) = 0$. Also ist $ra \in \operatorname{Tor}(M)$. Sei b ein weiteres Element von $\operatorname{Tor}(M)$ und $t \in R$ mit $t \neq 0$ und $tb = 0$. Dann ist $st(a + b) = t(sa) + s(tb) = 0$. Da R Integritätsring ist, ist $st \neq 0$. Damit ist $a + b \in \operatorname{Tor}(M)$.

Sei nun $a + \operatorname{Tor}(M)$ ein Torsionselement von $M/\operatorname{Tor}(M)$ und $s \in R$ mit $s \neq 0$ und $s(m + \operatorname{Tor}(M)) = 0 + \operatorname{Tor}(M)$. Dann ist $sm \in \operatorname{Tor}(M)$. Also existiert $t \in R$ mit $t \neq 0$ und $t(sm) = 0$. Es gilt $(ts)m = t(sm) = 0$. Da R Integritätsring ist, ist $ts \neq 0$. Also ist $m \in \operatorname{Tor}(M)$. Das zeigt $m + \operatorname{Tor}(M) = 0 + \operatorname{Tor}(M)$ und damit die Torsionsfreiheit von $M/\operatorname{Tor}(M)$. □

5.2. **Direkte Produkte und Summen von Moduln.**

Definition 5.13. Sei R ein Ring und $(M_i)_{i \in I}$ eine Familie von R-Linksmoduln. Auf dem mengentheoretischen Produkt

$$P := \prod_{i \in I} M_i = \left\{ f : I \to \bigcup_{i \in I} M_i : \forall i \in I (f(i) \in M_i) \right\}$$

definieren wir die Moduloperationen $+ : P \times P \to P$ und $\cdot : R \times P \to P$ punktweise: Für alle $f, g \in P$, alle $i \in I$ und alle $r \in R$ sei

$$(f + g)(i) := f(i) + g(i) \qquad \text{und} \qquad (r \cdot f)(i) := r \cdot f(i).$$

Mit diesen Operationen wird P zu einem R-Linksmodul, dem *direkten Produkt* der M_i. Ist $I = \emptyset$, so ist $P = \{0\}$.

$$\bigoplus_{i \in I} M_i := \left\{ f \in \prod_{i \in I} M_i : f(i) \neq 0 \text{ nur für endlich viele } i \in I \right\}$$

ist ein Untermodul von $\prod_{i \in I} M_i$, die (*äußere*) *direkte Summe* der M_i. Für endliches I ist $\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i$.

Wie man leicht nachrechnet, gilt

Satz 5.14. *Sei R ein Ring und $(M_i)_{i\in I}$ eine Familie von R-Linksmoduln.*
a) Ist $\pi : I \to I$ eine Permutation, so ist

$$\prod_{i\in I} M_i \cong \prod_{i\in I} M_{\pi(i)} \text{ und } \bigoplus_{i\in I} M_i \cong \bigoplus_{i\in I} M_{\pi(i)}.$$

b) Ist $(I_j)_{j\in J}$ eine Partition von I, so ist

$$\prod_{i\in I} M_i \cong \prod_{j\in J} \left(\prod_{i\in I_j} M_i \right) \text{ und } \bigoplus_{i\in I} M_i \cong \bigoplus_{j\in J} \left(\bigoplus_{i\in I_j} M_i \right).$$

Für ein direktes Produkt $\prod_{i\in I} M_i$ werden in natürlicher Weise Modulhomomorphismen $\pi_j : \prod_{i\in I} M_i \to M_j$, $j \in I$, durch $\pi_j(f) := f(j)$ definiert.

Dual dazu werden für jede direkte Summe $\bigoplus_{i\in I} M_i$ Modulhomomorphismen $\alpha_j : M_j \to \bigoplus_{i\in I} M_i$, $j \in I$, durch $\alpha_j(m) := (m_i)_{i\in I}$ definiert, wobei $m_j := m$ sei und $m_i := 0$ für $i \neq j$.

Satz 5.15. *Sei ${}_RA$ ein Modul und $(M_i)_{i\in I}$ eine Familie von R-Linksmoduln.*
a) Für jedes $i \in I$ sei $\varphi_i : A \to M_i$ R-linear. Dann gibt es genau eine R-lineare Abbildung $\varphi : A \to \prod_{i\in M_i} M_i$, so daß für alle $j \in I$ gilt: $\varphi_j = \pi_j \circ \varphi$.
b) Für jedes $i \in I$ sei $\psi_i : M_i \to A$ R-linear. Dann gibt es genau eine R-lineare Abbildung $\psi : \bigoplus_{i\in I} M_i \to A$, so daß für alle $j \in I$ gilt: $\psi_j = \psi \circ \alpha_j$.

Bemerkung 5.16. Die innere direkte Summe einer Familie $(M_i)_{i\in I}$ von Untermoduln eines Modul M isomorph zur äußeren direkten Summe der Familie.

5.3. **Freie Moduln.** Im folgenden sei R stets ein Ring mit 1, und alle vorkommenden Moduln seien unitär.

Definition 5.17. Sei ${}_RM$ ein Modul und $m_1, \ldots, m_n \in M$. $m_1, \ldots, m_n$ heißen *linear unabhängig*, falls für alle $r_1, \ldots, r_n \in R$ mit $\sum_{i=1}^n r_i m_i = 0$ gilt: $r_i = 0$ für alle $i \in \{1, \ldots n\}$. $S \subseteq M$ heißt *linear unabhängig*, wenn jede endliche Teilmenge von S linear unabhängig ist.

$S \subseteq M$ heißt Basis von M, wenn M von S erzeugt wird und S linear unabhängig ist. M heißt *frei*, wenn M eine Basis hat. Ist $S \subseteq M$ eine Basis von M, so heißt M *frei über* S.

Satz 5.18. *Ein Modul ${}_RM$ ist genau dann frei über $S \subseteq M$, wenn M die direkte Summe der zyklischen Untermoduln $R \cdot s$, $s \in S$, ist und S keine Torsionselemente enthält. Das ist genau dann der Fall, wenn sich jedes $m \in M$ eindeutig schreiben läßt als Summe der Form $\sum_{s\in S} r_s s$ mit $r_s \in R$.*

Beweis. Wie in der linearen Algebra sieht man, daß S genau dann eine Basis von M ist, wenn sich jedes Element von M eindeutig als R-Linearkombination von Elementen von S schreiben läßt.

Ist M die direkte Summe der $R \cdot s$, $s \in S$, und enthält S keine Torsionselemente, so rechnet man schnell nach, daß sich jedes Element von M eindeutig als R-Linearkombination von Elementen von S schreiben läßt. Umgekehrt sieht man leicht, daß das Erzeugnis einer linear unabhängigen Menge T direkte Summe der zyklischen Moduln $R \cdot t$, $t \in T$, ist. □

Folgerung 5.19. *a) Ist ${}_RM$ frei, so ist M isomorph zu einer direkten Summe von Kopien von R.*

b) Ist ${}_RM$ endlich erzeugt und frei, so existiert ein $n \in \mathbb{N}$ mit $M \cong R^n$.

Beweis. Nur b) bedarf eines Beweises. Sei $E \subseteq M$ ein endliches Erzeugendensystem von M und $B \subseteq M$ eine Basis von M. Jedes $e \in E$ ist eine R-Linearkombination endlich vieler Elemente von S. Es werden also nur endlich viele Elemente von S benötigt, um alle Elemente von E zu erzeugen. Eine endliche Teilmenge T von S, deren Erzeugnis alle Elemente von E enthält, erzeugt aber bereits M. Als Teilmenge von S ist T linear unabhängig. Also ist T eine Basis von M. Also hat T eine endliche Basis. Die Behauptung folgt nun aus a). □

Im Gegensatz zu Vektorraumbasen können Basen desselben Moduls verschiedene Mächtigkeiten haben. Jedoch gilt

Satz 5.20. *Ist R ein kommutativer Ring mit 1 und ${}_RM$ ein freier Modul, so haben je zwei Basen von M dieselbe Mächtigkeit.*

Beweis. Sei I ein maximales Ideal von R. Dann ist R/I ein Körper. IM ist ein Untermodul von M. Wie man leicht nachrechnet, ist M/IM ein R/I-Vektorraum. Sei nun S eine Basis von M. Dann ist $M = \bigoplus_{s\in S} Rs$. Daraus folgt $IM = \bigoplus Is$ und damit auch

$$M/IM \cong \bigoplus_{s\in S}(Rs/Is) \cong \bigoplus_{s\in S} R/I.$$

Damit ist die Mächtigkeit von S genau die Dimension von M/IM als R/I-Vektorraum. □

Definition 5.21. Die Mächtigkeit einer Basis eines freien, unitären Moduls über einem kommutativen Ring nennt man den *Rang* des Moduls.

Freie Moduln haben folgende universelle Eigenschaft:

Lemma 5.22. *Ist ${}_RM$ ein freier Modul über S, ${}_RN$ ein weiterer Modul und $f : S \to N$ eine beliebige Abbildung, so existiert genau eine R-lineare Abbildung $h : M \to N$ mit $h \restriction S = f$.*

Beweis. Sei $m \in M$. Dann gibt es eindeutig bestimmte $r_s \in R$, $s \in S$, mit $m = \sum_{s\in S} r_s s$. Setze $h(m) := \sum_{s\in S} r_s f(s)$. Wie man leicht nachrechnet leistet h das Gewünschte. Da man keine Wahl bei der Definition von h hat, ist h auch eindeutig bestimmt. □

Folgerung 5.23. *Jeder unitäre Modul ist homomorphes Bild eines freien Moduls.*

Beweis. Sei ${}_RN$ ein unitärer Modul. Dann ist $M := \bigoplus_{n\in N} R$ ein freier Modul. Für $n \in N$ sei $e_n : N \to R$ die Abbildung, die bei n den Wert 1 hat und sonst 0. Die Menge $\{e_n : n \in N\}$ ist eine Basis von M. Sei f die Abbildung, die jedem e_n das Element n von N zuordnet. Nach Lemma 5.22 läßt sich f zu einem Homomorphismus $h : M \to N$ fortsetzen. Offenbar ist h surjektiv. □

5.4. **Moduln über Hauptidealringen.** Ziel dieses Abschnittes ist es, endlich erzeugte Moduln über Hauptidealringen zu klassifizieren. Im folgenden sei R stets ein Hauptidealring.

Ein wichtiger Satz auf dem Wege zum angestrebten Klassifikationssatz ist der sogenannte Elementarteilersatz, der auch viele andere Anwendungen hat. Wir verallgemeinern zunächst den Begriff des Ranges eines Moduls.

Definition 5.24. Der Rang $\mathrm{rg}(M)$ eines Moduls ${}_RM$ ist das Supremum (in $\mathbb{N} \cup \{\infty\}$) der Mächtigkeiten von linear unabhängigen Teilmengen von M.

Satz 5.25. *(Elementarteilersatz) Sei ${}_RF$ ein endlich erzeugter freier Modul und M ein Untermodul von F vom Rang n. Dann existieren Elemente $x_1, \ldots, x_n \in F$, die Teil einer Basis von F sind, und $a_1, \ldots, a_n \in R \setminus \{0\}$, so daß gilt:*

(i) *$a_1x_1, \ldots, a_nx_n$ ist eine Basis von M und*
(ii) *für alle $i \in \{1, \ldots, n-1\}$ ist a_i ein Teiler von a_{i+1}.*

Dabei sind die Elemente $a_1, \ldots, a_n$ bis auf Assoziiertheit eindeutig bestimmt, unabhängig von der Wahl von $x_1, \ldots, x_n$. Man nennt $a_1, \ldots .a_n$ die Elementarteiler von M.

Wir zeigen den Elementarteilersatz ohne die Eindeutigkeitsaussage. Zum Beweis benötigen wir den Begriff des *Inhalts* $\mathrm{cont}(x)$ eines Elementes $x \in F$. Sei $y_1, \ldots, y_n$ eine Basis von F. Dann existieren $c_1, \ldots, c_n \in R$ mit $x = c_1y_1 + \cdots + c_ny_n$. $\mathrm{cont}(x)$ ist definiert als der größte gemeinsame Teiler von $c_1, \ldots, c_n$. Man beachte, daß $\mathrm{cont}(x)$ eigentlich eine Äquivalenzklasse von assoziierten Elementen von R ist.

Um zu zeigen, daß $\mathrm{cont}(x)$ nicht von der Wahl der Basis $y_1, \ldots, y_n$ abhängt, betrachte man den R-Linksmodul F^* aller Homomorphismen von F nach R. Die Menge $\{\varphi(x) : \varphi \in F^*\}$ ist ein Ideal von R. Da R Hauptidealring ist, existiert $c \in R$ mit $(c) = \{\varphi(x) : \varphi \in F^*\}$. Wir zeigen, daß $\mathrm{cont}(x) = c$ gilt.

$\mathrm{cont}(x)$ ist eine Linearkombination der c_i. Also existieren $a_1, \ldots, a_n \in R$ mit $\mathrm{cont}(x) = a_1c_1 + \cdots + a_nc_n$. Für jedes $i \in \{1, \ldots, n\}$ sei $\varphi_i \in F^*$ der Homomorphismus, der y_i auf 1 abbildet und alle y_j, $j \neq i$, auf 0. Setzt man $\varphi := a_1\varphi_1 + \cdots + a_n\varphi_n$, so ergibt sich $\varphi(x) = \mathrm{cont}(x)$. Da $\varphi_1, \ldots, \varphi_n$ eine Basis von F^* ist, ist $\mathrm{cont}(x)$ ein Teiler von $\psi(x)$ für alle $\psi \in F^*$. Das zeigt $\mathrm{cont}(x) = c$.

Lemma 5.26. *In der Situation von Satz 5.25 gilt:*

(i) *Zu jedem $x \in F$ existiert $\varphi \in F^*$ mit $\varphi(x) = \mathrm{cont}(x)$.*
(ii) *Für alle $x \in F$ und alle $\psi \in F^*$ ist $\mathrm{cont}(x)$ ein Teiler von $\psi(x)$.*
(iii) *Es gibt ein $x \in M$, so daß $\mathrm{cont}(x)$ alle $\mathrm{cont}(y)$, $y \in M$, teilt.*

Beweis. (i) und (ii) wurden bereits gezeigt. Für (iii) betrachte man die Menge aller Ideale $(\mathrm{cont}(y))$, $y \in M$. Da R Hauptidealring ist, gibt es unter diesen Idealen eines, welches bezüglich $\subseteq$ maximal ist. Sei $x \in M$ so gewählt, daß $\mathrm{cont}(x)$ dieses maximale Ideal erzeugt. Wähle $\varphi \in F^*$ mit $\varphi(x) = \mathrm{cont}(x)$. Wir zeigen zunächst, daß $\varphi(x)$ alle $\varphi(y)$, $y \in M$, teilt.

Sei $y \in M$ und d größter gemeinsamer Teiler von $\varphi(x)$ und $\varphi(y)$. Dann gibt es $a, b \in R$ mit $d = a\varphi(x) + b\varphi(y)$, also mit $\varphi(ax + by) = d$. Wegen (ii) ist $\mathrm{cont}(ax + by)$ ein Teiler von d und wegen $d|\varphi(x)$ sogar von $\mathrm{cont}(x)$.

Die Maximalitätseigenschaft von x impliziert nun $\operatorname{cont}(ax+by) = \operatorname{cont}(x)$. Insbesondere ist $\operatorname{cont}(x)$ ein Teiler von d und damit auch von $\varphi(y)$. Also teilt $\varphi(x)$ alle $\varphi(y)$, $y \in M$.

Um $\operatorname{cont}(x)|\operatorname{cont}(y)$ zu erhalten, genügt es nach (i) zu zeigen, daß $\varphi(x)$ für alle $\psi \in F^*$ ein Teiler von $\psi(y)$ ist. Da $\varphi(x)$ nach (ii) ein Teiler von $\psi(x)$ ist und nach dem eben gezeigten auch von $\varphi(y)$, können wir y durch $y - \frac{\varphi(y)}{\varphi(x)}x$ ersetzen und damit $\varphi(y) = 0$ annehmen. Durch nochmalige Anwendung dieses Argumentes können wir ψ durch $\psi - \frac{\psi(x)}{\varphi(x)}\varphi$ ersetzen und $\psi(x) = 0$ annehmen. Unter diesen Voraussetzungen sei d größter gemeinsamer Teiler von $\varphi(x)$ und $\psi(y)$, etwa $d = a\varphi(x) + b\psi(y)$ für geeignete $a, b \in R$. Dann gilt

$$(\varphi + \psi)(ax + by) = a\varphi(x) + b\psi(y) = d.$$

Mit (ii) folgt daraus $\operatorname{cont}(ax+by)|d$. Da d ein Teiler von $\varphi(x)$ ist, ergibt sich $\operatorname{cont}(ax+by)|\varphi(x)$. Die Maximalitätseigenschaft von x liefert nun $\operatorname{cont}(ax+by) = \varphi(x)$. Hieraus folgt $\varphi(x)|d$ und wegen $d|\psi(y)$ wie gewünscht $\varphi(x)|\psi(y)$. □

Beweis von Satz 5.25. Wir beweisen den Satz durch zwei Induktionen über den Rang n von M. Mit der ersten Induktion zeigen wir, daß jeder Untermodul M von F frei ist. Diese Aussage benutzen wir im zweiten Induktionsbeweis, um die Existenz der x_i und der a_i zu zeigen.

Man beachte, daß M torsionfrei ist. Daher gilt im Falle $n = 0$ auch $M = \{0\}$, und es ist nichts zu zeigen. Sei also $n > 0$. Nach Lemma 5.26 (iii) existiert ein $x \in M$ mit $\operatorname{cont}(x)|\operatorname{cont}(y)$ für alle $y \in M$. Nach Lemma 5.26 (i) existiert ein $\varphi \in F^*$ mit $\varphi(x) = \operatorname{cont}(x)$. Wegen der Definition von $\operatorname{cont}(x)$ gibt es ein $x_1 \in F$ mit $x = \varphi(x)x_1$. x_1 ist dabei eindeutig bestimmt. Sei nun F' der Kern von φ und $M' := M \cap F'$. Dann gilt $M = Rx \oplus M'$. Jedes $y \in M$ läßt sich nämlich schreiben als

$$y = \frac{\varphi(y)}{\varphi(x)}x + \left(y - \frac{\varphi(y)}{\varphi(x)}x\right).$$

Da nach Lemma 5.26 $\varphi(x)$ ein Teiler von $\varphi(y)$ ist und da wegen $M \neq \{0\}$ $\varphi(x) \neq 0$ gilt, ist der erste Summand in der Darstellung von y ein Element von Rx. Der zweite Summand liegt in M', da er sowohl im Kern von φ liegt, als auch in M. Es ist klar, daß die Summe direkt ist.

Auf ähnliche Weise, unter Ausnutzung der Tatsache, daß $\varphi(x_1) = 1$ ist, sieht man $F = Ax_1 \oplus F'$. Wegen $M = Ax \oplus M'$ gilt $\operatorname{rg}(M') < \operatorname{rg}(M)$. Nach Induktionvoraussetzung ist M' also frei. Damit ist aber auch M frei. Das beendet den ersten Induktionsbeweis.

Den zweiten Induktionsbeweis führen wir in gleicher Weise, bis wir zu den Zerlegungen $F = Ax_1 \oplus F'$ und $M = Ax \oplus M'$ gelangen. Nach dem ersten Induktionsbeweis ist F' als Untermodul eines freien Moduls frei. Also haben wir nach Induktionsvoraussetzung die Aussage des Satzes für $M' \leq F'$ zur Verfügung. Es existieren also Elemente $x_2, \ldots, x_n \in F'$, die sich zu einer Basis von F' ergänzen lassen, sowie $a_2, \ldots, a_n \in R$ mit $a_i|a_{i+1}$ für alle $i \in \{2, \ldots, n-1\}$ und der Eigenschaft, daß $a_2x_2, \ldots, a_nx_n$ eine Basis von M' ist.

Insgesamt sind dann $x_1, \ldots, x_n$ Teil einer Basis von $F = Ax_1 \oplus F'$. Setzt man $a_1 := \varphi(x)$, so bilden $a_1x_1, \ldots, a_nx_n$ eine Basis von $M = Ax \oplus M'$. Es

bleibt lediglich $a_1|a_2$ zu zeigen. Dazu wählt man $\varphi_2 \in F^*$ mit $\varphi_2(x_2) = 1$. φ_2 existiert, da x_2 Teil einer Basis von F ist. Nach Lemma 5.26 gilt dann $\varphi(x)|\varphi_2(a_2x_2)$ und damit $a_1|a_2$. □

Aus dem Elementarteilersatz läßt sich leicht der *Klassifikationssatz für endlich erzeugte Moduln über Hauptidealringen* ableiten.

Folgerung 5.27. *Sei ${}_RM$ ein endlich erzeugter Modul. Dann ist M die direkte Summe von endlich vielen zyklischen Moduln.*

Beweis. Sei $\{m_1, \dots, m_n\}$ ein Erzeugendensystem von M. Für $i \in \{1, \dots, n\}$ sei e_i der i-te Einheitsvektor in R^n. Da R^n frei über $\{e_1, \dots, e_n\}$ ist, existiert ein Homomorphismus $h : R^n \to M$, der jedes e_i auf m_i abbildet. Da die m_i den Modul M erzeugen, ist h surjektiv. Sei $K \leq R^n$ der Kern von h. Nach dem Elementarteilersatz existieren Elemente $x_1, \dots, x_k \in R^n$, die Teil einer Basis $x_1, \dots, x_n$ von R^n sind, und $a_1, \dots, a_k \in R$, so daß $a_1x_1, \dots, a_kx_k$ eine Basis von K ist.

Nach dem Homomorphiesatz für Moduln ist M isomorph zu R^n/K. Wegen $R^n = Rx_1 \oplus \dots \oplus Rx_n$ und $K = a_1Rx_1 \oplus \dots \oplus a_kRx_k$ ist R^n/K isomorph zu $R/a_1R \oplus \dots \oplus R/a_kR \oplus R^{n-k}$. Das zeigt die Behauptung. □

Da abelsche Gruppen $\mathbb{Z}$-Moduln sind, ergibt sich folgender *Klassifikationssatz für endlich erzeugte abelsche Gruppen*:

Folgerung 5.28. *Sei G eine endlich erzeugte abelsche Gruppe. Dann ist G isomorph zu einer Gruppe der Form*

$$\mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_k} \oplus \mathbb{Z}^n,$$

wobei jedes q_i eine Primzahlpotenz ist. Dabei ist n der Rang von G.

Beweis. Nach Folgerung 5.27 ist G die direkte Summe von endlich vielen zyklischen Gruppen. Jede unendliche zyklische Gruppe ist isomorph zu $\mathbb{Z}$. Jede endliche zyklische Gruppe ist isomorph zu einer Gruppe der Form $\mathbb{Z}_m$. Ist $m = q_1 \dots q_l$ die Zerlegung von m in paarweise teilerfremde Primzahlpotenzen, so ist $\mathbb{Z}_m$ nach dem chinesischen Restsatz isomorph zu $\mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_l}$. □

6. Freie Gruppen

Definition 6.1. Es sei A eine Menge, *Alphabet* genannt. Ein Tupel $w = (a_1, \dots, a_n) \in A^n$ heißt *Wort* über A. Üblicherweise wird w geschrieben als $a_1 \dots a_n$. Die Menge aller Wörter über A bezeichnet man mit $W(A)$. Das leere Wort (das einzige Element von A^0) wird mit e bezeichnet. (Wir nehmen dabei $e \notin A$ an.)

Sind $u = (a_1, \dots, a_n)$ und $v = (b_1, \dots, b_m)$ Wörter über A, so definiert man $u \cdot v := uv = (a_1, \dots, a_n, b_1, \dots, b_m)$.

Die Abbildung $\cdot : W(A) \times W(A) \to W(A)$ ist eine innere Verknüpfung auf $W(A)$, die assoziativ ist. Neutrales Element bezüglich dieser Verknüpfung ist offenbar e. Man beachte $W(\emptyset) = \{e\}$.

Sei nun B eine beliebige Menge und B^{-1} eine zu B disjunkte Menge gleicher Mächtigkeit. Die Abbildung $\cdot^{-1} : B \to B^{-1}; b \to b^{-1}$ sei eine Bijektion. Die Umkehrabbildung von $\cdot^{-1}$ bezeichnen wir ebenfalls mit $\cdot^{-1}$. Für $b \in B \cup B^{-1}$ nennen wir $b^{-1} \in B \cup B^{-1}$ das *formale Inverse* von b.

Wir betrachten die Halbgruppe $W(B \cup B^{-1})$.

Definition 6.2. Ein Wort $w = x_1 x_2 \dots x_n \in (B \cup B^{-1})^n$ heißt *reduziert*, wenn kein x_i neben seinem formalen Inversen steht, d.h., wenn $x_i \neq x_{i+1}^{-1}$ für alle $i \in \{1, \dots, n-1\}$ gilt. Sei $W_0 := W_0(B \cup B^{-1})$ die Menge der reduzierten Wörter in $W := W(B \cup B^{-1})$. (Man beachte, daß e ein reduziertes Wort ist.)

Die *Reduktionsabbildung* $\rho : W \to W_0$ ist wie folgt rekursiv definiert: Ist $w \in W$ ein reduziertes Wort, so sei $\rho(w) := w$. Ist $w \in W$ kein reduziertes Wort, so existieren $u, v \in W$ und $b \in B \cup B^{-1}$ mit $w = ubb^{-1}v$. Setze $\rho(w) := \rho(uv)$.

Lemma 6.3. *a)* $\rho(w) = w$ *für alle* $w \in W_0$.
b) $\rho(\rho(w)) = \rho(w)$ *für alle* $w \in W$.
c) $\rho(ubb^{-1}v) = \rho(uv)$ *für alle* $u, v \in W$ *und alle* $b \in B \cup B^{-1}$.
d) $\rho(uv) = \rho(\rho(u)v) = \rho(u\rho(v))$ *für alle* $u, v \in W$.

Beweis. Beweis über durch Induktion die Längen von Wörtern. □

Wir betrachten nun die von ρ auf W induzierte Äquivalenzrelation $R \subseteq W \times W$, die durch

$$(u, v) \in R :\Leftrightarrow \rho(u) = \rho(v)$$

definiert ist, und zeigen, daß R mit der Multiplikation auf W verträglich ist. Dazu müssen wir nachweisen, daß für alle $u, v, w \in W$ mit $\rho(u) = \rho(v)$ auch $\rho(uw) = \rho(vw)$ und $\rho(wu) = \rho(wv)$ gelten. Nach Lemma 6.3 gilt aber für $u, v, w \in W$ mit $\rho(u) = \rho(v)$

$$\rho(uw) = \rho(\rho(u)w) = \rho(\rho(v)w) = \rho(vw)$$

und

$$\rho(wu) = \rho(w\rho(u)) = \rho(w\rho(v)) = \rho(wv).$$

Damit ist auf der Menge $F(B) := W(B \cup B^{-1})/R$ der R-Äquivalenzklassen das Produkt $([u], [v]) \mapsto [u][v] := [uv]$ wohldefiniert. Dabei bezeichnet $[u]$ die R-Äquivalenzklasse von $u \in W$.

Satz 6.4. *$F(B)$ zusammen mit dem Produkt $([u],[v]) \mapsto [uv]$ ist eine Gruppe. Das neutrale Element ist $[e]$. Für alle $b_1, \dots, b_n \in B \cup B^{-1}$ ist $[b_n^{-1} \dots b_1^{-1}]$ das zu $[b_1 \dots b_n]$ inverse Element von $F(B)$.*

Beweis. Es ist klar, daß $F(B)$ mit dem Produkt $([u],[v]) \mapsto [uv]$ eine Halbgruppe ist. Da e neutrales Element von W ist, ist $[e]$ neutrales Element von $F(B)$. Wegen

$$\rho(b_1 \dots b_n b_n^{-1} \dots b_1^{-1}) = e$$

und

$$\rho(b_n^{-1} \dots b_1^{-1} b_1 \dots b_n) = e$$

ist $[b_n^{-1} \dots b_1^{-1}]$ zu $[b_1 \dots b_n]$ invers. □

Die Abbildung $B \to F(B); b \mapsto [b]$ ist injektiv. Deshalb läßt sich B als Teilmenge von $F(B)$ auffassen.

Definition 6.5. $F(B)$ heißt die *von B frei erzeugte Gruppe* oder die *freie Gruppe über B*.

Lemma 6.6. *In jeder Äquivalenzklasse aus $F(B)$ gibt es genau ein reduziertes Wort.*

Beweis. Wegen $\rho(\rho(w)) = \rho(w)$ gilt $(\rho(w), w) \in R$ für alle $w \in W$. Damit enthält jede R-Äquivalenzklasse mindestens ein reduziertes Wort. Seien nun $u, v \in W$ reduziert mit $(u, v) \in R$. Dann gilt $u = \rho(u) = \rho(v) = v$. □

Lemma 6.7. *Außer $[e]$ enthält $F(B)$ kein Element endlicher Ordnung.*

Beweis. Sei $w \in W$ ein reduziertes Wort $\neq e$. Dann existieren $r, s \in \mathbb{N}$ mit $s \neq 0$ sowie

$$b_1, \dots, b_r, a_1, \dots, a_s \in B \cup B^{-1}$$

mit

$$w = b_1 \dots b_r a_1 \dots a_s b_r^{-1} \dots b_1^{-1}$$

und $a_1 \neq a_s^{-1}$. Offenbar gilt für alle $n > 0$

$$[w]^n = [b_1 \dots b_r (a_1 \dots a_s)^n b_r^{-1} \dots b_1^{-1}] \neq [e].$$

□

Satz 6.8. *Sei G eine Gruppe und $f : B \to G$ eine Abbildung. Dann existiert genau ein Homomorphismus $h : F(B) \to G$, der f fortsetzt. (Hierbei wird jedes $b \in B$ mit $[b] \in F(B)$ identifiziert.)*

Beweis. Wir setzen f zunächst auf $B \cup B^{-1}$ fort. Für jedes $b \in B$ sei $\overline{f}(b) = f(b)$ und $\overline{f}(b^{-1}) = f(b)^{-1}$. Man rechnet leicht nach, daß die Abbildung

$$h : F(B) \to G; [(b_1, \dots, b_n)] \mapsto \overline{f}(b_1) \dots \overline{f}(b_n)$$

ein Homomorphismus ist. Die Eindeutigkeit von h folgt aus der Tatsache, daß $F(B)$ von B erzeugt wird. □

Folgerung 6.9. *Jede Gruppe ist homomorphes Bild einer freien Gruppe und damit auch isomorph zu einem Quotienten einer freien Gruppe.*

Beweis. Nach Satz 6.8 läßt sich die Abbildung $\mathrm{id}_G : G \to G$ zu einem Homomorphismus $h : F(G) \to G$ fortsetzen. Offenbar ist h surjektiv. Sei K der Kern von h. Nach dem Homomorphiesatz ist G isomorph zu $F(G)/K$. □

6.1. **Präsentierungen von Gruppen und Wortprobleme.** Die freie Gruppe über einer Menge X ist die Gruppe, die von X erzeugt wird und in der keine Relationen zwischen verschiedenen Elementen gelten außer denen, die von den Gruppenaxiomen vorgeschrieben werden. Wir wollen nun Gruppen konstruieren, in die von einer vorgebenen Menge erzeugt werden und in denen zusätzliche Relationen zwischen den Erzeugern gelten.

Sei X eine beliebige Menge. *Relationen zwischen den Elementen von X* sind Gleichungen der Form $x_1 \dots x_n = e$ mit $x_1, \dots, x_n \in X \cup X^{-1}$, wobei e für das neutrale Element der (noch zu konstruierenden) Gruppe steht. Sei N der Normalteiler in $F(X)$, der von $x_1 \dots x_n$ erzeugt wird. Dann gilt in $F(X)/N$ die Gleichung $\overline{x}_1 \dots \overline{x}_n = e_{F(X)/N}$, wobei $\overline{x}_i$ jeweils die N-Nebenklasse von x_i bezeichnet.

Allgemeiner kann man für eine Menge M von Relationen den von der Menge $\{x_1 \dots x_n : (x_1 \dots x_n = e) \in M\}$ erzeugten Normalteiler $N(M)$ von $F(X)$ betrachten. Für jede Relation $(x_1 \dots x_n = e) \in M$ gilt dann in $F(X)/N(M)$ die Gleichung $\overline{x}_1 \dots \overline{x}_n = e_{F(X)/N(M)}$. Üblicherweise wird $F(X)/N(M)$ mit $G(X|M)$ bezeichnet. $G(X|M)$ hat folgende universelle Eigenschaft:

Satz 6.10. *Sei M eine Menge von Relationen zwischen den Elementen von X, G eine Gruppe und $f : X \to G$ eine Abbildung. Weiter sei $\overline{f} : X \cup X^{-1} \to G$ die eindeutig bestimmte Fortsetzung von f, die mit $\cdot^{-1}$ vertauscht. Falls $\overline{f}(x_1) \dots \overline{f}(x_n) = e_G$ für jede Relation $(x_1 \dots x_n = e) \in M$ gilt, so existiert genau ein Homomorphismus $h : G(X|M) \to G$, so daß $h(x \cdot N(M)) = f(x)$ für alle $x \in X$ gilt.*

Beweis. Sei $g : F(X) \to G$ der eindeutig bestimmte Homomorphismus, der f fortsetzt. Wegen der Eigenschaften von f ist $N(M)$ eine Teilmenge des Kerns von g. Damit existiert genau ein Homomorphismus

$$h : G(X|M) = F(X)/N(M) \to G$$

mit den geforderten Eigenschaften. □

Definition 6.11. Eine Gruppe G heißt *endlich präsentierbar*, falls es eine endliche Menge X und eine endliche Menge M von Relationen zwischen den Elementen von X mit $G \cong G(X|M)$ gibt.

Ist $X = \{x_1, \dots, x_n\}$ und $M = \{m_1, \dots, m_k\}$, so schreibt man anstelle von $G(X|M)$ auch gerne $G(x_1, \dots, x_n|m_1, \dots, m_k)$.

Beispiel 6.12. a) Die zyklische Gruppe $\mathbb{Z}_n$ ist endlich präsentierbar. Es gilt nämlich $\mathbb{Z}_n \cong G(x|x^n = e)$.

b) Die Diedergruppe ist endlich präsentierbar. Es gilt

$$D_n \cong G(d, s|d^n = e, s^2 = e, (ds)^2 = e).$$

Sei X eine endliche Menge und M eine endliche Menge von Relationen zwischen den Elementen von X. Das *Wortproblem* der Gruppe $G(X|M)$ ist die Aufgabe, für jedes gegebene Wort $w \in W(X \cup X^{-1})$ in endlich vielen Schritten zu entscheiden, ob $[w]$ in $N(M)$ liegt, d.h., ob der Ausdruck w interpretiert in $G(X|M)$ gleich dem neutralen Element ist. Gesucht ist also ein Algorithmus.

Boone und Novikov konnten 1955 eine endlich präsentierte Gruppe angeben, deren Wortproblem nicht lösbar ist.