Algebra/Zahlentheorie und ihre Didaktik

Vorlesungsskript Sommersemester 2025

Felix Schmäschke

18. Juli 2025

Dies ist ein ergänzendes Vorlesungsskript zum Buch „Von den natürlichen Zahlen zu den Quaternionen “ von Jürg Kramer und Anna-Maria von Pippich.

I. Die natürlichen Zahlen

I.1. Die Peano-Axiome

Definition I.1.28. Ein *Peano-System* (P, o, σ) besteht aus einer Menge P, einem Element $o \in P$ und einer Abbildung $\sigma : P \to P$, der *Nachfolgerabbildung*, so dass

(i) Für alle $p \in P$ gilt $\sigma(p) \neq o$.

(ii) Die Abbildung σ ist injektiv.

(iii) Für jede Teilmenge $X \subset P$ mit $o \in X$ und $\sigma(X) \subset X$ gilt $X = P$.

Zwei Peano-Systeme (P, o, σ) und (P', o', σ') heißen *isomorph*, wenn es eine Bijektion $\phi : P \to P'$ gibt, so dass $\phi(o) = o'$ und $\phi(\sigma(p)) = \sigma'(\phi(p))$ für alle $p \in P$.

Ein Beispiel eines Peano-Systems liefern die natürlichen Zahlen $(\mathbb{N}_0, 0, \sigma)$ wobei $\sigma(n) := n + 1$ für alle $n \in \mathbb{N}$.

Satz I.1.29 (Isomorphiesatz von Dedekind)**.** *Jedes Peano-System ist isomorph zu den natürlichen Zahlen.*

- **Begriffe:** Peano-Axiome, Induktionsbeweis, Teilbarkeit, Primzahlen, geordnete Menge, Primfaktorzerlegung, ggT, kgV, teilerfremd
- **Sätze:** Rechengesetze auf $\mathbb{N}$ (d.h. Assoziativ-, Kommutativ- und Distributivgesetz), Prinzip des kleinsten Elements, Teilbarkeitsbeziehungen, Unendlich viele Primzahlen, Fundamentalsatz der Zahlentheorie, Euklidisches Lemma, Division mit Rest, (erweiterter) Euklidischer Algorithmus, Lemma von Bezout

II. Die ganzen Zahlen

II.5. Faktorgruppen und Homomorphiesatz

Satz II.5.12 (Erster Isomorphisatz)**.** *Sei G eine Gruppe, $H \subset G$ eine Untergruppe, $K \lhd G$ ein Normalteiler. Dann ist $H \cap K \lhd H$, die Menge*

$$HK = \{g \in G \mid \exists\ h \in H, k \in K \text{mit } g = hk\}\,,$$

ist eine Untergruppe und es gibt einen Isomorphismus

$$H/(H \cap K) \cong KH/H\,.$$

Beweis. Wir zeigen $H \cap K \lhd H$, d.h. $h\big(H \cap K\big)h^{-1} \subset H \cap K$ für alle $h \in H$. Die Inklusion $\subset H$ ist klar, da $H \subset G$ als Untergruppe abgeschlossen ist. Die Inklusion $\subset K$ gilt, da

$$h\big(H \cap K\big)h^{-1} \subset hKh^{-1} \subset K\,,$$

wobei die letzte Inklusion sogar für alle $h \in G$ gilt, da $K \lhd G$.

Wir zeigen $HK \subset G$ ist eine Untergruppe. Abgeschlossen unter Inversenbildung:

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k' \in HK\,,$$

wobei $k' = hk^{-1}h^{-1} \in K$. Abgeschlossen unter Multiplikation:

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1')k_2 = (h_1h_2)(k_1'k_2) \in HK\,,$$

wobei $k_1' = h_2^{-1}k_1h_2 \in K$.

Wir definieren $\phi : H \to G/K$ durch $h \mapsto hK$. Dies ist ein Gruppenhomomorphismus. Wir behaupten $\phi(H) = HK/K$. Die Inklusion $\subset$ ist klar. Die Inklusion $\supset$ folgt, denn $HK/K = \{hK \mid h \in H\}$ da $hkK = hK$. Wir berechnen den Kern

$$\ker\phi = \{h \in H \mid hK = K \iff h \in K\} = H \cap K\,.$$

Nach Homomorphiesatz ist $\bar{\Phi} : H/H \cap K \to HK/K$ eine injektive Abbildung mit gleichem Bild wie ϕ, also auch surjektiv. □

Satz II.5.13 (Zweiter Isomorphiesatz)**.** *Sei G eine Gruppe, $K, H \lhd G$ Normalteiler mit $K \subset H$, dann ist K normal in H und es gibt einen Isomorphismus*

$$\big(G/K\big)/\big(H/K\big) \cong G/H\,.$$

II.8. Erzeuger und Relationen

Wir wollen Gruppen G beschreiben, indem wir die Relationen, d.h. Gleichungen, angeben, die in ihnen gelten sollen. Hier ein Beispiel. Gesucht ist eine Gruppe G, welche die Elemente a und b enthält und die Relationen $a^2 = e$ sowie $b^2 = a$ erfüllt. Offensichtlich

ist a komplett durch b bestimmt und somit ist G auch mit einem Element b und der Relation $e = a^2 = b^4$ komplett beschrieben. Genauer ist G als Menge

$$G = \{e, b, b^2, b^3\},$$

und als Gruppe isomorph zu $\mathbb{Z}/4\mathbb{Z}$. Wir geben ein zweites Beispiel. Sei G erzeugt von den Elementen a und b mit den Relationen $a^2 = b^2 = (ab)^3 = e$. Es gilt demnach $a^{-1} = a$ und $b^{-1} = b$. Durch kurze Überlegung bestimmen wir G als Menge durch

$$G = \{e, a, ab, aba, abab, ababa\}.$$

Dies sind wirklich alle Elemente, denn $b = ababa$. Zu welcher Gruppe ist G isomorph?

Um diesen Prozess zu formalisieren, beschreiben wir nun zunächst ganz allgemein Gruppen in denen keine Relationen gelten.

Definition II.8.1 (freie Gruppe)**.** Sei S eine Menge. Die *freie Gruppe* über S ist die Menge $F(S)$ aller Äquivalenzklassen von Worten der Form

$$a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_k^{\varepsilon_k},$$

wobei $k \in \mathbb{N}$, $\varepsilon_i \in \{\pm 1\}$, $a_i \in S$ für alle $i = 1, \ldots, k$ sowie des leeren Worts, bezeichnet mit e, bezüglich der Äquivalenzrelation

$$wa^{-1}aw' \sim ww', \qquad waa^{-1}w' \sim ww',$$

für alle $a \in S$ und Worte w, w'. Die Gruppenmultiplikation ist das Hintereinanderschreiben von Worten. Das leere Wort e ist das neutrale Element. Es gilt a und a^{-1} sind invers zueinander für alle $a \in S$. Wir verwenden die Notation a^n und a^{-n} für das Wort mit n-mal dem Element a bzw. a^{-1} für $n \in \mathbb{N}$, $a \in S$, sowie $a^0 = e$.

Beispiel II.8.2. (a) Für $S = \{a\}$ ist $F(S) = \{a^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$.

(b) Für $S = \{a, b\}$ ist

$$F(S) = \{e, a, b, a^{-1}, b^{-1}, a^2, ab, ab^{-1}, a^{-2}, a^{-1}b, a^{-1}b^{-1}, \ldots\}.$$

Definition II.8.3. Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Wir sagen, dass G von S *erzeugt wird*, wenn die Abbildung

$$F(S) \to G, \qquad \text{Wort} \mapsto \text{Produkt}, \tag{1}$$

surjektiv ist. Die Gruppe G heißt *endlich erzeugt*, wenn es eine endliche Teilmenge S gibt, die G erzeugt.

Sei $R \subset F(S)$ eine Teilmenge. Wir sagen, dass G von S *erzeugt wird, mit den Relationen* R, wenn

$$F(S)/N(R) \to G, \tag{2}$$

ein Isomorphismus ist, wobei $N(R)$ der kleinste Normalteiler von $F(S)$ ist, der R enthält. Falls $S = \{a_1, \ldots, a_k\}$ und $R = \{r_1, \ldots, r_m\} \subset F(S)$ schreiben wir

$$\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle,$$

für die Gruppe erzeugt von S mit den Relationen R.

Beispiel II.8.4. Sei $G = \mathbb{Z} \times \mathbb{Z}$. Wir wählen $S = \{a, b\}$ wobei $a = (1, 0)$ und $b = (0, 1)$. Die Abbildung $F(S) \to G$ ist surjektiv, denn $a^n b^m$ ist ein Urbild von $(n, m) \in \mathbb{Z} \times \mathbb{Z}$. Wir wählen

$$R = \{aba^{-1}b^{-1}\} \subset F(S)\,,$$

in $F(S)/N(R)$ ist $aba^{-1}b^{-1} = e \iff ab = ba$. Also gilt in $F(S)/N(R)$ das Kommutativgesetz und es können in jedem Wort die Zeichen a und b so umsortiert werden, dass jedes Wort eindeutig durch $a^n b^m$ mit $n, m \in \mathbb{Z}$ repräsentiert wird. Also ist (2) ein Isomorphismus. Die Gruppe $\mathbb{Z} \times \mathbb{Z}$ kann also mit zwei Erzeugern und einer Relation beschrieben werden, d.h. $\mathbb{Z} \times \mathbb{Z} \cong \langle a, b \mid aba^{-1}b^{-1} \rangle$.

- **Begriffe:** (reguläre) Halbgruppe, (reguläres) Monoid, Gruppe, Untergruppe, Diedergruppe, Symmetrische Gruppe, Restklassengruppe, Ordnung einer Gruppe, Ordnung eines Elements, Gruppenhomomorphismus, Kern/Bild, Nebenklassen, Normalteiler, Faktorgruppe, Eulersche φ-Funktion, freie Gruppe, Erzeuger/Relationen, zyklische Gruppen,
- **Sätze:** Satz von Lagrange, Homomorphiesatz, Konstruktion von Gruppen aus regulären Halbgruppen (d.h. Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$), kleiner Satz von Fermat, Satz von Euler, Noethersche Isomorphiesätze

III. Die Rationalen Zahlen

III.3. Ringhomomorphismen, Ideale und Faktorringe

Für einen Ring A und Ideale $I, J \subset A$ definieren wir die *Idealsumme* und das *Idealprodukt* durch

$$I + J = \{c \in A \mid \exists a \in I,\ b \in J \text{ s.d. } c = a + b\} \text{ bzw.}$$
$$IJ = \{c \in A \mid \exists k \in \mathbb{N}, a_1, \ldots, a_k \in I,\ b_1, \ldots, b_k \in J \text{ s.d. } c = a_1 b_1 + \cdots + a_k b_k\}\,.$$

Gegeben Elemente $a_1, \ldots, a_n \in A$ definieren wir $(a_1, \ldots, a_n) \subset A$ als das kleinste Ideal, welches die Elemente $a_1, \ldots, a_n$ enthält. Im Fall $n = 1$, heißt (a) *Hauptideal*. Für ein Ideal $I \subset A$ und Elemente $a, b \in A$ schreiben wir $a \equiv b \mod I \iff a - b \in I$.

Satz III.3.30 (Chinesischer Restsatz)**.** *Sei A ein Ring mit 1 und $I_1, \ldots, I_n \subset A$ Ideale, so dass $I_i + I_j = A$ für $i \neq j$. Gegeben Elemente $x_1, \ldots, x_n \in A$, dann gibt es ein $x \in A$, so dass für alle $j = 1, \ldots, n$ gilt*

$$x \equiv x_j \mod I_j\,. \tag{3}$$

Außerdem gibt es den Ringisomorphismus

$$A/I \cong A/I_1 \times A/I_2 \times \cdots \times A/I_n\,, \qquad x + I \mapsto (x + I_1, x + I_2, \ldots, x + I_n)\,, \tag{4}$$

wobei $I = I_1 \cap I_2 \cap \ldots \cap I_n$.

Beweis. Im Fall $n = 1$ ist nichts zu zeigen. Sei $n = 2$. Aus $I_1 + I_2 = A$ folgt, dass es Elemente $a_1 \in I_1$ und $a_2 \in I_2$ gibt, so dass

$$a_1 + a_2 = 1\,.$$

Gegeben $x_1, x_2 \in A$ setzen wir $x = x_2 a_1 + x_1 a_2$. Dies erfüllt die Bedingung (3), denn

$$x \equiv x_1 a_2 = x_1(1 - a_1) = x_1 - x_1 a_1 \equiv x_1 \mod I_1\,,$$

und analog zeigen wir $x \equiv x_2 \mod I_2$. Sei nun $n > 2$. Nach Voraussetzung finden wir für $i = 2, \ldots, n$ Elemente $a_i \in I_1$ und $b_i \in I_i$ so dass $a_i + b_i = 1$. Damit gilt nach Ausmultiplizieren

$$1 = (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) = a_2 a_3 \cdots a_n + \cdots + b_2 b_3 \cdots b_n\,,$$

wobei alle bis auf den letzten Summanden in I_1 liegen, da jeweils mindestens ein a_i im Summanden als Faktor auftritt, und der letzte Summand im Idealprodukt $I_2 I_3 \cdots I_n$ liegt. Wir schließen

$$1 \in I_1 + I_2 I_3 \cdots I_n \quad \Rightarrow \quad I_1 + I_2 I_3 \cdots I_n = A\,.$$

Mit dem schon bewiesen Fall für $n = 2$ bezüglich den zwei Idealen I_1 und $I_2' = I_2 I_3 \cdots I_n$ finden wir ein Element $y_1 \in A$ so dass

$$y_1 \equiv 1 \mod I_1 \quad \text{und} \quad y_1 \equiv 0 \mod I_2 I_3 \cdots I_n\,.$$

Also $y_1 \in I_2 I_3 \cdots I_n \subset I_i$ für $i = 2, \ldots, n$. Damit folgt für alle $i = 2, \ldots, n$

$$y_1 \equiv 1 \mod I_1 \quad \text{und} \quad y_1 \equiv 0 \mod I_i \,.$$

Analog finden wir $y_2, \ldots, y_n \in A$ so dass für alle $j = 2, \ldots, n$ und $i = 1, \ldots, n$ mit $i \neq j$ gilt

$$y_j \equiv 1 \mod I_j \quad \text{und} \quad y_j \equiv 0 \mod I_i \,.$$

Sei nun $x_1, \ldots, x_n \in A$ gegeben, dann erfüllt $x = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$ die Bedingung (3) nach Konstruktion.

Um (4) zu zeigen, betrachten wir $\phi : A \to A/I_1 \times \cdots A/I_n$, $x \mapsto (x + I_1, \ldots, x + I_n)$. Die Abbildung ϕ ist offensichtlich ein Ringhomomorphismus. Mit dem obigen Schritt wurde gezeigt, dass ϕ surjektiv ist. Man sieht leicht, dass $\ker \phi = I$. □

Lemma III.3.31. *Seien $n, m \in \mathbb{N}$, dann gilt*

(i) $n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n, m)\mathbb{Z}$.

(ii) $n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}(n, m)\mathbb{Z}$.

Korollar III.3.32. *Gegeben $n, m \in \mathbb{N}$ teilerfremd, dann gilt*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \,.$$

Gegeben $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$, dann gilt

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{n_\ell}\mathbb{Z} \,.$$

Diese Isomorphismen sind Ringisomorphismen, insbesondere bilden sie Einheiten auf Einheiten ab. Wir erinnern, dass $\varphi(n) := \mathrm{ord}\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ für alle $n \in \mathbb{N}$.

Korollar III.3.33. *Seien $n, m \in \mathbb{N}$ teilerfremd, dann gilt für die Gruppe der Einheiten*

$$\left(\mathbb{Z}/nm\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/m\mathbb{Z}\right)^\times .$$

Insbesondere folgt für die Euler'sche φ-Funktion $\varphi(nm) = \varphi(n)\varphi(m)$.

III.7. Faktorielle, Euklidische und Hauptidealringe

Wir versuchen Begriffe, Sätze und Verfahren für die ganzen Zahlen auf allgemeine Ringe zu verallgemeinern.

III.7.2. Hauptidealringe

Satz III.7.26. *Jeder Hauptidealring ist ein faktorieller Ring.*

Beweis. Sei A ein Hauptidealring. Wir zeigen die Existenz von Faktorisierungen für jedes Element. Betrachte die Menge von Idealen

$$\mathcal{I} = \{I = (a) \subset A \mid 0 \neq a \text{ hat keine Faktorisierung}\}\,.$$

Wir müssen zeigen, dass $\mathcal{I}$ die leere Menge ist. Wir behaupten zunächst, dass jede aufsteigende Kette von Idealen in $\mathcal{I}$ endlich ist, d.h. es gibt keine unendliche Folge von Idealen $(I_n)_{n\in\mathbb{N}} \subset \mathcal{I}$ mit

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_k \subsetneq \ldots\,,$$

wobei $\subsetneq$ echte Teilmenge bedeutet, d.h. $A \subsetneq B \iff A \subset B$ und $A \neq B$. In der Tat, angenommen per Widerspruch es gäbe eine solche unendliche Kette $(I_n)_{n\in\mathbb{N}}$, dann ist $I := \bigcup_{n\in\mathbb{N}} I_n \subset A$ ein Ideal und da A ein Hauptidealring ist, gibt es ein $a \in A$ mit $(a) = I$. Nach Konstruktion gibt es ein $n \in \mathbb{N}$, so dass $a \in I_n$. Also auch $I = (a) \subset I_n$ und auch $I \subset I_n \subset I_{n+1} \subset I$, was $I_n = I_{n+1}$ impliziert, im Widerspruch zu $I_n \subsetneq I_{n+1}$. Damit ist gezeigt, dass es keine unendliche aufsteigende Kette geben kann.

Sei also $(a) \in \mathcal{I}$ ein maximales Element einer endlichen aufsteigenden Kette in $\mathcal{I}$, d.h. für jedes Ideal (b) mit $(a) \subsetneq (b)$ hat b eine Faktorisierung, sonst wäre (a) kein maximales Element und man könnte die Kette vergrößern. Da a nicht irreduzibel ist (jedes irreduzible Element ist nach Definition faktorisierbar) gibt es $b, c \in A$, welches beides keine Einheiten sind, so dass $a = bc$. Damit folgt $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Nach der Vorüberlegung haben b und c Faktorisierugen. Das Produkt der Faktorisierung von b und c liefert eine Faktorisierung von a im Widerspruch zu $(a) \in \mathcal{I}$.

Wir beweisen die Eindeutigkeit. Zunächst weisen wir das Euklidische Lemma nach, d.h. wir zeigen: Wenn $p \in A$ irreduzibel ist und $a, b \in A$ mit $p \mid ab$, dann $p \mid a$ oder $p \mid b$. Falls $p \nmid a$, sind p und a teilerfremd und es gibt $x, y \in A$ mit

$$1 = xp + ya\,.$$

Also ist auch $b = bxp + yab$ und da nach Voraussetzung $p \mid ab$ folgt $p \mid b$ wie gewünscht.

Seien nun zwei Faktorisierungen von a in irreduzible Elemente gegeben

$$p_1 p_2 \cdots p_r = a = q_1 q_2 \cdots q_s\,.$$

Da p_1 das Produkt auf der rechten Seite teilt, muss es nach dem eben gezeigten Euklidischen Lemma einen der Faktoren teilen, sagen wir q_1 nach Umbennen. Also gibt es eine Einheit $u_1 \in A$ mit $q_1 = u_1 p_1$. Wir erhalten durch Einsetzen und kürzen aus der obigen Gleichung

$$p_2 \cdots p_r = q_2' q_3 \cdots q_s\,,$$

wobei $q_2' = u_1 q_2$. Die Aussage folgt nach Induktion nach r. □

III.7.3. Euklidische Ringe

Sei A ein Ring. Ein *Polynom* $f = f(X) \in A[X]$ ist ein Ausdruck der Form

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n\,,$$

wobei $a_0, a_1, \ldots, a_n \in A$. Die Menge $A[X]$ ist ein Ring wobei die Multiplikation durch A-lineare Fortsetzung von $X^i \cdot X^j = X^{i+j}$ definiert ist. Der *Grad* von f, geschrieben $\deg f \in \mathbb{N}_0$, ist das Maximum aller $k \in \mathbb{N}_0$ mit $a_k \neq 0$. Falls $\deg f = n$, dann heißt $a_n \neq 0$ der *Leitkoeffizient*. Der Grad erfüllt folgende Rechenregeln für alle $f, g \in A[X]$ für $f, g \neq 0$

$$\deg(fg) = \deg f + \deg g\,, \qquad \deg(f+g) \leq \max\{\deg f, \deg g\}\,,$$

wobei die erste Gleichung nur gilt, falls die Leitkoeffizienten von f und g keine Nullteiler sind. Diese Rechenregeln erweitern formal auch auf den Fall $f = 0$ oder $g = 0$, indem wir setzen $\deg 0 = -\infty$ sowie $-\infty + \ell = \ell + (-\infty) = (-\infty) + (-\infty) = -\infty$ für alle $\ell \in \mathbb{N}_0$.

Satz III.7.39 (Polynomdivision)**.** *Sei K ein Körper. Für je zwei Polynome $f, g \in K[X]$ mit $g \neq 0$ gibt es eindeutige Polynome $q, r \in K[X]$ mit $f = q \cdot g + r$ und $\deg r < \deg g$.*

Beweis. Wir zeigen die Existenz. Wir führen eine Induktion nach $n = \deg f$. Ohne Einschränkung ist $\deg f \geq \deg g$, sonst ist $q = 0$ und $r = f$ eine Lösung. Sei a_n und b_m der Leitkoeffizient von f bzw. g. Setze $h = \frac{a_n}{b_m} X^{n-m}$. Nach Konstruktion ist $\deg(f - hg) < \deg f$ und somit findne wir nach Induktionsvoraussetzung h' und r mit $\deg r < \deg g$ und

$$f - hg = h'g + r \quad \Longleftrightarrow \quad f = (h + h')g + r\,.$$

Damit haben wir gewünschte Polynome $q = h + h'$ und r gefunden.

Für die Eindeutigkeit seien q' und r' so dass $\deg r' < \deg g$ und $f = q'g + r'$ eine weitere Lösung. Dann gilt

$$qg + r = f = q'g + r' \quad \Longleftrightarrow \quad (q - q')g = r' - r\,.$$

Wir erhalten für den Grad

$$\deg g > \max\{\deg r, \deg r'\} \geq \deg(r' - r) = \deg g(q - q') = \deg g + \deg(q - q')\,.$$

Daher $0 > \deg(q - q')$ und somit $q - q' = 0$ bzw. $q = q'$. Daraus folgt auch $r = r'$ mit obiger Gleichung. □

Sei A ein Ring und $f(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ ein Polynom. Eine *Nullstelle* von f ist ein $\alpha \in A$ so dass $f(\alpha) = \sum_{k=0}^{n} a_k \alpha^k = 0$.

Korollar III.7.40. *Sei A ein Integritätsbereich und $f \in A[X]$ mit $f \neq 0$ ein Polynom sowie $\alpha_1, \ldots, \alpha_k \in A$ paarweise verschiedene Nullstellen, dann gilt $\deg f \geq k$.*

Beweis. Sei K der Quotientenkörper von A. Wir zeigen durch Induktion, dass es ein Polynom $q \in K[X]$ mit $q \neq 0$ gibt, so dass $f = qg$ wobei $g(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$. Offenbar ist $\deg g = k$ und damit $\deg f = \deg q + \deg g \geq k$ wie gewünscht. Um die Behauptung zu zeigen, sei $k = 1$. Nach Satz III.7.39 gibt es q und r mit $f(X) = q(X)(X - \alpha_1) + r(X)$ wobei entweder $r = 0$ oder $0 \leq \deg r < \deg(X - \alpha_1) = 1$, also $\deg r = 0$, d.h. $r(X) = b \neq 0$ ist eine Konstante. Falls $r \neq 0$ gilt allerdings

$0 = f(\alpha_1) = q(\alpha_1)(\alpha_1 - \alpha_1) + r(\alpha_1) = b \neq 0$. Widerspruch. Sei nun $k > 1$ beliebig und nach Induktionvoraussetzung $f(X) = q(X)(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_{k-1})$. Dann gilt

$$0 = f(\alpha_k) = q(\alpha_k)(\alpha_k - \alpha_1)(\alpha_k - \alpha_2) \cdots (\alpha_k - \alpha_{k-1}),$$

und da A ein Integritätsbereich ist folgt $q(\alpha_k) = 0$. Mit gleichem Argument wie eben $q(X) = p(X)(X - \alpha_k)$ für ein weiteres Polynom $p \in K[X]$ mit $p \neq 0$. □

Satz III.7.41 (Wilson)**.** *Eine Zahl $n \in \mathbb{N}$ ist genau dann eine Primzahl, wenn $(n-1)!+1$ durch n teilbar ist.*

Beweis. Wir zeigen, wenn $n = p$ eine Primzahl ist, dann ist $(p-1)! + 1$ durch p teilbar. Die andere Richtung ist eine Hausaufgabe. Im Polynomring $\mathbb{F}_p[X]$ über dem Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ betrachte das Polynom

$$f(X) = (X-1)(X-2)\cdots(X-(p-1)) = X^{p-1} \pm \cdots + (p-1)!\,.$$

Zweitens betrachte $g(X) = X^{p-1} - 1 \in \mathbb{F}_p[X]$. Nach kleinem Satz von Fermat hat g die Nullstellen $1, 2, \ldots, p-1$. Nach Konstruktion hat f die gleichen Nullstellen, damit hat auch die Differenz $h = f - g$ die gleichen Nullstellen. Da die Leitkoeffizienten von f und g gleich sind und beide Polynome den gleichen Grad $p-1$ haben gilt $\deg h < p - 1$. Damit folgt nach Korollar III.7.40, dass $h = 0$ und insbesondere $(p-1)! + 1 = 0$ in $\mathbb{F}_p$. Also ist $(p-1)! + 1$ durch p teilbar. □

- **Begriffe:** Ringe, Unterringe, Ideale, Nullteiler, Integritätsbereich, Polynomring, Grad von Polynomen, (links/rechts) invertierbare Elemente, Einheiten, Charakteristik des Rings,(Schief-)Körper, Faktorring, Ringhomomorphismen, Kern/Bild, Hauptideal, Quotientenkörper, Euklidische Ringe, Faktorielle Ringe, Primelemente, Irreduzible Elemente, Primideale, Teilbarkeiten für Ideale, Idealsumme, Idealprodukt

- **Sätze:** Homomorphiesatz für Ringe, Lokalisierung (Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$), Euklidischer Algorithmus für Euklidische Ringe, Polynomdivision, Ungleichung von Anzahl der Nullstellen und Grad eines Polynoms, chinesischer Restsatz, Hauptidealringe sind faktoriell, Euklidische Ringe sind Hauptidealringe, Gegenbeispiel zu Faktoriellen Ringen, Irreduzible Elemente die keine Primelemente sind, Satz von Wilson

IV. Die reellen Zahlen

- **Begriffe:** Angeordneter Körper, Betrag, konvergente Folgen, Cauchy-Folgen, vollständiger Körper, Supremumsprinzip, Intervallschachtelungsprinzip, Supremum/ Infimum, Dezimalbruchdarstellung, Kettenbrüche
- **Sätze:** Vervollständigung eines angeordneten Körpers (Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$), Eindeutigkeit des vollständigen angeordneten Körpers, Äquivalenz der Vollständigkeitseigenschaften, Dezimalbrüche von rationalen Zahlen

V. Die komplexen Zahlen

- **Begriffe:** Komplexe Zahlen, komplexe Konjugation, Betrag, Inverse durch Betrag, algebraische Zahlen, Liouvillesche Zahl, Eulersche Zahl, komplexe Exponentialfunktion
- **Sätze:** Fundamentalsatz der Algebra, Satz von Liouville, Eigenschaften der komplexen Exponentialfunktion

V.6. Körpererweiterungen

Sei L ein Körper. Eine Teilmenge $K \subset L$ die mit der Addition und Multiplikation von L zu einem Körper wird heißt *Teilkörper* oder *Unterkörper von* L und L heißt *Erweiterungskörper* von K. Wir sagen L/K ist eine *Körpererweiterung*. Ein Element $a \in L$ heißt *algebraisch*, falls es ein Polynom $f \in K[X]$ gibt mit $f(a) = 0$. Wir sagen, das Element a *erfüllt die algebraische Gleichung* $f = 0$. Sei $a \in L$ algebraisch über K, dann gibt es ein eindeutiges *normiertes*, d.h. mit Leitkoeffizient gleich 1, irreduzibles Polynom $f \in K[X]$, so dass $f(a) = 0$. Dieses Polynom heißt *Minimalpolynom* von a. Die *Körpererweiterung* L/K heißt *algebraisch*, wenn alle Elemente von L über K algebraisch sind.

Beispiel V.6.1. (i) $\mathbb{C}/\mathbb{R}$ ist algebraisch.

(ii) $\overline{\mathbb{Q}}/\mathbb{Q}$ wobei $\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ ist algebraisch über } \mathbb{Q}\}$ ist algebraisch.

(iii) $\mathbb{C}/\mathbb{Q}$ ist *nicht* algebraisch.

Bemerkung. $\overline{\mathbb{Q}}$ ist abzählbar (die Menge $\mathbb{Q}$ ist abzählbar, also auch $\mathbb{Q}[X]$ und somit auch die Nullstellen aller Polynome), $\mathbb{C}$ jedoch nicht. Also muss es in $\mathbb{C}$ Zahlen geben, die nicht algebraisch sind. Solche Zahlen heißen *transzendente Zahlen*.

Wir wollen Körpererweiterungen als Quotienten von Polynomringen konstruieren. Dazu untersuchen wir zunächst die allgemeine Situation.

Lemma V.6.2. *Sei A ein kommutativer Ring mit 1 und $m \subset A$ ein Ideal, so dass A/m ein Körper ist. Dann gilt: $m \neq 0$ und für jedes Ideal $I \subset A$ mit $m \subset I$ folgt entweder $I = A$ oder $I = m$.*

Beweis. Wir untersuchen die Ideale des Körpers $K = A/m$. Sei also $J \subset K$ ein Ideal, dann gilt entweder $J = 0$ oder $J \neq 0$. In diesem Fall gibt es $0 \neq a \in J$. Damit auch $1 = aa^{-1} \in J$, also gilt $J = K$. Sei nun $I \subset A$ ein Ideal mit $m \subset I$, dann ist $J = \pi(I) \subset K$ ein Ideal, wobei $\pi : A \to A/m$, $a \mapsto a + m$ die kanonische Projektion ist. Also gilt entweder $0 = J = \pi(I) \iff I = m$ oder $K = J = \pi(I) \iff I = A$. □

Definition V.6.3. Sei $m \subset A$ ein Ideal, so dass $m \neq 0$ und für jedes weitere Ideal $I \subset A$ mit $m \subset I$ gilt entweder $I = m$ oder $I = A$, dann heißt m *maximales Ideal*.

Lemma V.6.4. *Sei A ein kommutativer Ring mit 1 und $m \subset A$ ein Ideal, dann ist m genau dann maximal, wenn A/m ein Körper ist.*

Beweis. Nach dem letzten Lemma reicht es zu zeigen, dass wenn m maximal ist, dass dann A/m ein Körper ist. Sei dazu $a \in A$ mit $a + m \in A/m$ ungleich 0, d.h. $a \notin m$. Dann ist die Idealsumme $(a) + m$ echt größer als m und nach Maximalität von m gilt $(a) + m = A$. Wir finden $b \in A$ und $c \in m$, so dass $1 = ab + c$. Dann ist $b + m \in A/m$ das Inverse, denn

$$(a + m)(b + m) = ab + m = (1 - c) + m = 1 + m\,,$$

wobei wir verwendet haben, dass $c \in m$. □

Gibt es maximale Ideale?

Satz V.6.5. *Sei A ein Hauptidealring und $I \subsetneq A$ ein Ideal, dann gibt es ein maximales $m \subset A$ mit $I \subset m$. Außerdem ist ein Ideal $m = (p)$ genau dann maximal wenn der Erzeuger p irreduzibel ist,*

Beweis. In den Hausaufgaben zeigen Sie, dass ein Ideal $m = (p) \subset A$ genau dann maximal ist, wenn p irreduzibel ist. Wir wissen nach Satz III.7.26, dass A ein faktorieller Ring ist. Sei $I = (a)$ ein Ideal und $a = p_1 p_2 \cdots p_n$ eine faktorisierung in irreduzible Elemente. Dann ist $m = (p_i)$ für jeden beliebigen irreduziblen Faktor p_i ein maximales Ideal mit $I \subset m$. □

Ab jetzt betrachten wir $A = K[X]$ den Polynomring über einem Körper. Für ein Polynom $f \in K[X]$ verwenden die Abkürzung $K[X]/f$ für den Quotientenring $K[X]/(f)$, wobei wie immer $(f) \subset K[X]$ das von f erzeugte Ideal bezeichnet. Offenbar ist $K[X]/f$ ein K-Vektorraum, denn es ist insbesondere durch Addition eine abelsche Gruppe und die skalare Multiplikation ist durch Multiplikation mit konstanten Polynomen gegeben.

Lemma V.6.6. *Sei $0 \neq f \in K[X]$, dann hat $K[X]/f$ die K-dimension* $\deg f$.

Beweis. Sei $n = \deg f$. Wir zeigen, dass $(1, X, X^2, \ldots, X^{n-1})$ eine Basis für $K[X]/f$ bildet. Wir betrachten die K-lineare Abbildung

$$\Phi : K^n \to K[X]/f\,, \qquad (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 X + \cdots a_{n-1} X^{n-1} + (f)\,,$$

Wir müssen zeigen, dass Φ injektiv ist. Sei also $(a_0, a_1, \ldots, a_{n-1}) \in \ker \Phi$, dann gilt $g(X) = a_0 + a_1 X + \cdots a_{n-1} X^{n-1} \in (f)$, d.h. es gibt $h \in K[X]$, so dass $g = hf$. Da aber $\deg g \leq n - 1 < n = \deg f$ muss gelten $g = 0$ nach Gradformel, also auch $(a_0, a_1, \ldots, a_{n-1}) = 0$. Somit ist Φ injektiv.

Wir müssen noch zeigen, dass Φ auch surjektiv ist. Sei dazu $g + (f) \in K[X]/f$ ein beliebiges Element. Nach Polynomdivision finden wir $q, r \in K[X]$ mit $\deg r < \deg f = n$ und $g = qf + r$. Damit liegt $g + (f) = qf + r + (f) = r + (f)$ im Bild von Φ. □

Um Körpererweiterungen zu verstehen müssen wir nach Satz V.6.5 die maximalen Ideale von $K[X]$, d.h. die irreduziblen Polynome verstehen. Dazu brauchen wir Kriterien.

Lemma V.6.7 (Gauß)**.** *Sei $0 \neq f \in \mathbb{Z}[X]$ ein Polynom mit $f = gh$ wobei $g, h \in \mathbb{Q}[X]$, dann gilt bereits $f = g'h'$ für $g', h' \in \mathbb{Z}[X]$,*

Beweis. Sei $b, c \in \mathbb{Z}$ die Hauptnenner der Koeffizienten von g bzw. h und $a = bc$. Damit ist $h' = bh \in \mathbb{Z}[X]$ und $g' = cg \in \mathbb{Z}[X]$ und es gilt

$$af = bcgh = bgch = g'h'\,.$$

Sei nun $p \in \mathbb{N}$ ein Primfaktor von a. Wir reduzieren die Gleichung modulo p und erhalten

$$0 = \bar{g}'\bar{h}' \in \mathbb{F}_p[X]\,,$$

wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ den Restklassenkörper bezeichnet und $\bar{g}', \bar{h}'$ die Polynome g' und h' sind, wobei wir die Koeffizienten in $\mathbb{F}_p$ interpretieren. Da $\mathbb{F}_p[X]$ nullteilerfrei ist, gilt $\bar{g}' = 0$ oder $\bar{h}' = 0$, d.h. alle Koeffizienten von g' oder alle Koeffizienten von h' sind durch p teilbar. Wir ersetzen a mit a/p und g' bzw. h' mit g'/p bzw. h'/p und wiederholen den Schritt bis a keine Primteiler mehr hat, d.h. $a = \pm 1$. □

Korollar V.6.8. *Sei $0 \neq f \in \mathbb{Z}[X]$ normiert und $\alpha \in \mathbb{Q}$ eine Nullstelle, dann gilt bereits $\alpha \in \mathbb{Z}$.*

Satz V.6.9 (Eisensteinkriterium)**.** *Sei $0 \neq f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ und $p \in \mathbb{N}$ prim, so dass $p \mid a_0, \ldots, p \mid a_{n-1}$ aber $p \nmid a_n$ und $p^2 \nmid a_0$, dann ist f irreduzibel über $\mathbb{Q}$.*

Beweis. Sei nach Widerspruch $f = gh$ mit $g, h \in \mathbb{Q}[X]$ und $\deg g, \deg h > 0$. Nach dem Gaußlemma nehmen wir an, dass bereits $g, h \in \mathbb{Z}[X]$, d.h. $g = b_0 + b_1 X + \cdots b_m X^m$ und $h = c_0 + c_1 X + \cdots c_k X^k$ mit $b_i, c_j \in \mathbb{Z}$. Wir erhalten modulo p die Gleichung

$$\bar{a}_n X^n = \bar{f} = \bar{g}\bar{h} \in \mathbb{F}_p[X]\,,$$

damit folgt $\bar{g} = \bar{b}_m X^m$ und $\bar{h} = \bar{c}_k X^k$ und alle anderen Koeffizienten sind durch p teilbar. Also ist auch $a_0 = b_0 c_0$ durch p^2 teilbar im Widerspruch zur Annahme. □

Beispiel V.6.10. (i) $X^4 - 2$ ist irreduzibel mit $p = 2$.

(ii) Sei $p \in \mathbb{N}$ prim und $f = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$. Darauf können wir zunächst nicht das Eisensteinkriterium anwenden. Wir verwenden einen Trick.

$$\begin{aligned} g(X) &\overset{\text{def}}{=} f(X+1) = \frac{(X+1)^p - 1}{X} \\ &= \frac{\sum_{k=0}^{p} \binom{p}{k} X^k - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} \\ &= p + \binom{p}{2} X + \cdots + \binom{p}{p-1} X^{p-2} + X^{p-1}\,. \end{aligned}$$

Hier greift das Eisensteinkriterium, denn für $k = 1, \ldots, p-1$ ist $\binom{p}{k}$ durch p teilbar. Somit ist g und damit auch f irreduzibel.

Als nächsten Schritt wollen wir die Struktur der algebraischen Zahlen verstehen. Unter anderem wollen wir zeigen, dass $\overline{\mathbb{Q}}$ ein Körper ist.

Definition V.6.11. Eine Körpererweiterung L/K ist *endlich*, wenn der *Grad*, definiert durch

$$[L : K] \overset{\text{def}}{=} \dim_K L\,,$$

endlich ist.

Satz V.6.12. *Jede endliche Körpererweiterung ist algebraisch.*

Beweis. Sei L/K eine endlich Körpererweiterung und $[L : K] = n < \infty$. Wir müssen zeigen, dass jedes beliebige Element $a \in L$ algebraisch ist. Entweder gilt $a^i = a^j$ für $i \neq j$ oder die Elemente $1, a, a^2, \ldots, a^n$ sind paarweise verschieden. Im ersten Fall ist a eine Nullstelle von $X^i - X^j$ und im zweiten Fall sind die genannten Elemente linear abhängig, d.h. es gibt Koeffizienten $a_0, a_1, \ldots, a_n \in K$, so dass

$$0 = a_0 \cdot 1 + a_1 a + a_2 a^2 + \cdots + a_n a^n \,,$$

Mit anderen Worten a ist eine Nullstelle des Polynoms $f(X) = a_0 + a_1 X + \cdots + a_n X^n$. Damit ist a algebraisch über K. □

Die Umkehrung ist falsch, denn $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Sei L/K eine Körpererweiterung und $a \in L$. Wir bezeichnen mit $K(a) \subset L$ den kleinsten Teilkörper, welcher K und a enthält und mit $K[a]$ den kleinsten Teilring, welcher K und a enthält.

Satz V.6.13. *Sei L/K eine Körpererweiterung und $a \in L$ algebraisch, dann ist äquivalent*

(i) a ist algebraisch.

(ii) $K[a]$ ist ein endlich dimensionaler K-Vektorraum.

(iii) $K[a]$ ist ein Körper und damit gleich $K(a)$.

(iv) $K(a)$ ist ein endlich dimensionaler K-Vektorraum.

Beweis. Sei $a \in L$ zunächst nicht algebraisch. Dann ist die Auswertungsabbildung injektiv

$$K[X] \to K[a] \,, \qquad X \mapsto a \,,$$

wobei diese durch $X \mapsto a$ eindeutig als K-linearer Ringhomomorphismus bestimmt ist. Die Auswertungssabbildung ist nach Konstruktion auch surjektiv und es folgt $K[X] \cong K[a]$ und damit ist die K-dimension von $K[a]$ unendlich und $K[a]$ ist kein Körper, denn X hat kein multiplikatives Inverses. Auch ist die K-Dimension von $K(a) \supset K[a]$ unendlich.

Sei nun $a \in L$ algebraisch und damit die Auswertungsabbildung nicht injektiv. Der Kern ist ein Ideal erzeugt vom Minimalpolynom f von a und es folgt nach dem Ringhomomorphiesatz $K[a] \cong K[X]/f$. Nach Lemma V.6.6 hat somit $K[a]$ endliche K-Dimension. Wir zeigen, dass $K[a]$ ein Körper ist. Sei dazu $b \in K[a]$ ungleich Null und betrachte die Multiplikationsabbildung

$$\varphi_b : K[a] \to K[a] \,, \qquad c \mapsto bc \,.$$

Da L keine Nullteiler hat, ist φ_b injektiv. Die Abbildung φ_b ist auch surjektiv, denn φ_b ist eine K-lineare Abbildung und $K[a]$ ist als K-Vektorraum endlich dimensional. Somit ist $b' = \varphi_b^{-1}(b)$ das Inverse von b und $K[a]$ ist ein Körper. Nach Minimalität folgt $K[a] = K(a)$ und somit ist $K(a)$ auch ein endlich dimensionaler K-Vektorraum. □

Lemma V.6.14 (Gradformel)**.** *Seien M/L und L/K endliche Körpererweiterungen, dann ist M/K endlich und es gilt*

$$[M : K] = [M : L][L : K] .$$

Beweis. Seien $x_1, \ldots, x_m \in L$ eine K-Basis von L und $y_1, \ldots, y_n \in M$ eine L-Basis von M. Wir zeigen, dass die Elemente $x_i y_j$ für alle i, j eine K-Basis von M bilden. Dazu müssen wir zunächst zeigen, dass sie erzeugend sind. Sei dazu $y \in M$ ein beliebiges Element. Nach Voraussetzung finden wir Elemente $a_1, \ldots, a_n \in L$ sowie für jedes j auch $b_{1j}, \ldots, b_{mj}$ so dass

$$y = \sum_{j=1}^{n} a_j y_j \qquad a_j = \sum_{i=1}^{m} b_{ij} x_i .$$

Zusammengefasst erhalten wir

$$y = \sum_{j=1}^{n} a_j y_j = \sum_{j=1}^{n} \sum_{i=1}^{m} b_{ij} x_i y_j .$$

Damit haben wir gezeigt, dass $x_i y_j$ erzeugend sind. Wir müssen noch zeigen, dass sie linear abhängig sind. Seien dazu nun b_{ij} so dass

$$0 = \sum_{i,j} b_{ij} x_i y_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} b_{ij} x_i \right) y_j .$$

Wegen linearer Unabhängigkeit der y_j und x_i folgern wir zunächst $\sum_{i=1}^{m} b_{ij} x_i = 0$ und damit auch $b_{ij} = 0$ für alle i, j. □

Korollar V.6.15. *Sei L/K eine Körpererweiterung und $a, b \in L$ algebraisch über K mit $b \neq 0$, dann sind auch $a - b$ und ab^{-1} algebraisch.*

Beweis. Da a algebraisch über K, ist $K(a)/K$ endlich nach Satz V.6.13. Auch ist b algebraisch über K, erst recht über $K(a)$, also ist $K(a, b) = K(a)(b)$ auch endlich über $K(a)$. Nach Lemma V.6.14 ist auch $K(a, b)$ endlich und nach Satz V.6.12 auch algebraisch über K. Alle beschriebenen Elemente liegen in $K(a, b)$. □

Korollar V.6.16. *Die Menge $\overline{\mathbb{Q}}$ ist ein Körper.*

Bemerkung. Es ist im allgemeinen schwer das Minimalpolynom von etwa $a+b$ oder ab^{-1} aus denen von a und b zu bestimmen.

Der Körper $\overline{\mathbb{Q}}$ erfüllt die wichtige Eigenschaft, dass er keine nicht-trivialen algebraischen Erweiterungen zulässt, ganz wie $\mathbb{C}$.

Satz V.6.17. *Sei $f \in \overline{\mathbb{Q}}[X]$ ein nicht-konstantes Polynom, dann hat f eine Nullstelle in $\overline{\mathbb{Q}}$.*

Beweis. Seien $a_0, \ldots, a_n \in \mathbb{C}$ die Koeffizienten von f, dann liegt f bereits in $L[X]$ mit $L = \mathbb{Q}(a_0, \ldots, a_n)$. Es ist $L/\mathbb{Q}$ endlich also algebraisch. Sei α eine Nullstelle von f. Dann ist $L(\alpha)/L$ algebraisch. Also ist auch $L(\alpha)/\mathbb{Q}$ algebraisch. Damit ist α algebraisch über $\mathbb{Q}$ und somit $\alpha \in \overline{\mathbb{Q}}$. □

Diese Eigenschaft von $\overline{\mathbb{Q}}$ und $\mathbb{C}$ verdient einen eigenen Namen.

Definition V.6.18. Sei K ein Körper.

(i) Ein Körper L heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante $f \in L[X]$ eine Nullstelle in L hat.

(ii) Ein Erweiterungskörper L heißt *algebraischer Abschluss von* K, falls L/K algebraisch ist und L algebraisch abgeschlossen.

(iii) Sei $f \in K[X]$. Ein Erweiterungskörper L heißt *Zerfällungskörper von* f, falls

$$f = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)\,,$$

mit $c \in K$ und $\alpha_i \in L$ sowie $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Der folgende Satz ist ohne Beweis.

Satz V.6.19. *Sei K ein Körper, dann gibt es einen algebraischen Abschluss von K. Je zwei algebraische Abschlüsse von K sind isomorph.*

V.6.1. Konstruktion mit Zirkel und Lineal

Als Anwendung der erarbeiten Theorie wenden wir uns nun den alten Problemen aus der Antike zu. Dazu wiederholen wir kurz. Es ist $\mathbb{C} \cong \mathbb{R}^2$ die Euklidische Ebene. Durch je zwei verschiedene Punkte gibt es eine eindeutige Gerade, der Abstand zwischen den Punkten $z, w \in \mathbb{C}$ ist gegeben durch den Betrag $|z - w|$. Eine *Konstruktion mit Zirkel und Lineal* ist ein Algorithmus der aus einer Menge $M \subset \mathbb{C}$ eine weitere Menge $N \subset \mathbb{C}$ bildet, wobei jeder Schritt des Algorithmuses einer der folgenden ist

(i) Konstruktion einer Gerade durch zwei zuvor konstruierte Punkte,

(ii) Konstruktion eines Kreises mit bereits konstruiertem Mittelpunkt und Radius gleich dem Abstand zweier zuvor konstruierten Punkte.

(iii) Benennen eines Schnittpunktes zweier konstruierten Geraden oder Kreise.

Hier die erste Beobachtung welche dieses Gebiet mit dem zuvor betrachteten verbindet.

Lemma V.6.20. *Die Menge K aller aus* 0 *und* 1 *konstruierbaren Zahlen ist ein Teilkörper von* $\mathbb{C}$

Beweis. Seien $z, w \in K$ beliebig gegeben und nehmen wir zunächst an, dass $z, w \in \mathbb{R}$ mit $w \neq 0$. Die Differenz erhalten wir durch folgende Konstruktion:

(1) Sei Γ der Kreis mit Mittelpunkt z und Radius $|w|$, d.h. der Abstand von 0 und w.

(2) Sei $\mathbb{R}$ die Gerade durch 0 und 1, d.h. die reelle Achse.

(3) Es gibt zwei Schnittpunkte von $\mathbb{R}$ und Γ. Je nach Vorzeichen entspricht einer der beiden der gesuchten Differenz $z - w$.

Für den Quotienten nehmen wir zusätzlich an, dass $z, w > 0$. Wir gehen davon aus, dass die reelle Achse $\mathbb{R}$ und die imaginäre Achse $i\mathbb{R}$ bereits aus 0 und 1 konstruiert sind. Auch setzen wir voraus, dass die Konstruktion einer Geraden, durch einen gegebenen Punkt und parallel zu einer gegebenen Geraden bekannt ist.

(1) Sei Γ der Kreis mit Mittelpunkt 0 und Radius 1.

(2) Sei Γ' der Kreis mit Mittelpunkt 0 und Radius $|w|$.

(3) Sei i der Schnittpunkt von Γ mit $i\mathbb{R}$ auf der positiven Halbebene.

(4) Sei iw der Schnittpunkt von Γ' mit $i\mathbb{R}$ auf der positiven Halbebene.

(5) Sei g die Gerade durch z und iw.

(6) Sei ℓ die Gerade durch 1 parallel zu g

(7) Nach Strahlensatz ist der Schnittpunkt von ℓ und $\mathbb{R}$ gleich zw^{-1}.

Für den allgemeinen Fall, wenn $z, w \in K$ nicht notwendigerweise reell sind, genügt es den Real- und Imaginärteil von $z - w$ und zw^{-1} aus z und w zu konstruieren, denn mit diesen, können wir eindeutig die komplexe Zahl durch Schnittpunkte von Geraden parallel zur reellen und imaginären Achse rekonstruieren. Sei dazu $z = x + iy$ und $w = x' + iy'$ mit $x, y, x', y' \in \mathbb{R}$. Es gilt $z - w = (x - x') + i(y - y')$ und $zw^{-1} = (x+iy)(x'-iy')((x')^2+(y')^2)^{-1} = (xx'-yy')((x')^2+(y')^2)^{-1}+i(x'y-xy')((x')^2+(y')^2)^{-1}$. Wir sehen, dass wir Real- und Imaginärteil mit den bereits erklärten Konstruktionen erhalten. □

Lemma V.6.21. *Sei $K \subset \mathbb{C}$ ein Teilkörper und $a \in K$, dann ist $\sqrt{a}$ aus K konstruierbar.*

Beweis. Sei zunächst $a \in \mathbb{R}$, so dass $a > 0$. Wir gehen mit dem letzten Lemma davon aus, dass die Geraden $\mathbb{R}$ und $i\mathbb{R}$ sowie -1 bereits konstruiert sind. Auch setzen wir als bekannt voraus, wie ein Kreises mit gegebenen Durchmesser konstruiert wird.

(1) Sei Γ der Thaleskreis mit Durchmesser der Strecke von -1 und a.

(2) Sei ih der Schnittpunkt mit Γ und $i\mathbb{R}$ in der positiven Halbebene.

(3) Nach Höhensatz ist $\sqrt{a}$ gleich dem Abstand von 0 zu ih.

Sei nun $0 \neq a \in K$ beliebig. Wir schreiben $a = re^{i\varphi}$ in Polarkoordinaten. Dann ist $\sqrt{a} = \sqrt{r}e^{i\varphi/2}$. Wir konstruieren $\sqrt{r}$ aus $r = |a|$ wie eben und $e^{i\varphi/2}$ als Winkelhalbierende. □

Theorem V.6.22. *Ein Element $z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal aus* 0 *und* 1 *konstruierbar, wenn es eine Kette von Körpererweiterungen gibt*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \,,$$

mit $z \in K_n$ und $[K_j : K_{j-1}] = 2$. Insbesondere ist z algebraisch über $\mathbb{Q}$ und $[\mathbb{Q}(z) : \mathbb{Q}]$ ist eine Potenz von 2.

Beweis. Wir nennen $z \in \mathbb{C}$ *erreichbar*, wenn es eine Kette von Körpererweiterungen, wie im Theorem gibt. Wir zeigen zunächst die Richtung: Sei z erreichbar, dann ist z konstruierbar. Per Induktion zeigen wir, dass alle Elemente in K_j erreichbar sind. Der Induktionsanfang $j = 0$ wurde in Lemma V.6.20 gezeigt. Sei nun $j \geq 0$ und bereits gezeigt, dass jedes Element in K_j konstruierbar ist. Gegeben $a \in K_{j+1} \setminus K_j$ beliebig. Dann folgt $K_j \subset K_j(a) \subset K_{j+1}$ und nach Gradformel

$$2 = [K_{j+1} : K_j] = [K_{j+1} : K(a)][K(a) : K_j] \,.$$

Da $K(a) \neq K_j$ und damit $[K(a) : K_j] \neq 1$ bleibt nur $[K(a) : K_j] = 2$. Damit s löst eine quadratische Gleichung mit Koeffizienten in K_j. Mit Lösungsformel und Lemma V.6.21 sehen wir, dass a konstruierbar ist. Aus obiger Überlegung schließen wir auch $K_{j+1} = K_j(a)$ und mit der Konstruierbarkeit von a und den Elementen von K_j folgt aus Lemma V.6.20 auch die konstruierbarkeit jedes Elements von K_{j+1}.

Wir zeigen die Implikation: Sei z konstruierbar, dann ist z erreichbar. Wir behaupten, wenn $z_1, z_2, \ldots, z_k \in \mathbb{C}$ erreichbar sind, dass auch alle Elemente von $\mathbb{Q}(z_1, z_2, \ldots, z_k) \subset \mathbb{C}$ erreichbar sind. Da z_1 und z_2 erreichbar sind, gibt es Körperketten $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \ni z_1$ und $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_m \ni z_2$ wobei $[K_{j+1} : K_j] = [L_{i+1} : L_i] = 2$ für $j = 1, \ldots, n$ und $i = 1, \ldots, m$ und mit der gleichen Überlegung wie letzten Abschnitt $K_{j+1} = K_j(a_j)$ für Elemente a_j mit quadratischem Minimalpolynom über K_j. Wir erweitern die Kette $L_{m+j+1} := L_{m+i}(a_j)$ für $j = 1, \ldots, n$ und erhalten, dass $z_1, z_2 \in L_{m+n}$ und damit erreichbar, denn nach Konstruktion $[L_{m+j}(a_j) : L_{m+j}] = 1, 2$. Also nach Lemma V.6.20 auch alle Elemente von $\mathbb{Q}(z_1, z_2)$. Falls $k \geq 3$ wiederholen wir diesen Argument und verlängern die Kette der $L_i's$ erneut.

Wir behaupten nun, dass wenn w erreichbar ist, dann auch $\overline{w}$ und $|w|^2$. In der Tat, gegeben eine Körperkette $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \ni w$ mit $[K_{j+1} : K_j] = 2$. Bezeichne mit $\kappa : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation. Dann bilden die $K_j' := \kappa(K_j)$ eine Körperkette $\mathbb{Q} = K_0' \subset K_1' \subset \cdots \subset K_n' \ni \bar{w}$ mit $[K_{j+1}' : K_j'] = 2$ womit gezeigt ist, dass $\bar{w}$ erreichbar ist. Nach dem letzten Schritt ist mit w und $\bar{w}$ auch $|w|^2 = w\bar{w}$ erreichbar.

Mit dieser Vorarbeit beweisen wir das Theorem. Wir führen Induktion über die Konstruktionsschritte und beweisen, dass alle in einer Konstruktion bestimmten Punkte auch erreichbar sind. Der Induktionsanfang ist gegeben, da 0 und 1 erreichbar sind. Im Induktionsschritt müssen wir zeigen, dass Schnittpunkte von folgenden geometrischen Objekten erreichbar sind:

(i) zwei Geraden $g = z_0 + \mathbb{R}z_1$ und $\ell = w_0 + \mathbb{R}w_1$, definiert durch erreichbaren Punkte z_0, z_1, w_0 und w_1,

(ii) eine Gerade $g = z_0 + \mathbb{R}z_1$ und ein Kreis Γ mit Mittelpunkt w und Radius r, definiert durch erreichbare Punkte z_0, z_1, w und r,

(iii) zwei Kreisen Γ_1 und Γ_2, definiert durch erreichbare Mittelpunkt w_1 bzw. w_2 und Radien r_1 bzw. r_2.

Zu (i). Der Schnittpunkt z ist bestimmt durch die Lösung $s, t \in \mathbb{R}$ von $z = z_0 + sz_1 = w_0 + tw_1$. Real- und Imaginärteil dieser Gleichung liefert zwei reelle Gleichungen. Die Lösung (s, t) lässt sich durch die erreichbaren Zahlen $z_0, z_1, w_0, w_1, \bar{z}_0, \bar{z}_1, \bar{w}_0$ und $\bar{w}_1$ ausdrücken und damit ist der Schnittpunkt erreichbar.

Zu (ii) und (iii). In beiden Fällen ist der Schnittpunkt z die Lösung eines der beiden quadratischen Gleichungssysteme

$$\begin{cases} |z - w|^2 = r^2 \\ z_0 + tz_1 = z \end{cases} \qquad \text{oder} \qquad \begin{cases} |z - w_1|^2 = r^2 \\ |z - w_2|^2 = r^2 \,, \end{cases}$$

deren Lösung sich durch erreichbare Zahlen und Quadratwurzeln aus diesen ausdrücken lässt, somit nach Lemma V.6.21 auch erreichbar. □

V.6.2. Anwendungen

Wir wenden Theorem V.6.22 an, um berühmte Fragestellugen aus der Antike zu lösen. Wir zeigen genauer, dass bestimmte Konstruktionen mit Zirkel und Lineal unmöglich sind.

- **Quadratur des Kreises** ist die Konstruktion eines Quadrats mit gleichem Flächeninhalt wie der Kreis mit Radius 1. Wir müssen also ein Quadrat mit Seitenlänge $\sqrt{\pi}$ konstruieren. Jedoch ist π nicht algebraisch über $\mathbb{Q}$ (siehe [2, Appendix 1, S. 867]), also auch nicht $\sqrt{\pi}$. Damit ist diese Konstruktion unmöglich.

- **Würfelverdopplung**. Gesucht ist die Konstruktion der Seitenlänge eines Würfels mit doppeltem Volumen wie ein gegebener Würfel mit Seitenlänge gleich 1. Wir müssen also $\sqrt[3]{2}$ konstruieren. Angenommen $\sqrt[3]{2}$ wäre erreichbar mit Körperkette $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \ni \sqrt[3]{2}$, dann gilt $\mathbb{Q}(\sqrt[3]{2}) \subset K_n$ und nach Gradformel $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = k \cdot 3$ für ein $k \in \mathbb{N}$. Das ist keine Zweierpotenz, also unmöglich.

- **Regeluläre d-Eck**. Die Ecken des regulären d-Ecks sind $1, \zeta_d, \zeta_d^2, \ldots, \zeta_d^{d-1}$ mit $\zeta_d = \exp(2\pi i/d) \in \mathbb{C}$. Wir müssen also ζ_d konstruieren. Um zu untersuchen, ob ζ_d konstruierbar ist, müssen wir den Grad der Körpererweiterung $\mathbb{Q}(\zeta_d)/\mathbb{Q}$, also das Minimalpolynom von ζ_d bestimmen. Es gilt $\zeta_d^d = 1$, also ist ζ_d eine Nullstelle von $X^d - 1$. Eine weitere offensichtliche Nullstelle ist 1. Nach teilen erhalten wir

  $$(X^d - 1) : (X - 1) = 1 + X + \cdots + X^{d-2} + X^{d-1} \,.$$

  Falls $d = p$ eine Primzahl ist, ist dieses Polynom irreduzibel (siehe Beispiel (b) von V.6.10). Damit ist ein notwendiges Kriterium dafür, dass ζ_p konstruierbar

ist, dass $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ eine Zweierpotenz ist, d.h. $p = 2^m + 1$ mit $m \in \mathbb{N}$. Primzahlen der Form $p = 2^m + 1$ heißen *Fermatsche Primzahlen* und es gilt notwendigerweise $m = 2^k$ ffür ein $k \in \mathbb{N}_0$. Es gibt nur vier bekannte Fermat'sche Primzahlen, nämlich die ersten vier $3, 5, 17$ und 65573 und es wird vermutet, dass es keine weiteren gibt.

Im allgemeinen Fall gilt, dass ein d-Eck genau dann konstruierbar ist, wenn

$$d = 2^m p_1 p_2 \dots p_r \,,$$

wobei $m \in \mathbb{N}$ und p_i paarweise verschiedene Fermatsche Primzahlen sind. Dazu werden wir noch später kommen. Mit derzeitigen Mittel können wir allerdings schon einzelne Fälle bestimmen. Etwa für $d = 9$ ist das Minimalpolynom von ζ_9 gleich $X^6 + X^3 + 1$ und somit $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$. Das ist wieder keine Zweierpotenz und daher ist das 9-Eck nicht konstruierbar.

- **Winkeldreiteilung** ist die Frage, ob ein gegebener Winkel mit Zirkel und Lineal in drei gleichgroße Winkel geteilt werden kann. Auch dies ist unmöglich, denn angenommen, der Winkel $\pi/3$ könnte dreigeteilt werden. Dann wäre auch ein 18-Eck und mit Winkelhalbierung auch ein 9-Eck konstruierbar. Dies ist aber nach dem letzten Punkt unmöglich.

Zusammenfassung

- **Begriffe:** Erweiterungskörper, Minimalpolynom, maximales Ideal, endlich, algebraisch, Grad, algebraischer Abschluss, Zerfällungskörper, Konstruktion Zirkel und Lineal

- **Sätze:** Lemma von Gauß, Eisensteinkriterium, L/K endlich $\Rightarrow$ algebraisch, Gradformel, Äquivalente Bedingungen für algebraische Erweiterungen, $\overline{\mathbb{Q}}$ ist Körper, Existenz des algebraischen Abschlusses, Bedingung für Konstruierbarkeit, Unmöglichkeit der Konstruktionen: Quadratur des Kreises, Würfelverdopplung, bestimmte reguläre n-Ecke, Winkeldreiteilung

V.7. Galoistheorie

Galoistheorie bildet eine Brücke zwischen Körpererweiterungen und Gruppentheorie.

Definition V.7.1. Eine Körpererweiterung L/K heißt *einfach*, wenn $L = K(\alpha)$ für ein $\alpha \in L$.

Satz V.7.2. *Sei $K' = K(\alpha)/K$ einfach, $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ das Minimalpolynom von α und $\sigma : K \to L$ ein Körperhomomorphismus. Dann gibt es eine Bijektion*

$$\{\sigma' : K' \to L \mid \sigma' \textit{ist Körperhom. mit } \sigma'|_K = \sigma\} \to \{\beta \in L \mid f^\sigma(\beta) = 0\}\,, \sigma' \mapsto \sigma'(\alpha)\,,$$

wobei $f^\sigma = \sigma(f) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n$.

Beweis. Die Abbildung ist wohl-definiert, denn

$$0 = \sigma'(0) = \sigma'(f(\alpha)) = \sigma'(f)(\sigma'(\alpha)) = \sigma(f)(\sigma'(\alpha)) = f^\sigma(\sigma'(\alpha))\,,$$

wobei wir in der dritten Gleichung verwendet habe, dass σ' ein Körperhomomorphismus ist und der vierten, dass σ' eingeschränkt auf K die gegebene Abbildung σ ist.

Wir konstruieren eine konkrete Umkehrabbildung. Sei $\beta \in L$ eine Nullstelle von f^σ. Dazu betrachte den Ringhomomorphismus

$$\Phi : K[X] \to L\,, \sum_i b_iX^i \mapsto \sum_i b_i\beta^i\,,$$

Nach Konstruktion $\Phi(f) = 0$, damit $\ker\Phi = (f)$. Nach Homomorphiesatz gibt es einen Ringhomomorphismus $\sigma' : K(a) \cong K[X]/f \to L$. Dieser ist ein Ringhomomorphismus zwischen Körper mit $\sigma(1) = 1$, somit ein Körperhomomorphismus. Außerdem gilt nach Konstruktion $\sigma'(\alpha) = \beta$. □

Korollar V.7.3. *Seien L und L' Zerfällungskörper eines $f \in K[X]$, dann gilt $L \cong L'$.*

Beweis. Da L' Zerfällungskörper ist, gilt

$$f = c(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)\,,$$

wobei $c \in K$ und $\alpha_i \in L'$. Sei f_1 das Minimalpolynom von α_1 über K. Da α_1 auch eine Nullstelle von f ist, wird f von f_1 geteilt. Da L auch Zerfällungskörper von f ist, hat f_1 auch eine Nullstelle β_1 in L. Verwende nun Satz V.7.2 mit $\sigma = \subset\colon K \to L$ und $\alpha = \alpha_1$. Wir erhalten eine Erweiterung $\sigma_1 = \sigma' : K(\alpha_1) \to L$ mit $\sigma_1|_K = \mathrm{id}_K$ und $\sigma_1(\alpha_1) = \beta_1$. Wir setzen dies nun fort. Sei dazu f_2 das Minimalpolynom von α_2 über $K(\alpha_1)$. Wieder teilt f_2 das Polynom $f^{\sigma_1} = f$ und damit gibt es eine Nullstelle β_2 von f_2 in L. Mit Satz V.7.2 finden wir $\sigma_2 : K(\alpha_1, \alpha_2) \to L$ mit $\sigma_2|_{K(\alpha_1)} = \sigma_1$ und $\sigma_2(alpha_2) = \beta_2$. Wir wiederholen diesen Schritt solange bis wir schließlich einen Körperhomomorphismus $\sigma_n : K(\alpha_1, \ldots, \alpha_n) \to L$ mit $\sigma_n(\alpha_i) = \beta_i$. Also zerfällt f bereits über dem Bild von σ_n in Linearfaktoren wegen Minimalität ist das Bild bereits ganz L. Somit ist σ_n der gesuchte Isomorphismus zwischen L und L'. □

Definition V.7.4. Sei L/K algebraisch, dann heißt

$$\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \sigma \text{ ist Körperiso. mit } \sigma|_K = \mathrm{id}|_K\}$$

die *Galoisgruppe von* L/K.

Lemma V.7.5. *Wenn* L/K *endlich, dann gilt* $\operatorname{ord}\mathrm{Gal}(L/K) \leq [L : K]$.

Beweis. Da L/K endlich ist, gilt $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ für Elemente $\alpha_i \in L$. Wir setzen $\sigma = \subset : K \to L$ schrittweise auf $K_j := K_{j-1}(\alpha_j)$ unter Verwendung von Satz V.7.2 fort, wobei $K_0 = K$. Es folgt, dass es bei jedem Schritt maximal $d_j := [K_{j-1}(\alpha_j) : K_j]$ viele Möglichkeiten zur Fortsetzung gibt. Insgesammt gibt es nach Gradformel also maximal $d_1 d_2 \ldots d_n = [L : K]$ viele Körperhomomorphismen $\sigma : L \to L$, welche auf K die Identität sind. Als Körperhomomorphismus ist jedes σ injektiv. Da L ein endlich dimensionaler K-Vektorraum ist, ist jedes σ auch surjektiv, also ein Element von $\mathrm{Gal}(L/K)$. □

Definition V.7.6. Eine Körpererweiterung L/K heißt *galois*, wenn $\operatorname{ord}\mathrm{Gal}(L/K) = [L : K]$.

Definition V.7.7. Eine Körpererweiterung L/K heißt *normal*, wenn für jedes irreduzible Polynom, welches in L eine Nullstelle hat, auch alle anderen Nullstellen in L liegen.

Definition V.7.8. (i) Ein irreduzibles Polynom $f \in K[X]$ heißt *separabel*, wenn f im algebraischen Abschluss keine doppelten Nullstellen hat.

(ii) Ein Polynom $f \in K[X]$ heißt *separabel*, wenn jeder irreduzibler Faktor separabel ist.

(iii) Sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt *separabel über* K, wenn das Minimalpolynom über K separabel ist.

(iv) Eine Körpererweiterung L/K heißt *separabel*, wenn jedes Element von L separabel über K ist.

Normale Erweiterungen

Lemma V.7.9. *Sei* L/K *endlich und normal, dann gibt es ein Polynom* $f \in K[X]$*, so dass* L *der Zerfällungskörper von* f *ist.*

Beweis. Da L/K endlich, gilt $L = K(\alpha_1, \ldots, \alpha_n)$. Sei f_i das Minimalpolynom von α_i, setze $f = \prod f_i$. Da L normal ist, zerfällt f über L in Linearfaktoren. Würde f bereits über einem Teilkörper von L zerfallen, würde dieser die Nullstellen $\alpha_1, \ldots, \alpha_n$ enthalten und ist also gleich L. □

Lemma V.7.10. *Sei* $f \in K[X]$ *und* L *der Zerfällungskörper von* f*, dann ist* L/K *normal.*

Beweis. Sei $g \in K[X]$ irreduzibel und $\alpha \in L$ eine Nullstelle von g. Sei L_1 der Zerfällungskörper von g und $\beta \in L_1$ eine weitere Nullstelle von g. Es genügt zu zeigen, dass $\beta \in L$. Nach Satz V.7.2 gibt es einen Körperhomomorphismus $\sigma : K(\alpha) \to K(\beta)$, welche auf K die Identität ist. Da beide die gleiche K-dimension, nämlich $\deg g$, haben, ist σ ein Körperiso. Es ist L der Zerfällungskörper von f und $L(\beta)$ der Zerfällungskörper von $\sigma(f) = f \in K(\beta)[X]$. Also nach Korolloar V.7.3 gibt es einen Körperisomorphismus $\sigma' : L \to L(\beta)$ welche σ fortsetzt. Damit haben L und $L(\beta)$ den gleichen Grad über K somit folgt $L = L(\beta)$. □

Korollar V.7.11. *Sei L/K endlich und normal. Gegeben ein Zwischenkörper $K \subset F \subset L$ ein Zwischenkörper, dann ist L/F normal.*

Beweis. Nach dem Lemma ist L Zerfällungskörper von einem $f \in K[X]$. Dann ist L auch Zerfällungskörper von f über F. □

Bemerkung. Es ist nicht zwangsläufig auch F/K normal. Etwa im Fall $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ ist $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ nicht normal.

Korollar V.7.12. *Sei L/K endlich, dann gibt es eine Körpererweiterung N/L, so dass N/K normal ist.*

Beweis. Sei $L = K(\alpha_1, \ldots, \alpha_n)$ und $f = \prod f_i$ das Produkt der Minimalpolynome f_i der Elemente α_i. Dann setze N den Zerfällungskörper von f. □

Definition V.7.13. Sei L/K endlich, dann heißt ein Erweiterungskörper N von K *normale Hülle von L/K*, wenn N/K normal ist und für jede normale Körpererweiterung N'/K mit $K \subset N' \subset N$ gilt $N = N'$.

Satz V.7.14. *Die normale Hülle einer endlichen Körpererweiterung L/K ist eindeutig bis auf Isomorphie.*

Beweis. Seien N, N' zwei normale Hüllen und N Zerfällungskörper von $f \in K[X]$. Auch über N' zerfällt f in Linearfaktoren. Wie im Beweis von Kororllar V.7.3 gibt es einen Körperhomomorphismus $\sigma : N \to N'$, welcher die Inklusion $L \subset N'$ fortsetzt. Das Bild von σ ist normal über K, also ist σ auch surjektiv. □

Lemma V.7.15. *Sei L/K eine Körpererweiterung, $\sigma \in \mathrm{Gal}(L/K)$ und $\alpha \in L$, dann haben α und $\alpha' = \sigma(\alpha)$ das gleiche Minimalpolynom über K.*

Beweis. Sei $f = a_0 + a_1 X + \cdots + a_n X^n$ das Minimalpolynom von α, dann gilt $0 = \sigma(f(\alpha)) = \sigma(f)(\sigma(\alpha) = f(\alpha')$, wobei $\sigma(f) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n$. Also ist α' auch eine Nullstelle von f. □

Definition V.7.16. Sei L/K eine Körpererweiterung. Zwei Elemente α und α' heißen *konjugiert*, wenn α und α' über K das gleiche Minimalpolynom haben.

Lemma V.7.17. *Sei L/K normal und $\alpha, \alpha' \in L$. Dann sind α und α' genau dann konjugiert, wenn es ein Element $\sigma \in \mathrm{Gal}(L/K)$ mit $\alpha' = \sigma(\alpha)$ gibt.*

Beweis. Seien α und α' zwei Nullstellen eines irreduziblen normierten Polynoms f. Nach Satz V.7.2 gibt es einen Körperhomomorphimus $\sigma : K(\alpha) \to L$ mit $\sigma|_K = \mathrm{id}_K$ und $\sigma(\alpha) = \alpha'$. Da L/K normal kann dieser zu einem $\sigma : L \to L$ fortgesetzt werden (vgl. Beweis von Lemma V.7.5). Das ist das gesucht Element von $\mathrm{Gal}(L/K)$. □

Separable Erweiterungen

Lemma V.7.18. *Sei L/K endlich und separabel sowie $K \subset F \subset L$ ein Zwischenkörper, dann ist L/F und F/K separabel.*

Beweis. Direkt nach Definition ist auch F/K separabel. Sei $\alpha \in L$ mit Minimalpolynom f_F bzw. f_K über F bzw. K. Da f_F das Polynom f_K teil und f_K über dem algebraischen Abschluss keine doppelten Nullstellen hat, gilt das auch für f_F. □

Definition V.7.19. Sei $f = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$, dann definiere die *Ableitung von f* durch

$$f' = \sum_{i=0}^{n} i a_i X^{i-1} = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}\,.$$

Lemma V.7.20. *Seien $f, g \in K[X]$ und $\lambda \in K$, dann gilt*

(i) $(f+g)' = f' + g'$

(ii) $(fg)' = f'g + fg'$

(iii) $(\lambda f)' = \lambda f'$

Beweis. Übungsaufgabe. □

Lemma V.7.21. *Sei $f \in K[X]$ und α eine mehrfache Nullstelle im algebraischen Abschluss von K, dann gilt $f'(\alpha) = 0$. Falls f irreduzibel ist, dann ist f genau dann separabel, wenn $f' = 0$, d.h. das konstante Nullpolynom ist.*

Beweis. Über dem algebraischen Abschluss $\overline{K}$ zerfällt $f(X) = c(X-\alpha)\prod_i (X-\alpha_i)$ mit $\alpha, \alpha_i \in \overline{K}$ und $c \in K$. Wir berechnen

$$f'(X) = c\prod_i (X-\alpha_i) + c(X-\alpha)\Big(\prod_i (X-\alpha_i)\Big)'\,.$$

Also $f'(\alpha) = c\prod_i (X-\alpha_i)$ und daher

$$f'(\alpha) = 0 \quad \Longleftrightarrow \quad \alpha = \alpha_i \text{ für ein i.}$$

Sei nun f irreduzibel und nicht separabel, d.h. es hat eine doppelte Nullstelle $\alpha \in \overline{K}$. Dann ist α eine Nullstelle von f und f'. Da f das Minimalpolynom von α ist und $\deg f' < \deg f$ muss f' das Nullpolynom sein. □

Korollar V.7.22. *Sei K ein Körper.*

(i) Wenn $\operatorname{char} K = 0$*, dann ist jedes Polynom über* K *separabel.*

(ii) Wenn K *eine endliche Menge ist, dann ist jedes Polynom über* K *separabel.*

Insbesondere ist in beiden Fällen jede algebraische Körpererweiterung von K *separabel.*

Beweis. Sei f irreduzibel und nicht konstant.
Zu (i). Es gilt $\deg f' = \deg f - 1 \geq 0$, also ist f' nicht das Nullpolynom und somit f separabel.
Zu (ii). Da K endlich ist, ist automatisch $\operatorname{char}, K = p > 0$. In der Übungsaufgabe wird gezeigt, dass die Frobeniusabbildung

$$\Phi : K \to K\,, \qquad x \mapsto x^p\,,$$

ein Körperhomomorphismus ist. Da wieder K eine endliche Menge und Φ injektiv ist, folgt dass Φ auch surjektiv, also bijektiv, ist. Angenommen $f' = 0$, dann folgt mit Lemma V.7.23, dass $f(X) = \sum_i a_i X^{ip}$. Sei $b_i := \Phi^{-1}(a_i) \in K$, d.h. $b_i^p = a_i$, damit folgt wieder durch verwenden, dass Φ ein Körperhomomorphismus ist, dass

$$\big(\sum_i b_i X^i\big)^p = \sum_i b_i^p X^{ip} = \sum_i a_i X^{ip} = f(X)\,.$$

Also ist f nicht irreduzibel im Widerspruch zur Annahme. □

Lemma V.7.23. *Sei* K *ein Körper mit Charakteristik* $\operatorname{char} K = p > 0$ *und* $f \in K[X]$ *dann ist* $f' = 0$ *genau dann wenn*

$$f(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \cdots + a_{np} X^{np}\,,$$

d.h. mit anderen Worten $f \in K[X^p]$.

Beweis. Sei $f = \sum_i a_i X^i$. Nach Definition ist $f' = \sum_i i a_i X^{i-1}$ genau dann das Nullpolynom, wenn $i a_i = 0$ für alle i, d.h. wenn $a_i \neq 0$, dann muss $i = 0$ in K. Also nach Definition der Charakteristik ist $i = kp$ mit $k \in \mathbb{N}_0$. □

Galoiserweiterungen

Definition V.7.24. Gegeben seien ein Körper L und eine Untergruppe $G \subset \operatorname{Aut}(L) = \{\sigma : L \to L \mid \sigma \text{ ist ein Körperiso.}\}$. Wir definieren den *Fixkörper von* G durch

$$L^G = \{a \in L \mid \sigma(a) = a \;\forall\; \sigma \in G\}\,.$$

Bemerkung. Der Fixkörper L^G ist tatsächlich ein Körper, genauer ein Teilkörper von L.

Satz V.7.25 (Galoiskriterium)**.** *Sei* L/K *endlich. Dann ist äquivalent:*

(i) L/K *galois.*

(ii) $\operatorname{ord} \operatorname{Gal}(L/K) = [L : K]$.

(iii) L/K *ist normal und separabel.*

(iv) $L^{\mathrm{Gal}(L/K)} = K$.

Beweis. Die Äquivalenz $(i) \iff (ii)$ ist die Definition.
Wir zeigen $(ii) \Rightarrow (iii)$. Angenommen L/K ist nicht normal und separabel, dann gibt es ein $\alpha \in L$, so dass sein Minimalpolynom in L weniger Nullstellen als der Grad des Minimalpolynoms hat. Wir verfahren wie im Beweis von Lemma V.7.5 mit $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Ohne Einschränkung ist $\alpha = \alpha_1$ und wir setzen Schrittweise die Körperhomomorphimen fort. Nach Lemma V.7.2 gibt es im ersten Schritt, bei der Fortsetzung von $\sigma = \subset\colon K \to L$ zu $\sigma : K(\alpha_1) \to L$ allerdings weniger Möglichkeiten als der Grad $[K(\alpha_1) : K]$. Dieses Defizit kann später auch nicht mehr aufgeholt werden, denn bei jedem Schritt gibt es maximal $[K_j : K_{j-1}]$ viele Möglichkeiten zur Fortsetzung. Also gilt $\operatorname{ord}\mathrm{Gal}(L/K) < [L : K]$ im Widerspruch zu (ii).

Wir zeigen $(iii) \Rightarrow (iv)$. Sei $\alpha \in L^{\mathrm{Gal}(L/K)}$ und f sein Minimalpolynom. Wir haben in Lemma V.7.17 gesehen, dass die Nullstellen von f genau die Elemente der Menge $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\} = \{\alpha\}$ entsprechen. Damit hat f nur eine Nullstelle, ist von Grad 1 und daher $\alpha \in K$. Also folgt $L^{\mathrm{Gal}(L/K)} \subset K$ und daher (iv).

Wir zeigen $(iv) \Rightarrow (ii)$. Das folgt aus dem Lemma V.7.27 unten mit $H = \mathrm{Gal}(L/K)$. □

Korollar V.7.26. *Sei K ein Körper und L der Zerfällungskörper eines separablen Polynoms $f \in K[X]$, dann ist L/K galois.*

Beweis. Nach Lemma V.7.10 ist L/K normal und nach Voraussetzung separabel. □

Lemma V.7.27. *Sei L ein Körper und $H \subset \mathrm{Aut}(L)$ eine endliche Untergruppe, dann gilt*

$$[L : L^H] = \operatorname{ord} H\,,$$

damit ist L/L^H galois mit Galoisgruppe H.

Beweis. Setze $K = L^H$. Es gilt $H \subset \mathrm{Gal}(L/K)$ und nach Lemma V.7.5

$$\operatorname{ord} H \leq \operatorname{ord}\mathrm{Gal}(L/K) \leq [L : K]\,,$$

Sei $n = \operatorname{ord} H$ und $r = [L : K]$. Es genügt zu zeigen, dass $n = r$. Angenommen per Widerspruch $n < r$. Sei $H = \{\sigma_1, \ldots, \sigma_n\}$ und $b_1, \ldots, b_r \in L$ eine K-Basis. Das Gleichungsystem über L

$$\begin{cases} x_1\sigma_1(b_1) + x_2\sigma_1(b_2) + \cdots + x_r\sigma_1(b_r) = 0 \\ x_1\sigma_2(b_1) + x_2\sigma_2(b_2) + \cdots + x_r\sigma_2(b_r) = 0 \\ \quad\vdots \qquad\quad \vdots \qquad\qquad \vdots \\ x_1\sigma_n(b_1) + x_2\sigma_n(b_2) + \cdots + x_r\sigma_n(b_r) = 0\,, \end{cases} \tag{5}$$

hat weniger Gleichungen als Unbekannte $x_1, x_2, \ldots, x_r \in L$. Also gibt es mindestens eine nicht-triviale Lösung $(x_1, x_2, \ldots, x_r)$. Für jedesolche Lösung sei $N = N(x_1, x_2, \ldots, x_r)$

die Anzahl der j mit $x_j \neq 0$. Wähle eine nicht-triviale Lösung, so dass $1 \leq N(x_1, \ldots, x_r)$ minimal ist. Wir wenden σ_k auf jede Gleichungen von (5) an und erhalten für jedes $i = 1, \ldots, n$

$$0 = \sum_{j=1}^{r} \sigma_k(x_j)\sigma_k(\sigma_i(b_j)) = \sum_{j=1}^{r} \sigma_k(x_j)(\sigma_k \circ \sigma_i)(b_j)\,.$$

Die $\sigma_k \circ \sigma_i$ mit $i = 1, \ldots, n$ durchlaufen ganz H, also gibt für jedes i ein eindeutiges i', so dass $\sigma_k \circ \sigma_i = \sigma_{i'}$ und

$$0 = \sum_{j=1}^{r} \sigma_k(x_j)\sigma_{i'}(b_j)\,, \qquad \text{für alle } i' = 1, \ldots, n.$$

Damit ist das Tupel $(\sigma_k(x_1), \ldots, \sigma_k(x_r))$ auch eine Lösung von (5). Da (5) ein homogenes lineares Gleichungssystem ist, ist auch $(y_1, \ldots, y_r)$ mit $y_j = x_j - \sigma_k(x_j)$ eine Lösung von (5). Nach möglichen vertauschen der Basiselemente und Skalieren der Lösung, nehmen wir an, dass $x_1 = 1$. Damit ist auch $y_1 = 1 - \sigma_k(1) = 0$ und $N(y_1, \ldots, y_r) < N(x_1, \ldots, x_r)$. Nach minimaler Wahl von $(x_1, \ldots, x_r)$ muss $(y_1, \ldots, y_r)$ die triviale Lösung sein. Damit folgt

$$x_j = \sigma_k(x_j)\,,$$

für alle $j = 1, \ldots, r$ und $k = 1, \ldots, n$. Wir erhalten, dass $x_j \in K$ und für k, so dass $\sigma_k = \mathrm{id}_L$ erhalten wir eine nicht-triviale Lösung

$$0 = x_1 b_1 + x_2 b_2 + \cdots + x_r b_r\,,$$

mit $x_1, \ldots, x_r \in K$ im Widerspruch zur K-linearen Unabhängigkeit von $b_1, \ldots, b_r$. □

Theorem V.7.28 (Hauptsatz der Galoistheorie)**.** *Sei L/K eine endliche Galoiserweiterung. Bezeichne mit $\mathcal{G}$ bzw. $\mathcal{K}$ die Menge aller Untergruppen der Galoisgruppe bzw. Zwischenkörper von L/K. Es gilt*

(i) Die Abblidungen

$$\begin{aligned} \kappa :&\mathcal{G} \to \mathcal{K}\,, \quad G \mapsto L^G \\ \gamma :&\mathcal{K} \to \mathcal{G}\,, \quad F \mapsto \mathrm{Gal}(L/F)\,, \end{aligned}$$

sind invers zueinander, insbesondere bijektiv, und inklusionsumkehrend;

(ii) für jeden Zwischenkörper $F \in \mathcal{K}$ ist L/F galois und für jede Untergruppe $H \in \mathcal{G}$ gilt

$$[L : L^H] = \operatorname{ord} H\,, \qquad [L^H : K] = [\mathrm{Gal}(L/K) : H]\,;$$

(iii) für jeden Zwischenkörper $F \in \mathcal{K}$ ist F/K genau dann normal (und damit auch galois), wenn $H = \mathrm{Gal}(L/F)$ ein Normalteiler von $\mathrm{Gal}(L/K)$ ist. In diesem Fall ist dann

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

Beweis. Für Zwischenkörper $K \subset F_1 \subset F_2 \subset L$ gilt

$$\mathrm{Gal}(L/F_1) = \{\sigma \mid \sigma|_{F_1} = \mathrm{id}\} \supset \{\sigma \mid \sigma|_{F_2} = \mathrm{id}\} = \mathrm{Gal}(L/F_2)\,.$$

Für Untergruppen $H_1 \subset H_2 \subset \mathrm{Gal}(L/K)$ gilt

$$L^{H_1} = \{\alpha \mid \sigma(\alpha) = \alpha \;\forall\; \sigma \in H_1\} \supset \{\alpha \mid \sigma(\alpha) = \alpha \;\forall\; \sigma \in H_2\} = L^{H_2}\,.$$

Sei nun $F \in \mathcal{K}$. Da nach Voraussetzung L/K galois ist, gilt nach dem Kriterium, dass L/K normal und separabel ist. Also gilt nach Korollar V.7.11 und Lemma V.7.18, dass auch L/F normal und separabel ist, also auch galois ist und mit dem Kriterium gilt auch $[L : F] = \mathrm{ord}\,\mathrm{Gal}(L/F)$ sowie

$$\kappa(\gamma(F)) = L^{\mathrm{Gal}(L/F)} = F\,.$$

Sei nun $H \in \mathcal{G}$ und $F = L^H$. Als Zwischenkörper ist wieder L/F galois und mit Lemma V.7.27, folgt $H = \mathrm{Gal}(L/F)$, d.h.

$$\gamma(\kappa(H)) = \mathrm{Gal}(L/L^H) = H\,.$$

Die Formeln für $[L^H : K]$ folgen aus der Gradformel für Zwischenkörper und Indexformel für Untergruppen. Damit wurde (i) und (ii) gezeigt.

Sei nun $F \in \mathcal{K}$, so dass F/K normal. Da mit Lemma V.7.18 auch F/K separabel ist, ist bereits F/K galois. Außerdem bildet jedes $\sigma \in \mathrm{Gal}(L/K)$ Elemente $\alpha \in F$ auf Elemente von F ab, da α und $\sigma(\alpha)$ das gleiche Minimalpolynom über K haben und wegen Normalität beide Nullstellen in F liegen müssen. Wir erhalten die Abbildung

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)\,, \qquad \sigma \mapsto \sigma|_F\,,$$

mit Kern $\mathrm{Gal}(L/F)$, also ist $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ ein Normalteiler. Die Abbildung ist auch surjektiv, denn da L/K normal ist, lässt sich jedes $\sigma : F \to F \subset L$ zu einem $\sigma \in \mathrm{Gal}(L/K)$ wie im Beweis V.7.5 fortsetzen. Damit folgt die Formel in (iii) aus dem Homomorphiesatz.

Sei umgekehrt $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ ein Normalteiler. Wir müssen zeigen, dass für jedes $\alpha \in F$ und $\sigma \in \mathrm{Gal}(L/K)$ auch $\sigma(\alpha) \in F$, denn damit ist F/K normal, da $\sigma(\alpha)$ alle Nullstellen des Minimalpolynoms von α durläuft. Sei dazu $\tau \in \mathrm{Gal}(L/F)$ beliebig. Nach Voraussetzung gilt

$$\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/F) \qquad \Rightarrow \qquad \sigma^{-1}\tau\sigma(\alpha) = \alpha\,.$$

Das zeigt, dass $\sigma(\alpha) \in L^{\mathrm{Gal}(L/F)} = F$ wie gewünscht. □

Zyklotomische Körper

Sei L ein Körper. Ein Element $\zeta \in L$ heißt

(i) *d-te Einheitswurzel*, wenn $\zeta^d = 1$.

(ii) *primitive d-te Einheitswurzel*, wenn die (multiplikative) Ordnung von ζ gleich d ist.

Wir bezeichnen mit $\mu_d(L) \subset L^\times$ die Untergruppe der d-ten Einheitswurzeln.

Beispiel V.7.29. (i) $\zeta = \exp(2\pi i/d)$ ist eine primitive d-te Einheitswurzel in $\mathbb{C}$.

(ii) In $\mathbb{F}_q$ sind alle Elemente in $\mathbb{F}_q^\times$ bereits $q-1$-te Einheitswurzeln.

Lemma V.7.30. *Sei L ein Körper, der eine primitive d-te Einheitswurzel enthält, dann ist*

$$\mu_d(L) \cong \mathbb{Z}/d\mathbb{Z}\,.$$

Dabei werden primitive d-te Einheitswurzeln auf die Einheiten $(\mathbb{Z}/d\mathbb{Z})^\times$ abgebildet.

Beweis. Sei $\zeta \in L$ eine primitive d-te Einheitswurzel. Alle d-te Einheitswurzeln sind die d Nullstellen $1, \zeta, \zeta^2, \ldots, \zeta^{d-1}$ von X^d-1. Somit erhalten wir einen Gruppenisomorphismus

$$\mu_d(L) \to \mathbb{Z}/d\mathbb{Z}\,, \qquad \zeta^k \mapsto k\,.$$

Jeder Gruppenisomorphismus erhält die Ordnung der Elemente. Die Elemente mit Ordnung d in $\mathbb{Z}/d\mathbb{Z}$ entsprechen genau den Einheiten. □

Satz V.7.31 (Zyklotomische Körper)**.** *Sei K ein Körper und $L = K(\zeta)$ für eine primitive d-te Einheitswurzel ζ. Dann ist L der Zerfällungskörper von X^d-1, die Erweiterung ist galois mit*

$$\mathrm{Gal}(L/K) \cong H \subset (\mathbb{Z}/d\mathbb{Z})^\times\,.$$

Insbesondere ist die Galoisgruppe abelsch. Falls $\mathbb{Q} = K$, dann gilt

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^\times\,.$$

Beweis. Das Polynom X^d-1 hat die Nullstellen $1, \zeta, \zeta^2, \ldots, \zeta^{d-1}$, also ist L Zerfällungskörper. Sei f das Minimalpolynom von ζ. Dann ist f ein Teiler von X^d-1 und hat somit paarweise verschiedene, also $\deg f$ viele Nullstellen. Damit ist die Erweiterung galois. Jedes $\sigma \in \mathrm{Gal}(L/K)$ ist nach Satz V.7.2 eindeutig durch den Wert $\sigma(\zeta)$ festgelegt. Dies ist erneut eine primitive d-te Einheitswurzel, also $\sigma(\zeta) = \zeta^{n_\sigma}$ für ein $n_\sigma \in (\mathbb{Z}/d\mathbb{Z})^\times$. Die Abbildung

$$\mathrm{Gal}(L/K) \to (\mathbb{Z}/d\mathbb{Z})^\times\,, \qquad \sigma \mapsto n_\sigma\,, \tag{6}$$

ist somit injektiv. Bleibt zu zeigen, dass dies ein Gruppenhomomorphismus ist. Seien $\sigma, \tau \in \mathrm{Gal}(L/K)$. Wir berechnen

$$\zeta^{n_{\sigma\circ\tau}} = (\sigma\circ\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{n_\tau}) = \sigma(\zeta)^{n_\tau} = \left(\zeta^{n_\sigma}\right)^{n_\tau} = \zeta^{n_\sigma n_\tau}\,.$$

Daher $n_{\sigma\circ\tau} = n_\sigma n_\tau$ und die Abbildung ist ein Gruppenhomomorphismus. Bleibt der Fall $K = \mathbb{Q}$. Sei p eine Primzahl welche d nicht teilt. Wir behaupten, dass dann auch ζ^p eine Nullstelle von f ist. Betrachte die Faktorisierung

$$X^d - 1 = f(X)h(X)\,,$$

wobei nach Lemma von Gauß V.6.7 $f, h \in \mathbb{Z}[X]$. Angenommen ζ^p ist keine Nullstelle von $f(X)$, dann aber notwendigerweise eine Nullstelle von $h(X)$. Also ist ζ eine Nullstelle von $h(X^p)$. Da $f(X)$ das Minimalpolynom von ζ ist, folgt

$$f(X) \mid h(X^p)\,, \qquad h(X^p) = f(X)g(X)\,,$$

für ein $g(X) \in \mathbb{Z}[X]$ (wieder mit dem Lemma von Gauß V.6.7). Wir reduzieren modulo p und mit Verwendung des Frobenius sowie des kleinen Fermats $a^p = a$ in $\mathbb{F}_p$ erhalten wir

$$\bar{h}(X)^p = \bar{h}(X^p) = \bar{f}(X)\bar{g}(X)\,,$$

wobei $\bar{f}(X), \bar{g}(X), \bar{h}(X) \in \mathbb{F}_p[X]$ die Polynome mit Koeffizienten reduziert modulo p bedeuten. Wir schließen, dass jede Nullstelle von $\bar{f}$ auch eine Nullstelle von $\bar{h}$ ist, und daher $X^d - 1$ über dem algebraischen Abschluss von $\mathbb{F}_p$ doppelte Nullstellen hat. Das kann aber nicht sein, da p kein Teiler von d ist und somit $X^d - 1$ keine doppelten Nullstellen hat. Nach Widerspruch folgt also, dass auch ζ^p eine Nullstelle von $f(X)$ ist.

Sei nun ζ^n eine beliebige primitive d-te Einheitswurzel. Nach dem Lemma muss gelten, dass $n \in \left(\mathbb{Z}/d\mathbb{Z}\right)^\times$, d.h. $ggT(d, n) = 1$. Damit folgt für eine Primfaktorzerlegung $n = p_1 p_2 \cdots p_r$ (wobei Widerholungen möglich sind), dass $p_i \nmid d$. Nach den vorherigen Argument sind also alle $\zeta^{p_1}, \left(\zeta^{p_1}\right)^{p_2} = \zeta^{p_1 p_2}, \ldots, \zeta^{n=p_1 p_2 \cdots p_r}$ Nullstellen von f und nach dem Fortsetzungssatz V.7.2 gibt es ein $\sigma \in \mathrm{Gal}(L/K)$, so dass $\sigma(\zeta) = \zeta^n$. Damit ist die Abbildung (6) auch surjektiv. □

Definition V.7.32. Wir nennen das Minimalpolynom über $\mathbb{Q}$ der primitiven d-te Einheitswurzeln, das *d-te zyklotomische Polynom*

$$\Phi_d(X) = \prod_{\mathrm{ord}\,\zeta = d} X - \zeta\,,$$

wobei das Produkt über alle primitiven d-ten Einheitswurzeln ζ in $\mathbb{C}$ läuft. Der Körper

$$\mathbb{Q}(\zeta) \cong \mathbb{Q}[X]/\Phi_d\,,$$

heißt *zyklotomischer Körper*. Nach dem letzten Satz gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(d)$, wobei $\varphi(d) = \mathrm{ord}\left(\mathbb{Z}/d\mathbb{Z}\right)^\times$ die Eulsche φ-Funktion ist.

d-te Wurzeln

Satz V.7.33 (Kummererweiterungen)**.** *Sei K ein Körper welcher eine d-te Einheitswurzel enthält, $a \in K$ sowie $L = K(\beta)$ wobei β eine Nullstelle von $X^d - a$ ist. Dann ist L der Zerfällungskörper von $X^d - a$, die Erweiterung L/K ist galois mit*

$$\mathrm{Gal}(L/K) \cong H \subset \mathbb{Z}/d\mathbb{Z}\,.$$

Insbesondere ist die Galoisgruppe abelsch.

Beweis. Sei ζ eine primitive d-te Einheitswurzel in K. Man überprüft direkt, dass $\beta, \zeta\beta, \ldots, \zeta^{d-1}\beta$ alle d Nullstellen von $X^d - a$ sind, womit L der Zerfällungskörper ist. Das Minimalpolynom f von β teilt $X^d - a$ und zerfällt in L in paar-weise verschiedene $\deg f$ viele Nullstellen. Also ist L/K galois. Wir betrachten

$$\mathrm{Gal}(L/K) \to \mu_d(L)\,, \qquad \sigma \mapsto \frac{\sigma(\beta)}{\beta}\,.$$

Diese Abbildung ist injektiv, denn $\sigma(\beta)$ legt σ eindeutig fest. Dies ist auch ein Gruppenhomomorphismus, denn sei für σ, τ die Zahlen, $n_\sigma, n_\tau \in \mathbb{Z}/d\mathbb{Z}$ definiert durch $\sigma(\beta) = \zeta^{n_\sigma}\beta$ und $\tau(\beta) = \zeta^{n_\tau}\beta$, dann folgt

$$\beta^{-1}(\sigma \circ \tau)(\beta) = \beta^{-1}(\sigma(\tau(\beta)) = \beta^{-1}\sigma(\zeta^{n_\tau}\beta) = \beta^{-1}\zeta^{n_\tau}\zeta^{n_\sigma}\beta = \zeta^{n_\tau + n_\sigma}\,,$$

Damit folgt die Gruppenhomomorphieeigenschaft. □

Endliche Körper

Satz V.7.34. *Sei $\mathbb{F}_q$ der endlicher Körper mit q vielen Elementen und Charakteristik p, dann ist $\mathbb{F}_q/\mathbb{F}_p$ galois mit zyklischer Galoisgruppe.*

Beweis. Hausaufgabe. □

Galoisgruppe S_5

Nicht alle Galoisgruppen sind abelsch.

Lemma V.7.35. *Sei L der Zerfällungskörper von $f(X) = X^5 - 4X + 2$ über $K = \mathbb{Q}$, dann ist L/K galois mit*

$$\mathrm{Gal}(L/K) \cong S_5$$

Beweis. Da L der Zerfällungskörper ist und $\mathbb{Q}$ Charakteristik gleich 0 hat, ist L/K normal und separabel, also galois. Nach dem Eisensteinkriterium mit $p = 2$ ist $f(X)$ irreduzibel. Sei α eine Nullstelle von f, dann gilt nach Gradformel

$$\mathrm{ord}\,\mathrm{Gal}(L/K) = [L : K] = [L : K(\alpha)][K(\alpha) : K] = k \cdot 5\,,$$

mit $k \in \mathbb{N}$. Insbesondere ist 5 ein Teiler der Ordnung der Galoisgruppe. Wir setzen den Beweis nach einem kurzen Einschub über Gruppentheorie fort. □

Sei G eine Gruppe. Wir definieren das *Zentrum*

$$Z(G) = \{h \in G \mid hg = gh \;\forall\; g \in G\}$$

und für ein $a \in G$ den *Zentralisator*

$$Z_a = \{g \in G \mid ga = ag\}\,.$$

Zwei Elemente $a, b \in G$ heißen *konjugiert*, schreibe $a \sim b$, wenn $b = gag^{-1}$ für ein $g \in G$. Man sieht leicht, dass $\sim$ eine Äquivalenzrelation auf G definiert. Wir setzen

$$C\ell(a) := \{b \in G \mid a \sim b\},$$

die sogennante *Konjugationsklasse*, d.h. die Äquivalenzklasse von a bezüglich $\sim$.

Satz V.7.36 (Klassenformel)**.** *Sei G eine endliche Gruppe, dann gibt es Elemente $a_1, \ldots, a_k \in G$ und es gilt*

$$\operatorname{ord} G = \operatorname{ord} Z(G) + \sum_{i=1}^{k} [G : Z_{a_i}], \tag{7}$$

wobei $Z_{a_1}, \ldots, Z_{a_k} \subsetneq G$ echte Untergruppen sind.

Beweis. Wir behaupten, dass die Abbildung

$$\phi : G/Z_a \to C\ell(a), \qquad gZ_a \mapsto gag^{-1},$$

eine Bijektion ist. In der Tat ist ϕ wohl-definiert, denn wenn $gZ_a = hZ_b$, dann $h = gz$ für ein $z \in Z_a$, und demnach $hah^{-1} = gzaz^{-1}g^{-1} = gag^{-1}$. Die Umkehrabbildung ist $gag^{-1} \mapsto gZ_a$. Diese ist wieder wohl-definiert, denn wenn $gag^{-1} = hah^{-1}$, dann $g^{-1}hah^{-1}g = a$, also $h^{-1}g \in Z_a$ bzw. $h = gz$ für ein $z \in Z_a$, womit $gZ_a = hZ_a$. Aus der Bijektion erhalten wir, dass $C\ell(a)$ genau $[G : Z_a]$ viele Elemente enthält.

Wie für jede Äquivalenzrelation sind je zwei Konjugationsklassen entweder gleich oder disjunkt. Es gilt $C\ell(a) = \{a\}$ genau dann wenn $a \in Z(G)$. Für die übrigen Äquivalenzklassen wählen wir Repräsentanten $a_1, \ldots, a_k \in G$, so dass wir eine disjunkte Zerlegung erhalten

$$G = Z(G) \cup C\ell(a_1) \cup C\ell(a_2) \cup \ldots \cup C\ell(a_k).$$

Damit erhalten wir (7) durch abzählen. □

Ausgestattet mit der Klassenformel können wir eine teilweise Umkehrung des Satzes von Lagrange beweisen.

Korollar V.7.37. *Sei G eine endliche Gruppe und $p \in \mathbb{N}$ eine Primzahl, so dass $p \mid \operatorname{ord} G$, dann gibt es eine Element in G mit Ordnung gleich p.*

Beweis. Wir zeigen die Aussage zunächst für abelsche Gruppen. Dazu reicht es aus ein Element der Ordnung pk zu finden, dann die k-fache Potenz dieses Elements hat Ordnung p. Sei nun $e \neq g \in G$ mit $p \nmid \operatorname{ord} g$, dann hat der Quotient $\overline{G} = G/\langle g \rangle$ weniger Elemente als G und es gilt $p \mid \overline{G}$. Nach Induktion nach der Gruppenordnung enthält $\overline{G}$ ein Element $h\langle g \rangle \in G/\langle g \rangle$ von Ordnung pk. Damit folgt $h^{pk} = g^{\ell}$ für ein $\ell \in \mathbb{N}$. Damit hat $h^{k \operatorname{ord} g}$ die Ordnung p wie gewünscht. Wir kommen zum allgemeinen Fall. Wir führen Induktion nach Gruppenordnung über alle Gruppen. Sei nun G eine Gruppe und wir nehmen an, dass die Aussage schon für alle Gruppen H mit $\operatorname{ord} H < \operatorname{ord} G$ bewiesen

wurde. Betrachte die Gleichung (7). Entweder teilt p die Ordnung von Z_{a_i} für ein i, womit wir ein Element von Ordnung p darin finden nach Induktionsvoraussetzung oder $p \nmid \operatorname{ord} Z_{a_i}$ für alle i. Dann teilt aber nach Satz Lagrange $p \mid \operatorname{ord} G = \operatorname{ord} Z_{a_i}[G : Z_{a_i}]$, also $p \mid [G : Z_{a_i}]$ für alle i nach Euklidischem Lemma. Nach der Klassenformel (7) also auch $p \mid \operatorname{ord} Z(G)$. Nun ist $Z(G)$ eine abelsche Gruppe mit $p \mid \operatorname{ord} Z(G)$ und wir haben in solchen bereits ein Element von Ordnung p gefunden. □

Bevor wir zum Beweis zurückkehren brauchen wir noch ein Lemma.

Lemma V.7.38. *Sei L der Zerfällungskörper eines irreduziblen Polynoms $f \in \mathbb{Q}[X]$ mit $\deg f = n$, dann gilt $\operatorname{Gal}(L/K) \cong G \subset S_n$.*

Beweis. Nach Fortsetzungssatz V.7.2 ist jedes Element $\sigma \in \operatorname{Gal}(L/K)$ eindeutig durch die Werte der Nullstellen $M = \{\alpha_1, \ldots, \alpha_n\}$ von f bestimmt. Wir erhalten eine injektive Abbildung

$$\operatorname{Gal}(L/K) \to S(M)\,, \qquad \sigma \mapsto (\alpha_i \mapsto \sigma(\alpha_i))\ ,$$

wobei wir mit $S(M)$ die Gruppe der Bijektionen von M bezeichnen. Es ist leicht gezeigt, dass dies ein Gruppenhomomorphismus ist und $S(M) \cong S_n$. □

Fortsetzung Beweis von Lemma V.7.35. Wir identifizieren nach V.7.38, die Galoisgruppe $\operatorname{Gal}(L/K)$ mit einer Untergruppe $G \subset S_5$. Außerdem wissen wir nach Korollar V.7.37, dass G ein Element der Ordnung 5 enthält. Wir führen eine Kurvendiskussion von f durch. Wir erhalten

x	-2	-1	0	1	2
$f(x)$	-22	5	2	-1	26

Demach gibt es mindestens drei reelle Nullstellen nach dem Zwischenwertsatz. Für die Extrempunkte berechnen wir $f'(X) = 5X^4 - 4$. Also gibt es genau ein lokales Maximum und Minimum bei $-\sqrt[4]{4/5}$ bzw. $\sqrt[4]{4/5}$. Wir schließen, dass f genau drei reelle Nullstellen hat. Die anderen beiden sind komplex und zueinander komplex konjugiert. Damit ist die komplexe Konjugation ein Element der Galoisgruppe G.

Wir haben gezeigt, dass $G \subset S_5$ ein Element τ von Ordnung 5 und κ von Ordnung 2. Nach Umbenennen der Zahlen und durch mögliches Ersetzen von τ mit einer Potenz von τ gilt $\kappa = (1\ 2)$ und $\tau = (1\ 2\ 3\ 4\ 5)$. Wir berechnen weitere Elemente in G

$$\tau^2 = (1\ 3\ 5\ 2\ 4)\,, \quad \tau^3 = (1\ 4\ 2\ 5\ 3) \quad \text{und} \quad \tau^4 = (1\ 5\ 4\ 3\ 2)\,.$$

Für alle $\sigma \in S_5$ gilt $\sigma\,(1\ 2)\sigma^{-1} = (\sigma(1)\ \sigma(2))$. Damit erhalten wir weitere Elemente in G

$$(2\ 3) = \tau(1\ 2)\tau\,, \quad (3\ 4) = \tau^2(1\ 2)\tau^{-2}\,, \quad (4\ 5) = \tau^3(1\ 2)\tau^{-3}\,, \quad (1\ 5) = \tau^4(1\ 2)\tau^{-4}\,,$$

und mit diesen erhalten wir wiederum

$$(1\ 3) = (2\ 3)(1\ 2)(2\ 3)\,, \quad (1\ 4) = (3\ 4)(1\ 3)(3\ 4)\,, \quad (1\ 5) = (4\ 5)(1\ 3)(4\ 5).$$

Damit liegt jede beliebige Vertauschung $(n\ m) = (1\ n)(1\ m)(1\ n)$ in G wobei hier $n, m \neq 1$. Dies sind die Erzeuger von S_5, also gilt $G = S_5$. □

Auflösbarkeit durch Radikale

Sei $f \in \mathbb{Q}[X]$. Wir wollen die Lösungen der Gleichung $f(X) = 0$ durch eine Formel in den Koeffizienten von f mit den Operationen: Addition, Multiplikation, Inversenbildung sowie n-te Wurzelziehen $\sqrt[n]{\cdot}$ ausdrücken. Das funktioniert im Fall $\deg f = 2$ (quadratische Lösungsformel) sowie auch $\deg f = 3, 4$. Für Gleichungen höheren Grades funktioniert des im Allgemeinen nicht.

Definition V.7.39. Das Element $\alpha \in \overline{\mathbb{Q}}$ (der Körper K, bzw. das Polynom $f \in \mathbb{Q}[X]$) heißt *durch Radikale auflösbar*, wenn es eine Körperkette gibt

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \,,$$

$\alpha \in K_n$ ($K \subset K_n$, bzw. der Zerfällungskörper von f in K_n enthalten ist) und $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ wobei $a_i \in K_i$ und $n_i \in \mathbb{N}$.

Definition V.7.40. Eine Gruppe G heißt *auflösbar*, wenn es eine Kette von Untergruppen gibt

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G \,,$$

so dass $G_{i+1} \subset G_i$ ein Normalteiler und der Quotient G_i/G_{i+1} abelsch ist.

Lemma V.7.41. *Untergruppen und Quotienten von auflösbaren Gruppen sind auflösbar.*

Beweis. Sei $H \subset G$ eine Untergruppe einer auflösbaren Gruppe G, dann setze $H_i := H \cap G_i$. Es ist $H_{i+1} \subset H_i$ Normalteiler und nach Noetherschen Isomorphiesatz gilt

$$\frac{H_i}{H_{i+1}} = \frac{H \cap G_i}{H \cap G_{i+1}} = \frac{H \cap G_i}{\big(H \cap G_i\big) \cap G_{i+1}} \cong \frac{\big(H \cap G_i\big)G_{i+1}}{G_{i+1}} \xrightarrow{\text{inj}} \frac{G_i}{G_{i+1}} \,,$$

wobei die letzte Abbildung injektiv ist. Damit ist H_i/H_{i+1} isomorph zu einer Untergruppe einer abelschen Gruppe und demnach abelsch.

Sei nun $H = G/N$ ein Quotient, wobei $N \subset G$ ein Normalteiler ist. Diesmal setze $H_i := (G_i \cap N)/N$. Wieder ist $H_{i+1} \subset H_i$ ein Normalteiler und mit dem zweiten Noetherschen Isomorphiesatz gilt

$$\frac{G_i}{G_{i+1}} = \frac{G_i/\big(G_{i+1} \cap N\big)}{G_{i+1}/\big(G_{i+1} \cap N\big)} \xrightarrow{\text{surj}} \frac{G_i/\big(G_i \cap N\big)}{G_{i+1}/\big(G_{i+1} \cap N\big)} = \frac{H_i}{H_{i+1}} \,,$$

wobei die Abbildung surjetiv ist. Damit ist H_i/H_{i+1} ein Quotient einer abelschen Gruppe und demnach abelsch. In beiden Fällen haben wir gezeigt, dass H wieder auflösbar ist. □

Theorem V.7.42. *Sei $K/\mathbb{Q}$ eine endliche Erweiterung mit normaler Hülle L, dann ist äquivalent*

(i) K ist durch Radikale auflösbar.

(ii) $\mathrm{Gal}(L/\mathbb{Q})$ *ist auflösbar.*

Beweis. Wir beweisen nur $(i) \Rightarrow (ii)$. Im ersten Schritt zeigen wir, dass wir dass wir für jedes i eine endliche Erweiterung L_i/K_i finden, so dass $L_i/\mathbb{Q}$ normal ist und L_i aus K_i durch Adjungieren von Wurzeln entsteht. Dazu sei nach Induktion bereits L_i gefunden, dann ist L_i der Zerfällungskörper eines Polynoms $f \in \mathbb{Q}[X]$. Wir wissen, dass $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ wobei $a_i \in K_i$ und $n_i \in \mathbb{N}$, dann setze

$$g(X) = \prod_{\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})} X^{n_i} - \sigma(a_i)\,.$$

Da für jedes $\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})$ gilt $\sigma(g) = g$ und $L_i/\mathbb{Q}$ galois ist, liegt jeder Koeffizient von g im Fixkörper, also $g \in \mathbb{Q}[X]$. Setze nun L_{i+1} als den Zerfällungskörper von fg. Damit ist $L_{i+1}/\mathbb{Q}$ normal und entsteht aus L_i durch adjungieren von n_i-ten Wurzeln. Wir haben so diesen Schritt gezeigt.

Nach dem letzten Schritt nehmen wir ohne Einschränkung nach möglichen Verlängern der Kette an, dass $K_n/\mathbb{Q}$ normal ist. Damit ist $L \subset K_n$ nach der universellen Eigenschaft der normalen Hülle. Setze $d := n_1 n_2 \cdots n_n$ und sei ζ eine primitive d-te Einheitswurzel. Dann ist auch $K_n(\zeta)/\mathbb{Q}$ normal. Wir betrachten die Körperkette bestehend aus $M_i := K_i(\zeta)$. Wegen $M_{i+1} = M_i(\sqrt[n_i]{a_i})$ ist dies wieder eine Kette von Körper, wie in der Definition V.7.39 mit $L \subset M_n$. Auch ensteht $M_0 = \mathbb{Q}(\zeta)$ aus $\mathbb{Q}$ durch adjungieren einer Wurzel. Die Erweiterungen M_{i+1}/M_i sind nun Kummererweiterungen wie in Satz V.7.33, denn M_i enthält mit ζ auch eine primitive n_i-te Einheitswurzel, nämlich ζ^{d/n_i}. Somit ist M_{i+1}/M_i galois mit abelscher Galoisgruppe. Sei $H_i := \mathrm{Gal}(M_n/M_i)$ die Folge von Untergruppen der Körperkette. Nach dem Hauptsatz der Galoistheorie ist H_{i+1} ein Normalteiler in H_i, und es gilt

$$\mathrm{Gal}(M_{i+1}/M_i) \cong H_i/H_{i+1}\,.$$

Damit ist $\mathrm{Gal}(M_n/\mathbb{Q})$ auflösbar und als Quotient auch $\mathrm{Gal}(L/\mathbb{Q})$. □

Um diese Aussage auf unsere Ausgangsfrage anzuwenden, zeigen wir nun noch, dass S_5 nicht auflösbar ist.

Satz V.7.43. *Die symmetrische Gruppe S_5 ist nicht auflösbar.*

Beweis. Wir erinnern, dass jedes Element in S_5 als eine Verknüpfung von Vertauschungen geschrieben werden kann und dass $A_5 \subset S_5$ die Untergruppe aus allen Elementen ist, welche als eine gerade Anzahl von Vertauschungen geschrieben werden kann. Im ersten Schritt zeigen wir, dass A_5 von allen 3-Zykeln erzeugt ist, d.h. Elementen der Ordnung 3. Sei dazu $(m\ n)(k\ \ell)$ ein Produkt aus zwei Vertauschungen. Es gibt zwei Fälle, entweder $\{m,n\} \cap \{k,\ell\} = \emptyset$ oder $\{m,n\} \cap \{k,\ell\} \neq \emptyset$ und wir schreiben entsprechend

$$\begin{aligned}
&(m\ n)(k\ \ell) = (m\ n)(n\ k)(n\ k)(k\ \ell) = (m\ n\ k)(n\ k\ \ell), \quad \text{bzw.}\\
&(m\ n)(k\ \ell) = (m\ n)(n\ \ell) = (m\ n\ \ell)\,,
\end{aligned}$$

wobei wir im zweiten Fall ohne Einschränkung annehmen, dass $n = k$. Wir haben gezeigt, dass jedes Element in A_5 als Verknüpfung von 3-Zykeln geschrieben werden kann.

Wir zeigen nun, dass A_5 und damit nach Lemma V.7.41 auch S_5 nicht auflösbar ist. Dazu genügt es zu zeigen, dass für jeden 3-Zykel $\tau \in A_5$ es Elemente $\gamma, \kappa \in A_5$ gibt, so dass

$$\tau = \gamma\kappa\gamma^{-1}\kappa^{-1}\,, \tag{8}$$

denn mit dieser Gleichung ist das Bild von τ und nach dem ersten Schritt das Bild jedes Elementes in einem beliebigen abelschen Quotienten von A_5 trivial. Damit ist nur die triviale Gruppe als abelscher Quotient möglich. Insbesondere ist A_5 selbst nicht abelsch. Wäre nun A_5 auflösbar, dann gibt es eine Kette von Normalteilern $G_i \subset A_5$, wie in der Definition. Insbesondere ist G_i/G_{i+1} abelsch. Also muss $G_i = A_5$ für alle i. Das ist ein Widerspruch zu $G_n = \{e\}$.

Wir müssen noch die Gleichung (8) zeigen. Ohne Einschränkung ist $\tau = (1\ 2\ 3)$. Wir definieren $\gamma = (1\ 4\ 3)$ und $\kappa = (3\ 2\ 5)$ und berechnen

$$(1\ 4\ 3)(3\ 2\ 5)(1\ 4\ 3)^{-1}(3\ 2\ 5)^{-1} = (1\ 2\ 5)(3\ 2\ 5)^{-1} = (1\ 2)(2\ 5)(2\ 5)(3\ 2) = (1\ 2\ 3)\,.$$

Damit ist der Beweis beendet.

□

Korollar V.7.44. *Es gibt keine Lösungsformel für die Gleichung* $X^5 - 4X + 2 = 0$.

Beweis. Sei per Widerspruch $X^5 - 4X + 2$ durch Radikale auflösbar. Dann ist mit Theorem V.7.42 und Lemma V.7.35 die Gruppe S_5 auflösbar. Das steht im Widerspruch zum letzten Satz. □

Literatur

[1] J. Kramer und A. Pippich, *Von den natürlichen Zahlen zu den Quarternionen*, Springer Berlin, 2022.

[2] S. Lang, *Algebra*, Springer Berlin, 2000.