Einführung in die Algebra

Sommersemester 2018

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

Druckversion vom 16. Juli 2018, 10:43 Uhr.

Diese Vorlesung setzt die Vorlesung „Einführung in die Zahlentheorie und algebraische Strukturen“ aus dem Wintersemester 2017/2018 fort. Sie behandelt zwei Hauptthemen: Einerseits werden (insbesondere endliche) Gruppen genauer studiert; auf der anderen Seite geht es um algebraische Körpererweiterungen. Für die Konstruktion solcher Körpererweiterungen spielen die im vorigen Semester genauer betrachteten Polynomringe eine wesentliche Rolle.

Einige Abschnitte in diesem Skript sind kleiner gedruckt. Dabei kann es sich um ergänzende Bemerkungen zur Vorlesung handeln, die nicht zum eigentlichen Stoff gehören, die Sie aber vielleicht trotzdem interessant finden. Manchmal handelt es sich auch um Beweise, die in der Vorlesung nicht ausgeführt werden, zum Beispiel weil sie relativ lang sind und fürs Verständnis nicht unbedingt benötigt werden, die aber doch der Vollständigkeit halber oder auch als Anregung etwa für Übungsaufgaben im Skript stehen sollten.

Einige der Definitionen und Sätze (oder eventuell Lemmas und Folgerungen) sind mit einem Stern markiert. In der Klausur wird jeweils eine der Definitionen und einer der Sätze abgefragt werden.

Für die Zwecke dieser Vorlesung ist Null eine natürliche Zahl:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\};$$

gelegentlich werden wir die Schreibweise

$$\mathbb{N}_+ = \{1, 2, 3, \ldots\}$$

für die Menge der positiven natürlichen (oder ganzen) Zahlen verwenden. Meistens werden wir zur Vermeidung von Unklarheiten aber $\mathbb{Z}_{\geq 0}$ und $\mathbb{Z}_{>0}$ für diese Mengen schreiben. Wie üblich steht $\mathbb{Z}$ für den Ring der ganzen Zahlen, $\mathbb{Q}$ für den Körper der rationalen Zahlen, $\mathbb{R}$ für den Körper der reellen Zahlen und $\mathbb{C}$ für den Körper der komplexen Zahlen. Außerdem steht $A \subset B$ für die nicht notwendig strikte Inklusion ($A = B$ ist also erlaubt); für die strikte Inklusion schreiben wir $A \subsetneq B$.

1. Permutationen

Um uns wieder mit Gruppen (den Objekten, die wir zunächst weiter studieren werden) vertraut zu machen, wollen wir uns als relativ konkretes (und auch wichtiges) Beispiel für endliche Gruppen in diesem Abschnitt die symmetrische Gruppe S_n und ihre Elemente etwas genauer anschauen.

DEF symmetrische Gruppe

Allgemein war für eine Menge X die *symmetrische Gruppe* $S(X)$ *von* X definiert als die Menge aller bijektiven Abbildungen („Permutationen“) von X nach X, mit der Hintereinanderausführung von Abbildungen als Verknüpfung. Im Fall $X = \{1, 2, \dots, n\}$ wird die Gruppe auch mit S_n bezeichnet.

Wir beginnen mit einer Definition für beliebige Mengen X.

DEF Zykel

Transposition

1.1. **Definition.** Seien X eine Menge und $T \subset X$ eine endliche Teilmenge mit $\#T = m > 0$. Eine Permutation $\sigma \in S(X)$ heißt ein *Zykel* auf T, wenn man die Elemente von T so als $t_1, t_2, \dots, t_m$ nummerieren kann, dass gilt

$$\forall j \in \{1, 2, \dots, m-1\}\colon \sigma(t_j) = t_{j+1}, \quad \sigma(t_m) = t_1, \quad \forall x \in X \setminus T\colon \sigma(x) = x\,.$$

Wir schreiben $\sigma = (t_1\, t_2\, \dots\, t_m)$. Dabei ist zu beachten, dass die Schreibweise nicht eindeutig ist, denn es gilt zum Beispiel auch $\sigma = (t_2\, t_3\, \dots\, t_m\, t_1)$. σ heißt dann auch ein *m-Zykel* und m heißt die *Länge* des Zykels σ. Ein 2-Zykel heißt auch eine *Transposition*. Zwei Zykel heißen *disjunkt*, wenn die zugehörigen Mengen T disjunkt sind. ♢

Es ist klar, dass die Ordnung eines m-Zykels σ genau m ist: $\sigma^m = \mathrm{id}$ und für $1 \le k < m$ ist $\sigma^k \neq \mathrm{id}$ (da zum Beispiel $\sigma^k(t_1) = t_{k+1} \neq t_1$ ist).

BSP Anzahl von Zykeln

1.2. **Beispiel.** Wie viele Zykel gibt es auf einer m-elementigen Menge?

Es gibt $m!$ Möglichkeiten, die Elemente als $(t_1\, t_2\, \dots\, t_m)$ hinzuschreiben. Davon ergeben aber jeweils m denselben Zykel (denn wir können einen Zykel beginnend mit einem beliebigen Element notieren). Es gibt also $m!/m = (m-1)!$ verschiedene Zykel auf einer m-elementigen Menge.

Wie viele m-Zykel gibt es in der S_n? (Für $m > 1$; jeder 1-Zykel ist die Identität.) Es gibt $\binom{n}{m}$ Möglichkeiten, eine m-elementige Teilmenge von $\{1, 2, \dots, n\}$ auszuwählen; auf jeder dieser Teilmengen gibt es $(m-1)!$ Zykel. Insgesamt gibt es also

$$\binom{n}{m}(m-1)! = \frac{n!}{(n-m)!m!}\,(m-1)! = \frac{n!}{(n-m)!\,m} = \frac{n(n-1)\cdots(n-m+1)}{m}$$

verschiedene m-Zykel in der S_n. ♣

Wir schreiben noch eine einfache Eigenschaft von Zykeln auf.

LEMMA disjunkte Zykel kommutieren

1.3. **Lemma.** *Sind $\sigma_1, \sigma_2 \in S(X)$ zwei disjunkte Zykel, dann gilt $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.*

Beweis. Seien T_1, T_2 die zugehörigen Mengen. Dann gilt:

$$\begin{aligned} x \in X \setminus (T_1 \cup T_2) &\implies (\sigma_1 \circ \sigma_2)(x) = x = (\sigma_2 \circ \sigma_1)(x)\,, \\ x \in T_1 &\implies (\sigma_1 \circ \sigma_2)(x) = \sigma_1(x) = (\sigma_2 \circ \sigma_1)(x)\,, \\ x \in T_2 &\implies (\sigma_1 \circ \sigma_2)(x) = \sigma_2(x) = (\sigma_2 \circ \sigma_1)(x)\,, \end{aligned}$$

woraus die Behauptung folgt. ❑

Zykel sind wichtig wegen der folgenden Beschreibung von Permutationen. Wir werden ab jetzt die Verknüpfung in der S_n einfach als Multiplikation schreiben statt mit dem Verknüpfungszeichen „$\circ$“.

* 1.4. **Satz.** *Jede Permutation $\sigma \in S_n$ kann eindeutig (bis auf Reihenfolge) als Produkt von paarweise disjunkten Zykeln geschrieben werden, in denen insgesamt alle Elemente von $\{1, 2, \ldots, n\}$ vorkommen.* **SATZ** Permutation als Produkt von Zykeln

Beweis. Für $x \in \{1, 2, \ldots, n\}$ sei $B(x) = \{x, \sigma(x), \sigma^2(x), \ldots\}$ die „Bahn von x unter σ“. Da σ endliche Ordnung hat, gilt $y \in B(x) \iff B(x) = B(y)$; wir erhalten also eine Partition von $\{1, 2, \ldots, n\}$ in die verschiedenen Mengen $B(x)$. Auf jeder dieser Mengen ist σ ein Zykel; insgesamt ist σ das Produkt dieser Zykel. Jede Zerlegung von σ als Produkt disjunkter Zykel muss die Mengen $B(x)$ als zugehörige Teilmengen haben; daraus folgt die Eindeutigkeit. ❑

Da 1-Zykel „nichts tun“ (sie sind die Identität), werden sie üblicherweise nicht mit aufgeschrieben. Der Satz lässt sich also auch alternativ so formulieren:

Jede Permutation $\sigma \in S_n$ kann eindeutig (bis auf Reihenfolge) als Produkt von paarweise disjunkten Zykeln der Länge ≥ 2 geschrieben werden.

Um eine eindeutige Notation zu haben, beginnt man einen Zykel meistens mit dem kleinsten Element, also $(1\,2\,3)$ und nicht $(2\,3\,1)$ oder $(3\,1\,2)$. Die verschiedenen Zykel im Produkt ordnet man meistens aufsteigend nach dem kleinsten Element.

1.5. **Beispiel.** Sei etwa $\sigma = [531674289] \in S_9$ (also $\sigma(1) = 5$, $\sigma(2) = 3$ usw.). Wir verfolgen die „Bahnen“ der Elemente unter σ: **BSP** Zykelzerlegung

$$1 \longmapsto 5 \longmapsto 7 \longmapsto 2 \longmapsto 3 \longmapsto 1, \quad 4 \longmapsto 6 \longmapsto 4, \quad 8 \longmapsto 8, \quad 9 \longmapsto 9\,.$$

Daraus ergibt sich die Zykelzerlegung

$$\sigma = (1\,5\,7\,2\,3)(4\,6)(8)(9) = (1\,5\,7\,2\,3)(4\,6)\,. \qquad \clubsuit$$

1.6. **Definition.** Sei $\sigma \in S_n$. Die in der Zerlegung von Satz 1.4 auftretenden Längen der Zykel ergeben den *Zykeltyp* von σ. Man schreibt ihn häufig in „Exponentialschreibweise“, also $1^{k_1} 2^{k_2} \cdots n^{k_n}$ für k_1 1-Zykel, k_2 2-Zykel usw. (wobei Terme mit Exponent null weggelassen werden). ♢ **DEF** Zykeltyp

1.7. **Beispiele.** **BSP** S_3, S_4

(1) Wir schreiben die Elemente der S_3 in dieser Zykelschreibweise auf:

$$S_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}\,.$$

Hier gibt es also die drei Zykeltypen 1^3, $1^1 2^1$ und 3^1.

(2) In der S_4 gibt es die folgenden Zykeltypen (in Klammern das Signum):

1^4 $(+1)$: id

$1^2 2^1$ (-1): $(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4)$

$1^1 3^1$ $(+1)$: $(1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3)$

2^2 $(+1)$: $(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)$

4^1 (-1): $(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)$

Insgesamt erhalten wir $1+6+8+3+6 = 24$ Elemente, wovon $1+8+3 = 12$ positives Signum haben, wie es sein muss. ♣

Zykel verhalten sich gut unter Konjugation.

LEMMA Zykel und Konjugation

1.8. **Lemma.** *Seien $\zeta = (t_1\, t_2\, \ldots\, t_m) \in S_n$ ein m-Zykel und $\sigma \in S_n$ beliebig. Dann gilt*

$$\sigma\,(t_1\, t_2\, \ldots\, t_m)\,\sigma^{-1} = (\sigma(t_1)\,\sigma(t_2)\, \ldots\, \sigma(t_m))\,.$$

Beweis. Sei $T = \{t_1, t_2, \ldots, t_m\}$. Für $x \in \{1, 2, \ldots, n\} \setminus \sigma(T)$ gilt $\sigma^{-1}(x) \notin T$, also $\zeta(\sigma^{-1}(x)) = \sigma^{-1}(x)$ und damit $(\sigma\zeta\sigma^{-1})(x) = x$. Für $x = \sigma(t_j)$ gilt

$$\big(\sigma\,(t_1\, t_2\, \ldots\, t_m)\,\sigma^{-1}\big)(x) = \big(\sigma\,(t_1\, t_2\, \ldots\, t_m)\big)(t_j) = \sigma(t_{j+1}) \quad \text{bzw. } \sigma(t_1) \text{ für } j = m\,.$$

Also ist $\sigma\zeta\sigma^{-1}$ der angegebene Zykel. ❑

FOLG Konjugationsklassen in S_n

1.9. **Folgerung.** *Zwei Permutationen $\tau_1, \tau_2 \in S_n$ sind genau dann zueinander konjugiert (d.h., es gibt $\sigma \in S_n$ mit $\tau_2 = \sigma\tau_1\sigma^{-1}$), wenn sie denselben Zykeltyp haben.*

Beweis. Sind τ_1 und $\tau_2 = \sigma\tau_1\sigma^{-1}$ konjugiert und ist $\tau_1 = \zeta_1\zeta_2\cdots\zeta_k$ ein Produkt von paarweise disjunkten Zykeln, dann ist nach Lemma 1.8

$$\tau_2 = \sigma\tau_1\sigma^{-1} = (\sigma\zeta_1\sigma^{-1})(\sigma\zeta_2\sigma^{-1})\cdots(\sigma\zeta_k\sigma^{-1})$$

ein Produkt von disjunkten Zykeln derselben Längen, hat also denselben Zykeltyp wie τ_1.

Haben τ_1 und τ_2 denselben Zykeltyp, dann können wir schreiben

$$\tau_1 = \zeta_1\zeta_2\cdots\zeta_k \quad \text{und} \quad \tau_2 = \zeta_1'\zeta_2'\cdots\zeta_k'$$

als Produkte paarweise disjunkter Zykel, in denen jeweils alle $i \in \{1, 2, \ldots, n\}$ auftreten, und sodass die Längen von ζ_j und ζ_j' übereinstimmen. Wir fixieren jeweils eine Schreibweise für jeden vorkommenden Zykel. Es gibt dann eine Permutation $\sigma \in S_n$, die die im Produkt für τ_1 von links nach rechts vorkommenden Elemente auf die entsprechenden Elemente im Produkt von τ_2 abbildet (denn es kommt jeweils jedes Element aus $\{1, 2, \ldots, n\}$ genau einmal vor). Nach Lemma 1.8 gilt dann $\sigma\zeta_j\sigma^{-1} = \zeta_j'$ für $1 \le j \le k$ und damit auch $\sigma\tau_1\sigma^{-1} = \tau_2$. ❑

Manchmal ist es hilfreich zu wissen, dass die Gruppe S_n von gewissen Elementen erzeugt wird. So kann man zum Beispiel zeigen, dass eine Untergruppe U der S_n schon die ganze S_n sein muss, indem man nachweist, dass U Erzeuger von S_n enthält. Es ist klar, dass (für $n \ge 3$) ein Erzeuger nicht ausreicht, da die S_n nicht abelsch und damit auch nicht zyklisch ist. Es zeigt sich allerdings, dass man mit zwei Erzeugern auskommt.

SATZ Erzeugung von S_n

1.10. **Satz.** *Sei $n \ge 2$.*

(1) *Es gilt $S_n = \big\langle (1\,2), (2\,3), (3\,4), \ldots, (n-1\,n) \big\rangle$ („bubble sort“).*

(2) *Es gilt $S_n = \big\langle (1\,2), (1\,2\,3\,\ldots\,n) \big\rangle$.*

(3) *Ist $n = p$ eine Primzahl, dann wird S_p von einer beliebigen Transposition zusammen mit einem beliebigen p-Zykel erzeugt.*

Beweis.

(1) Das ist das Prinzip hinter dem bekannten „bubble sort“-Sortieralgorithmus: Man kann eine Folge von Elementen durch sukzessives Vertauschen benachbarter Glieder in jede beliebige Reihenfolge bringen.

Etwas formaler: Für $\sigma \neq \mathrm{id}$ sei j die kleinste Zahl aus $\{1, 2, \dots, n\}$ mit $\sigma(j) \neq j$. Mit diesem j sei dann

$$\sigma' = (j\ j+1)(j+1\ j+2)\cdots(\sigma(j)-1\ \sigma(j))\sigma\,;$$

dann gilt $\sigma'(i) = i$ für alle $i \leq j$. Nach endlich vielen Wiederholungen dieser Prozedur erhalten wir

$$\mathrm{id} = P\sigma\,,$$

wobei P ein Produkt von Transpositionen benachbarter Elemente ist. Es folgt $\sigma = P^{-1}$, was ebenfalls ein Produkt solcher Transpositionen ist.

(2) Seien $\sigma = (1\,2\,\dots\,n)$ und $\tau = (1\,2)$. Dann ist nach Lemma 1.8

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

also sind $(1\,2), (2\,3), \dots, (n-1\,n) \in \langle\tau, \sigma\rangle$, und weil diese Transpositionen nach Teil (1) die S_n erzeugen, gilt das auch für τ und σ.

(3) Seien $\tau = (i\,j)$ die Transposition und σ der p-Zykel. Es gibt $k \geq 0$ mit $\sigma^k(i) = j$. Da $i \neq j$ ist, ist σ^k wieder ein p-Zykel (hier benutzen wir, dass p eine Primzahl ist: Die Ordnung jeder Potenz eines m-Zykels ist ein Teiler von m, in unserem Fall also 1 oder p) und es gilt $\langle\sigma^k\rangle = \langle\sigma\rangle$ und damit auch $\langle\tau, \sigma\rangle = \langle\tau, \sigma^k\rangle$. Es ist $\sigma^k = (i\,j\,\dots)$; es gibt dann $\rho \in S_p$ mit

$$\rho\sigma^k\rho^{-1} = (1\,2\,\dots\,p) \quad \text{und} \quad \rho\tau\rho^{-1} = (1\,2)\,.$$

Nach Teil (2) ist $\langle\rho\tau\rho^{-1}, \rho\sigma^k\rho^{-1}\rangle = S_p$, also auch

$$\langle\tau, \sigma\rangle = \langle\tau, \sigma^k\rangle = \rho^{-1}S_p\rho = S_p\,. \qquad \text{❑}$$

Aussage (3) ist für zusammengesetztes n im Allgemeinen falsch (Übung).

1.11. **Beispiel.** Nach Teil (1) von Satz 1.10 ist jede Permutation ein Produkt von Transpositionen. Zum Beispiel ist

BSP
Zykel als Produkt von Trans-positionen

$$\begin{aligned}(1\,2\,3) &= (1\,2)(2\,3)\\ (1\,2\,3\,4) &= (1\,2)(2\,3)(3\,4)\\ &\vdots \qquad\quad \vdots\\ (1\,2\,\dots\,n) &= (1\,2)(2\,3)\cdots(n-1\,n)\end{aligned}$$

Da Transpositionen τ ungerade Permutationen sind (also $\mathrm{sign}(\tau) = -1$) folgt (fieserweise), dass m-Zykel ζ für gerades m *ungerade* und für ungerades m *gerade* sind: $\mathrm{sign}(\zeta) = (-1)^{m-1}$. Zum Beispiel sind 3-Zykel gerade, also Elemente der A_n. Allgemeiner ist eine Permutation genau dann gerade, wenn in ihrer Zykelzerlegung eine gerade Anzahl von Zykeln gerader Länge vorkommt. ♣

2. Operationen von Gruppen auf Mengen

Gruppen sind nicht nur an sich wichtig, weil sie interessante algebraische Strukturen darstellen, sondern auch, weil sie häufig auch noch „etwas tun“. Die im letzten Semester als Beispiel erwähnten Automorphismen- und Symmetriegruppen eines Objekts X (eines Vektorraums, eines Rings, einer Gruppe, eines Graphen ...) zum Beispiel haben bereits definitionsgemäß die Eigenschaft, dass ihre Elemente Abbildungen $X \to X$ sind, also mit den Elementen von X „etwas tun“. Dies kann man etwas allgemeiner fassen und gelangt dann zum Konzept der Operation (auch als „Wirkung“ bezeichnet, engl. *action*) einer Gruppe auf einer Menge (oder einer Struktur).

∗ 2.1. **Definition.** Seien G eine Gruppe und X eine Menge. Eine *Operation* (von links) von G auf X ist eine Abbildung $m\colon G \times X \to X$, so dass für alle $x \in X$ und $g, g' \in G$ gilt

DEF Operation

$$m(1_G, x) = x \qquad \text{und} \qquad m(gg', x) = m(g, m(g', x))\,.$$

Meistens schreibt man $g \cdot x$ (oder auch nur gx) für $m(g, x)$; dann lauten die Bedingungen $1_G \cdot x = x$ und $gg' \cdot x = g \cdot (g' \cdot x)$.

Analog kann man Operationen *von rechts* als Abbildungen $X \times G \to X$ definieren (mit $(x \cdot g) \cdot g' = x \cdot (gg')$). ♢

Eine Operation m von G auf X ist dasselbe wie ein Gruppenhomomorphismus $\mu\colon G \to S(X)$ von G in die symmetrische Gruppe von X:

2.2. **Lemma.** *Seien G eine Gruppe und X eine Menge. Die Abbildungen*

LEMMA Operation ist Homom. nach $S(X)$

$$\{m\colon G \times X \to X \mid m \text{ ist Operation}\} \longleftrightarrow \{\mu\colon G \to S(X) \mid \mu \text{ Homomorphismus}\}$$
$$m \longmapsto \big(g \mapsto (x \mapsto m(g, x))\big)$$
$$\big((g, x) \mapsto (\mu(g))(x)\big) \longmapsfrom \mu$$

sind zueinander inverse Bijektionen.

Ist X eine Menge mit Struktur (zum Beispiel ein Vektorraum, ein Ring, eine Gruppe, ein metrischer Raum ...) und ist das Bild von μ enthalten in der entsprechenden Automorphismengruppe, dann sagt man, G operiere auf dem Vektorraum, Ring, der Gruppe, dem metrischen Raum X, oder G operiere auf X durch lineare Abbildungen, Ringautomorphismen, Gruppenautomorphismen, Isometrien.

Beweis. Wir zeigen zunächst, dass die beiden Abbildungen wohldefiniert sind (also das Bild von m ein Homomorphismus und das Bild von μ eine Operation ist).

Sei $m\colon G \times X \to X$ eine Operation von G auf X. Für $g \in G$ schreiben wir $\mu(g)$ für die Abbildung $X \to X$, $x \mapsto m(g, x)$. Dann gilt für $g, g' \in G$ und $x \in X$:

$$\mu(gg')(x) = m(gg', x) = m\big(g, m(g', x)\big) = \mu(g)\big(\mu(g')(x)\big) = \big(\mu(g) \circ \mu(g')\big)(x)\,,$$

also ist $\mu(gg') = \mu(g) \circ \mu(g')$. Da außerdem $\mu(1_G)(x) = m(1_G, x) = x$ ist, gilt $\mu(1_G) = \mathrm{id}_X$. Es folgt $\mu(g) \in S(X)$, denn $\mu(g^{-1}) \circ \mu(g) = \mathrm{id}_X = \mu(g) \circ \mu(g^{-1})$. Insgesamt sehen wir, dass das Bild von m, nämlich $\mu\colon g \mapsto \mu(g)$, tatsächlich ein Homomorphismus $G \to S(X)$ ist.

Sei jetzt $\mu\colon G \to S(X)$ ein Homomorphismus und $m\colon G \times X \to X$ definiert durch $m(g, x) = \mu(g)(x)$. Dann gilt $m(1_G, x) = \mu(1_G)(x) = \mathrm{id}_X(x) = x$ und

$$m\big(g, m(g', x)\big) = \mu(g)\big(\mu(g')(x)\big) = \big(\mu(g) \circ \mu(g')\big)(x) = \mu(gg')(x) = m(gg', x)\,,$$

also ist m eine Operation von G auf X.

Es bleibt zu zeigen, dass die Abbildungen invers zueinander sind. Wir haben

$$m \longmapsto \big(g \mapsto (x \mapsto m(g,x))\big) \longmapsto \big((g,x) \mapsto (x \mapsto m(g,x))(x) = m(g,x)\big) = m$$

und

$$\mu \longmapsto \big((g,x) \mapsto (\mu(g))(x)\big) \longmapsto \big(g \mapsto (x \mapsto \mu(g)(x)) = \mu(g)\big) = \mu$$

wie behauptet. ❑

BSP natürliche Operationen

2.3. **Beispiel.** Manche Gruppen operieren in natürlicher Weise auf gewissen Mengen. Zum Beispiel operiert eine Untergruppe G der S_n auf $X = \{1, 2, \ldots, n\}$ durch $g \cdot x = g(x)$ — die Elemente von G sind schon von Natur aus Abbildungen $X \to X$. In analoger Weise operiert eine Untergruppe G von $\mathrm{GL}(n, K)$ (für einen Körper K) in natürlicher Weise auf dem Vektorraum K^n (hier ist $g \cdot x$ die Multiplikation der Matrix g mit dem Spaltenvektor X). ♣

Wir führen einige grundlegende Begriffe im Zusammenhang mit Operationen ein.

DEF Bahn transitiv Fixpunkt Stabilisator

2.4. **Definition.** Eine Gruppe G operiere auf einer Menge X. Für $x \in X$ heißt

$$G \cdot x = \{g \cdot x \mid g \in G\} \subset X$$

die *Bahn* oder der *Orbit* von x (unter G). Die Kardinalität $\#(G \cdot x)$ heißt auch *Länge* der Bahn. Die Operation heißt *transitiv*, wenn $G \cdot x = X$ gilt (für alle $x \in X$). x heißt *Fixpunkt* von $g \in G$, wenn $g \cdot x = x$ ist; x heißt *Fixpunkt* der Operation, wenn $G \cdot x = \{x\}$ ist (wenn also x Fixpunkt von jedem $g \in G$ ist). Die Menge der Fixpunkte der Operation ist

$$X^G = \{x \in X \mid g \cdot x = x \text{ für alle } g \in G\}\,.$$

Die Untergruppe (!)

$$G_x = \{g \in G \mid g \cdot x = x\} \leq G$$

heißt der *Stabilisator* oder die *Standgruppe* von x.

Die Relation $x \sim_G y \iff x \in G \cdot y$ ist eine Äquivalenzrelation (!) auf X, deren Äquivalenzklassen gerade die Bahnen sind. Wir bezeichnen mit

$$G\backslash X = \{G \cdot x \mid x \in X\}$$

die Menge der Äquivalenzklassen (X/G im Falle einer Operation von rechts). ♢

Eine Gruppe G bietet selbst ein reichhaltiges Angebot von möglichen Operationen von (Untergruppen von) G auf diversen Mengen.

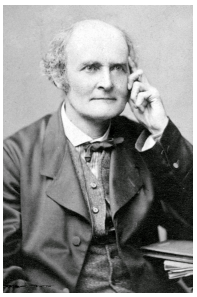
BSP Operation durch Translation

2.5. **Beispiel.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann operiert U auf G durch *Translation*: $u \cdot g = ug$ (bzw. $g \cdot u = gu$) für $u \in U$ und $g \in G$. Die Bahnen der Operation von links sind gerade die Rechtsnebenklassen, die Bahnen der Operation von rechts sind die Linksnebenklassen bezüglich U. Die Quotientenmenge $U\backslash G$ bzw. G/U entspricht unserer früheren Definition. ♣

Dass hier Links und Rechts nicht so recht zusammenpassen wollen, ist vielleicht etwas verwirrend, wird aber dadurch ausgeglichen, dass G in natürlicher Weise von links auf der Menge der Linksnebenklassen operiert:

BSP Operation auf G/U

2.6. **Beispiel.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann operiert G transitiv auf G/U via $g \cdot g'U = (gg')U$. Nach Lemma 2.2 erhalten wir also einen Gruppenhomomorphismus $G \to S(G/U)$. Ist U eine Untergruppe von endlichem Index n, dann kann man $S(G/U)$ mit der symmetrischen Gruppe S_n identifizieren, indem man die Nebenklassen durchnummeriert.



A. Cayley
1821–1895

Der Kern des Homomorphismus $G \to S(G/U)$ besteht aus allen $g \in G$ mit der Eigenschaft, dass für alle $h \in G$ gilt $ghU = hU$, oder äquivalent $g \in hUh^{-1}$. Der Kern ist also $\bigcap_{h \in G} hUh^{-1}$, der größte in U enthaltene Normalteiler von G. Ist dieser trivial (z.B. wenn $U = \{1_G\}$ ist oder wenn $U \neq G$ und G einfach ist), dann hat man G als eine Untergruppe in die symmetrische Gruppe $S(G/U)$ eingebettet. Insbesondere sieht man mit $U = \{1_G\}$ (Satz von Cayley):

Jede endliche Gruppe der Ordnung n ist isomorph zu einer (transitiven) Untergruppe von S_n. ♣

Man kann diese Art der Operation auch dazu verwenden, die Aussage, dass eine Untergruppe vom Index 2 immer ein Normalteiler ist, zu verallgemeinern.

SATZ Normalteiler von kleinem Index

2.7. **Satz.** *Seien G eine endliche Gruppe und p der kleinste Primteiler von $\#G$. Ist $U \leq G$ eine Untergruppe vom Index p, dann ist U ein Normalteiler von G.*

Beweis. Die Operation von G auf G/U liefert einen Homomorphismus $\phi\colon G \to S_p$. Sein Kern K ist ein echter Normalteiler von G (denn die Operation ist transitiv und $U \neq G$; der Homomorphismus hat also nichttriviales Bild), dessen Index also > 1 und außerdem ein Teiler von $\#G$ und auch von $\#S_p = p!$ sein muss (nach dem Homomorphiesatz für Gruppen ist $(G : K) = \#\operatorname{im}(\phi)$). Da p der *kleinste* Primteiler von $\#G$ ist, gilt $\operatorname{ggT}(\#G, p!) = p$, also ist der Index genau p. K ist außerdem in U enthalten, da U der Stabilisator der trivialen Nebenklasse $U \in G/U$ ist (K ist der Durchschnitt aller Stabilisatoren). Es bleibt wegen $(G : U) = p$ nur die Möglichkeit, dass $K = U$ ist (denn $K \subset U$ und $\#K = \#G/p = \#U$), also ist U als Kern eines Homomorphismus ein Normalteiler. ❑

BSP Operation durch Konjugation

DEF Konjugationsklasse

Zentralisator

2.8. **Beispiel.** Jede Gruppe G operiert auf sich selbst durch Gruppenautomorphismen via $g \mapsto c_g$, also $g \cdot x = c_g(x) = gxg^{-1}$ (Operation „durch Konjugation“). Die Bahnen dieser Operation heißen die *Konjugationsklassen* von G. Der Kern des Homomorphismus $G \to \operatorname{Aut}(G)$, $g \mapsto c_g$, ist gerade das Zentrum $Z(G)$ von G, wie wir in der „Einführung in die Zahlentheorie und algebraische Strukturen“ gesehen haben. Der Stabilisator von $x \in G$ unter dieser Operation heißt der *Zentralisator* $C_G(x) = \{g \in G \mid gx = xg\}$ von x in G.

Auf analoge Weise operiert G auf der Menge aller Untergruppen von G (auch auf der Menge aller Untergruppen von fester Ordnung oder festem Index) via $g \cdot U = gUg^{-1}$. Die Bahnen heißen wieder *Konjugationsklassen* (von Untergruppen). Eine Untergruppe U ist genau dann ein Fixpunkt dieser Operation, wenn U ein Normalteiler von G ist. Der Stabilisator von U unter dieser Operation heißt der *Normalisator* $N_G(U) = \{g \in G \mid gU = Ug\}$ von U in G. U ist ein Normalteiler in $N_G(U)$, und $N_G(U)$ ist die größte Untergruppe von G mit dieser Eigenschaft (Übung). ♣

DEF Normalisator

Wir beweisen jetzt eine einfache, aber grundlegende Tatsache.

2.9. **Lemma.** *Die Gruppe G operiere auf der Menge X; $x \in X$ sei ein Element. Dann ist die Abbildung*

$$G/G_x \longrightarrow G \cdot x\,, \qquad gG_x \longmapsto g \cdot x$$

(wohldefiniert und) eine Bijektion. Insbesondere gelten die Relationen

$$\#(G \cdot x) = (G : G_x) \qquad \textit{und} \qquad \#G_x\,\#(G \cdot x) = \#G\,.$$

LEMMA Bahn und Stabilisator

Beweis. Wir zeigen, dass die Abbildung wohldefiniert ist: Es gelte $gG_x = g'G_x$, also $g = g'h$ mit $h \in G_x$. Dann ist $g \cdot x = g'h \cdot x = g' \cdot (h \cdot x) = g' \cdot x$, weil $h \cdot x = x$ ist.

Die Abbildung ist offensichtlich surjektiv (jedes Element von $G \cdot x$ hat die Form $g \cdot x$). Wir zeigen, dass sie auch injektiv ist: Seien $gG_x, g'G_x \in G/G_x$ mit $g \cdot x = g' \cdot x$. Dann folgt

$$x = 1_G \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x\,,$$

also ist $g^{-1}g' \in G_x$ und damit $gG_x = g'G_x$.

Die angegebenen Gleichheiten erhält man durch Vergleich der Kardinalitäten und mit dem Satz von Lagrange (aus seinem Beweis ergibt sich, dass die Gleichung auch im Fall $\#G = \infty$ richtig ist; dann bedeutet sie einfach, dass G_x oder der Index $(G : G_x)$ unendlich ist). ❑

Der Zusammenhang zwischen den Stabilisatoren verschiedener Elemente von X in derselben Bahn wird durch folgendes Lemma hergestellt.

2.10. **Lemma.** *Die Gruppe G operiere auf der Menge X; es seien $x \in X$ und $g \in G$. Dann gilt $G_{g \cdot x} = gG_xg^{-1}$.*

LEMMA Stabilisator von $g \cdot x$

Beweis. Für $h \in G$ gilt

$$h \cdot (g \cdot x) = g \cdot x \iff g^{-1}hg \cdot x = x \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1}\,. \quad ❑$$

∗ 2.11. **Folgerung.** *Die endliche Gruppe G operiere auf der endlichen Menge X. Dann gilt*

$$\#X = \#X^G + \sum_{G \cdot x \in G\backslash X, \#(G \cdot x) \geq 2} (G : G_x)\,.$$

FOLG Bahnengleichung

Dabei sind alle Terme $(G : G_x)$ in der Summe Teiler der Ordnung von G.

Man kann das so interpretieren, dass in der Summe x über ein *Repräsentantensystem* der Bahnen in $X \setminus X^G$ läuft. Nach Lemma 2.10 hängt der Index $(G : G_x)$ nicht vom gewählten Repräsentanten der Bahn $G \cdot x$ ab.

Beweis. Wir schreiben $\#X$ als Summe aller Kardinalitäten $\#(G \cdot x)$ der Bahnen. Die Bahnen der Länge 1 ergeben gerade die Fixpunkte X^G; für die übrigen verwenden wir die Relation $\#(G \cdot x) = (G : G_x)$ aus Lemma 2.9. Dass $(G : G_x)$ ein Teiler von $\#G$ ist, folgt aus dem Satz von Lagrange. ❑

Diese harmlos erscheinende Relation hat interessante Anwendungen.

2.12. **Definition.** Sei p eine Primzahl. Eine endliche Gruppe G heißt eine *p-Gruppe*, wenn G nicht trivial ist und die Ordnung $\#G$ eine Potenz von p ist. ♢

DEF p-Gruppe

2.13. **Folgerung.** *Sei G eine p-Gruppe, die auf der endlichen Menge X operiert.* **FOLG** Operation einer p-Gruppe

(1) *Ist p kein Teiler von $\#X$, dann hat G Fixpunkte in X.*

(2) *Ist p ein Teiler von $\#X$ und ist $X^G \neq \emptyset$, dann ist $\#X^G \geq p$.*

Beweis. Ist $U \leq G$ eine Untergruppe mit $U \neq G$, dann muss der Index $(G : U)$ ein Vielfaches (sogar eine Potenz) von p sein. Aus der Relation in Folgerung 2.11 ergibt sich also die Kongruenz $\#X \equiv \#X^G \bmod p$. Daraus folgen sofort die beiden Behauptungen. ❑

2.14. **Beispiel.** Seien G eine endliche Gruppe und p eine Primzahl mit $p \mid \#G$. Der *Satz von Cauchy* besagt dann, dass es in G (mindestens) ein Element der Ordnung p gibt. Der Beweis kann durch Betrachtung der Operation der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ auf G^p durch „Rotation“ geführt werden: Der Erzeuger von $\mathbb{Z}/p\mathbb{Z}$ bewirkt die Permutation **BSP** Satz von Cauchy

$$(g_1, g_2, \ldots, g_p) \longmapsto (g_2, g_3, \ldots, g_p, g_1)\,.$$

Diese Operation kann auf die Teilmenge M der p-Tupel mit $g_1 g_2 \cdots g_p = 1_G$ eingeschränkt werden (denn aus $g_1 g_2 \cdots g_p = 1_G$ folgt $g_2 \cdots g_n g_1 = g_1^{-1}(g_1 \cdots g_n) g_1 = g_1^{-1} g_1 = 1_G$). Diese Menge M hat durch p teilbare Kardinalität $\#M = (\#G)^{p-1}$, und es gibt jedenfalls den Fixpunkt $(1_G, 1_G, \ldots, 1_G) \in M$. Nach Folgerung 2.13 gibt es also noch (mindestens $p-1$) weitere Fixpunkte. Diese sind von der Form $(g, g, \ldots, g)$ mit $g^p = 1_G$ und $g \neq 1_G$, liefern also Elemente der Ordnung p in G. ♣

2.15. **Beispiel.** Als weiteres Beispiel hier ein Beweis des *kleinen Satzes von Fermat*: $a^p \equiv a \bmod p$ für Primzahlen p und ganze Zahlen a. Wir beweisen das hier für $a > 0$ (was natürlich reicht, da es nur auf die Restklasse von a modulo p ankommt). Dazu lassen wir die zyklische Gruppe $\mathbb{Z}/p\mathbb{Z}$ wie in Beispiel 2.14 durch „Rotation“ auf der Menge $X = \{1, 2, \ldots, a\}^p$ operieren. Fixpunkte sind wie eben die Tupel, die p-mal dasselbe Element enthalten, also gilt $a^p = \#X \equiv \#X^{\mathbb{Z}/p\mathbb{Z}} = a \bmod p$. ♣ **BSP** kleiner Satz von Fermat

2.16. **Beispiel.** Im Fall der Operation einer endlichen Gruppe G auf sich durch Konjugation heißt die Bahnengleichung auch *Klassengleichung*. Wenn wir $\mathcal{C}(G)$ für ein Repräsentantensystem der Konjugationsklassen außerhalb des Zentrums von G schreiben, dann lautet sie **BSP** Klassengleichung

$$\#Z(G) + \sum_{g \in \mathcal{C}(G)} (G : C_G(g)) = \#G\,.$$

Man beachte, dass die Elemente des Zentrums hier gerade die Fixpunkte der Operation sind. ♣

Es ergibt sich daraus eine interessante Strukturaussage über p-Gruppen.

FOLG Zentrum einer p-Gruppe

2.17. **Folgerung.** *Sei G eine p-Gruppe. Dann ist das Zentrum $Z(G)$ nicht trivial. Insbesondere ist eine p-Gruppe genau dann einfach, wenn sie Ordnung p hat.*

Beweis. Wir betrachten die Operation von G durch Konjugation auf sich selbst. Dann ist $\#X = \#G$ durch p teilbar, und 1_G ist ein Fixpunkt, also hat die Menge der Fixpunkte mindestens p Elemente. Die Fixpunktmenge ist aber gerade das Zentrum $Z(G)$. Da $Z(G) \triangleleft G$, gilt $Z(G) = G$, wenn G einfach ist. Dann ist G aber abelsch, muss also Ordnung p haben (die abelschen einfachen Gruppen sind gerade die zyklischen Gruppen von Primzahlordnung). ❑

LEMMA $G/Z(G)$ nicht zyklisch

2.18. **Lemma.** *Sei G eine Gruppe mit Zentrum $Z(G)$. Ist $G/Z(G)$ zyklisch, dann ist G abelsch (also ist $G/Z(G)$ dann sogar trivial).*

Beweis. Sei $a \in G$ ein Element, dessen Bild $aZ(G)$ in $G/Z(G)$ die Faktorgruppe erzeugt. Ist $g \in G$ beliebig, dann gibt es $n \in \mathbb{Z}$, sodass $gZ(G) = a^n Z(G)$ ist, also können wir schreiben $g = a^n z$ mit $n \in \mathbb{Z}$ und $z \in Z(G)$. Ist $h = a^m z'$ ein weiteres Element von G (mit $m \in \mathbb{Z}$ und $z' \in Z(G)$), dann ist

$$gh = a^n z a^m z' = a^n a^m z z' = a^m a^n z' z = a^m z' a^n z = hg\,,$$

also ist G abelsch. ❑

FOLG Gruppen der Ordnung p^2

2.19. **Folgerung.** *Sei p eine Primzahl. Jede Gruppe der Ordnung p^2 ist abelsch. Damit gilt $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Sei G eine Gruppe mit $\#G = p^2$. Nach Folgerung 2.17 ist $Z(G)$ nicht trivial, also gilt entweder $\#Z(G) = p$ oder $\#Z(G) = p^2$. Im zweiten Fall ist $Z(G) = G$, also G abelsch. Im ersten Fall ist $G/Z(G)$ eine Gruppe der Ordnung p, also zyklisch. Nach Lemma 2.18 ist G dann ebenfalls abelsch (bzw. dieser Fall tritt nicht auf). Die letzte Aussage folgt dann aus dem Klassifikationssatz für endliche abelsche Gruppen. ❑

3. Die Sätze von Sylow

Wir werden jetzt Operationen einer endlichen Gruppe auf verschiedenen aus dieser Gruppe konstruierten Mengen benutzen, um einige wichtige Aussagen über ihre Struktur zu beweisen. Und zwar geht es um die Existenz und Eigenschaften von Untergruppen von Primzahlpotenzordnung. Ist d ein beliebiger Teiler der Gruppenordnung, dann muss es nicht unbedingt eine Untergruppe der Ordnung d geben (z.B. hat die alternierende Gruppe A_4 der Ordnung 12 keine Untergruppe der Ordnung 6). Ist d aber eine Primzahlpotenz, dann kann man die Existenz (und mehr) beweisen. Diese Resultate gehen auf den norwegischen Mathematiker Peter Ludwig Mejdell Sylow zurück.

P.L.M. Sylow
1832–1918

Wir beginnen mit einem einfachen Spezialfall.

LEMMA
Erzeuger einer zyklischen Gruppe

3.1. **Lemma.** *Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe der Ordnung n. Dann hat G genau $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ Erzeuger, nämlich alle g^a mit $0 \le a < n$ und $a \perp n$.*

Beweis. Ist $d = \mathrm{ggT}(a,n) > 1$, dann gilt $g^{a\cdot n/d} = g^{\mathrm{kgV}(a,n)} = 1_G$, also ist $\mathrm{ord}(g^a) \le n/d < n$ und g^a kann kein Erzeuger sein. Die Bedingung $a \perp n$ ist also notwendig. Gilt $a \perp n$, dann gibt es $b \in \mathbb{Z}$ mit $ab \equiv 1 \bmod n$; es folgt $(g^a)^b = g$ und damit auch $\langle g^a \rangle \supset \langle g \rangle = G$. ❑

Wir erinnern uns an die Relation

$$\sum_{d|n} \varphi(d) = n$$

(die Summe läuft über die positiven Teiler von $n \in \mathbb{Z}_{>0}$).

LEMMA
Untergruppen einer zyklischen Gruppe

3.2. **Lemma.** *Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe der Ordnung n. Dann gibt es zu jedem Teiler d von n genau eine Untergruppe der Ordnung d in G, nämlich $\langle g^{n/d} \rangle$.*

Beweis. Das war eine Übungsaufgabe im letzten Semester.

Sei $h = g^{n/d}$ und $H = \langle h \rangle$. Dann gilt $h^d = g^n = 1_G$, und d ist die kleinste positive ganze Zahl mit dieser Eigenschaft (denn n ist der kleinste Exponent mit $g^n = 1_G$). Es folgt $\#H = \mathrm{ord}(h) = d$. Nach Lemma 3.1 hat H genau $\varphi(d)$ Erzeuger, damit hat G mindestens $\varphi(d)$ Elemente der Ordnung d. Da die Ordnung jedes Elements von G ein Teiler von n ist, folgt aus der Relation für die φ-Funktion, dass es für jeden Teiler d von n *genau* $\varphi(d)$ Elemente der Ordnung d gibt. Wir hatten im Zusammenhang mit dem Klassifikationssatz für endlich erzeugte abelsche Gruppen gesehen, dass jede Untergruppe einer zyklischen Gruppe zyklisch ist. Gäbe es nun zwei verschiedene Untergruppen der Ordnung d, dann müssten die Mengen ihrer Erzeuger disjunkt sein und es gäbe mindestens $2\varphi(d)$ Elemente der Ordnung d; das ist ein Widerspruch. ❑

Für endliche abelsche Gruppen folgt die Umkehrung dieser Aussage leicht aus dem Klassifikationssatz für endliche abelsche Gruppen: Ist G eine endliche abelsche Gruppe, die nicht zyklisch ist, dann ist $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$ mit $m \ge 2$ und $2 \le d_1 \mid d_2$. Die ersten beiden Faktoren enthalten jeweils eine Untergruppe der Ordnung d_1 und die Bilder in G dieser beiden Untergruppen sind verschieden.

Diese Umkehrung gilt leicht verschärft sogar für beliebige endliche Gruppen:

3.3. **Lemma.** *Sei G eine endliche Gruppe der Ordnung n mit der Eigenschaft, dass es für jeden Teiler d von n höchstens eine Untergruppe von G der Ordnung d gibt. Dann ist G zyklisch.* **LEMMA** Umkehrung

Beweis. Hat $g \in G$ die Ordnung d, dann erzeugt g eine (und damit die einzige) Untergruppe U_d der Ordnung d, die also zyklisch ist und genau $\varphi(d)$ Erzeuger hat; dies sind dann genau die Elemente der Ordnung d in G. Es folgt

$$a_d := \#\{g \in G \mid \operatorname{ord}(g) = d\} = \big(\varphi(d) \text{ oder } 0\big) \leq \varphi(d)$$

für alle Teiler d von n. Aus

$$\sum_{d|n} a_d = \#G = n = \sum_{d|n} \varphi(d)$$

folgt dann $a_d = \varphi(d)$ für alle $d \mid n$. Insbesondere ist $a_n = \varphi(n) \geq 1$, also gibt es Elemente der Ordnung n in G. So ein Element erzeugt G, demnach ist G zyklisch. ❑

Seien jetzt G eine endliche Gruppe, p eine Primzahl und $e \geq 1$ mit $p^e \mid \#G$. Sei weiter $\mathcal{T}$ die Menge, deren Elemente alle Teilmengen $M \subset G$ mit $\#M = p^e$ sind. Auf $\mathcal{T}$ operiert G durch Translation von links: $g \cdot M = gM = \{gm \mid m \in M\}$.

Die interessierenden Bahnen sind jetzt nicht die Fixpunkte, aber insoweit damit verwandt, als es die Bahnen sind, deren Elemente die größten Stabilisatoren haben:

3.4. **Lemma.** *Sei $M \in \mathcal{T}$ und sei $G_M = \{g \in G \mid gM = M\}$ der Stabilisator von M. Dann gilt:* **LEMMA**

(1) *M ist disjunkte Vereinigung von Rechtsnebenklassen bezüglich G_M.*

(2) *$\#G_M \mid p^e$.*

(3) *M ist genau dann eine Rechtsnebenklasse bezüglich einer Untergruppe U von G, wenn G_M Ordnung p^e hat. In diesem Fall ist $U = G_M$, und alle Mengen gM in der Bahn von M sind Rechtsnebenklassen bezüglich einer Untergruppe.*

(4) *Jede Bahn, deren Elemente Rechtsnebenklassen sind, enthält genau eine Untergruppe von G.*

Beweis.

(1) Der Stabilisator G_M operiert auf M durch Translation von links. M zerfällt also in Bahnen bezüglich dieser Operation; diese Bahnen (auf ganz G) sind gerade die Rechtsnebenklassen bezüglich G_M.

(2) Da die Rechtsnebenklassen von G_M alle dieselbe Mächtigkeit $\#G_M$ haben, folgt aus Teil (1), dass $\#G_M$ ein Teiler von $\#M = p^e$ sein muss.

(3) Gilt $\#G_M = p^e$, dann ist M eine Rechtsnebenklasse bezüglich G_M nach Teil (1), denn die Anzahl der Rechtsnebenklassen bezüglich G_M in M ist gegeben durch $p^e/\#G_M$.
Gilt umgekehrt $M = Ug$ mit einer Untergruppe $U \leq G$, dann ist $U \subset G_M$, und es folgt mit Teil (2) $p^e = \#M = \#U \mid \#G_M \mid p^e$, also $\#G_M = p^e$ und damit $U = G_M$.
Hat der Stabilisator G_M von M Ordnung p^e, dann gilt das auch für den Stabilisator $G_{gM} = gG_Mg^{-1}$ (siehe Lemma 2.10) jeder anderen Menge gM

in der Bahn von M. Damit ist auch gM eine Rechtsnebenklasse (bezüglich gG_Mg^{-1}).

(4) Die Bahn enthalte die Rechtsnebenklasse Ug bezüglich der Untergruppe U; dann enthält die Bahn die Untergruppe $U' = g^{-1}Ug \leq G$. Die Bahn besteht dann genau aus den Linksnebenklassen bezüglich U'; U' selbst ist die einzige Linksnebenklasse, die eine Untergruppe ist. ❑

Wir schreiben $\#G = kp^e$ mit $k \in \mathbb{Z}_{\geq 1}$. Wir wenden die Bahnengleichung 2.11 auf die Operation von G auf $\mathcal{T}$ an:

$$\binom{kp^e}{p^e} = \#\mathcal{T} = \sum_{j\in J} (G : G_{M_j}) \,,$$

wobei $(M_j)_{j\in J}$ ein Repräsentantensystem der Bahnen ist. Nach Teil (2) von Lemma 3.4 ist $\#G_{M_j}$ ein Teiler von p^e; es folgt $(G : G_{M_j}) = \#G/\#G_{Mj} = kp^f$ mit $f \geq 0$ und damit (unter Verwendung von Teil (3) und (4) des Lemmas)

$$\binom{kp^e}{p^e} = k\big(\#\{j \in J \mid \#G_{M_j} = p^e\} + p\ell(G)\big) = k\big(\#\{U \leq G \mid \#U = p^e\} + p\ell(G)\big)$$

mit einer ganzen Zahl $\ell(G)$. Ist G die zyklische Gruppe der Ordnung kp^e, dann gibt es nach Lemma 3.2 genau eine Untergruppe der Ordnung p^e, also gilt

$$\binom{kp^e}{p^e} = k\big(1 + p\ell(\mathbb{Z}/kp^e\mathbb{Z})\big) \,.$$

Wir setzen das oben ein und teilen durch k; das liefert

$$\#\{U \leq G \mid \#U = p^e\} \equiv 1 \bmod p \,.$$

Wir haben also folgenden Satz bewiesen, der den Satz von Cauchy (Beispiel 2.14) verallgemeinert. (Dieser Beweis stammt von Frobenius.)

F.G. Frobenius
1849–1917

* 3.5. **Satz.** *Seien G eine endliche Gruppe, p eine Primzahl und p^e ein Teiler von $\#G$. Dann ist die Anzahl der Untergruppen von G der Ordnung p^e von der Form $1 + \ell p$ mit $\ell \in \mathbb{Z}_{\geq 0}$. Insbesondere gibt es stets solche Untergruppen.*

SATZ
1. Satz
von Sylow

* 3.6. **Definition.** Seien G eine endliche Gruppe und p ein Primteiler von $\#G$. Eine Untergruppe $U \leq G$ heißt *p-Untergruppe* von G, wenn $\#U = p^e$ ist mit $e \geq 1$. U heißt *p-Sylowgruppe* von G, wenn e maximal ist, also wenn $\#G = kp^e$ ist mit $p \nmid k$. ♢

DEF
p-Sylow-
gruppe

Der 1. Satz von Sylow sagt also, dass es zu jeder möglichen Ordnung auch (mindestens) eine p-Untergruppe gibt; insbesondere gibt es stets wenigstens eine p-Sylowgruppe. Wir zeigen jetzt eine schärfere Aussage.

* 3.7. **Satz.** *Seien G eine endliche Gruppe, p ein Primteiler von $\#G$, S eine p-Sylowgruppe von G und $U \leq G$ eine p-Untergruppe. Dann gibt es $g \in G$, sodass $U \subset gSg^{-1}$ ist. Insbesondere sind je zwei p-Sylowgruppen von G zueinander konjugiert, und S ist genau dann ein Normalteiler von G, wenn S die einzige p-Sylowgruppe von G ist.*

SATZ
2. Satz
von Sylow

Beweis. Diesmal lassen wir G (und damit U) auf der Menge $G/S = \{gS \mid g \in G\}$ der Linksnebenklassen von S durch Linkstranslation operieren: $h \cdot gS = (hg)S$. Weil S eine p-Sylowgruppe von G ist, ist $\#(G/S) = \#G/\#S$ nicht durch p teilbar. Auf der anderen Seite ist U eine p-Gruppe. Nach Folgerung 2.13 hat die Operation von U auf G/S einen Fixpunkt gS. Das bedeutet $ugS = gS$ und damit $u \in gSg^{-1}$ für alle $u \in U$, also $U \subset gSg^{-1}$.

Wenden wir das Ergebnis auf eine weitere p-Sylowgruppe S' von G an, dann folgt $S' \subset gSg^{-1}$ für ein geeignetes $g \in G$. Da beide Seiten dieselbe Ordnung haben, muss Gleichheit gelten, also sind S und S' zueinander konjugiert. Die Konjugationsklasse von S besteht also genau aus den p-Sylowgruppen von G. Eine Untergruppe ist genau dann ein Normalteiler, wenn sie das einzige Element in ihrer Konjugationsklasse ist; das zeigt die letzte Aussage im Satz. ❑

Als letzte Aussage der „Sätze von Sylow“ haben wir noch Einschränkungen für die mögliche Anzahl der p-Sylowgruppen.

* 3.8. **Satz.** *Seien G eine endliche Gruppe und p ein Primteiler von $\#G$. Wir schreiben $\#G = kp^e$ mit $p \nmid k$. Dann gilt für die Anzahl s_p der p-Sylowgruppen von G:*

SATZ
3. Satz von Sylow

$$s_p \equiv 1 \bmod p \qquad \textit{und} \qquad s_p \mid k\,.$$

Beweis. Die erste Aussage $s_p \equiv 1 \bmod p$ ist ein Spezialfall des 1. Satzes von Sylow 3.5. Für die zweite Aussage betrachten wir die Operation von G durch Konjugation auf der Menge der p-Sylowgruppen von G: $g \cdot S = gSg^{-1}$. Nach Satz 3.7 ist die Operation transitiv. Die Anzahl s_p ist also gleich der Länge der (einzigen) Bahn und muss demnach ein Teiler von $\#G$ sein. Da nach der ersten Aussage p kein Teiler von s_p ist, folgt $s_p \mid k$. ❑

Man kann die zweite Aussage auch direkt ohne Rückgriff auf die erste beweisen, indem man bemerkt, dass der Stabilisator $N_G(S)$ von S unter der Operation durch Konjugation S enthält. Es folgt $s_p = (G : N_G(S)) \mid (G : S) = k$.

Man kann die Sätze von Sylow dazu benutzen, Strukturaussagen über endliche Gruppen zu gewinnen und zum Beispiel die Gruppen vorgegebener Ordnung bis auf Isomorphie zu klassifizieren. Wir werden dazu gleich ein Beispiel betrachten. Vorher brauchen wir noch eine Hilfsaussage.

3.9. **Lemma.** *Sei G eine Gruppe und seien N und N' zwei Normalteiler von G mit $N \cap N' = \{1_G\}$. Dann gilt für alle $n \in N$ und $n' \in N'$, dass $nn' = n'n$ ist.*

LEMMA
Produkt von Normalteilern

Beweis. Wir betrachten den *Kommutator* $[n, n'] = nn'n^{-1}n'^{-1}$. Es gilt

DEF
Kommutator

$$[n, n'] = (nn'n^{-1})n'^{-1} \in (nN'n^{-1})N' = N'N' = N' \qquad \text{und}$$
$$[n, n'] = n(n'n^{-1}n'^{-1}) \in N(n'Nn'^{-1}) = NN = N\,,$$

also $[n, n'] \in N \cap N' = \{1_G\}$ und damit $nn'n^{-1}n'^{-1} = 1$. Multiplikation mit $n'n$ von rechts liefert $nn' = n'n$. ❑

Wir erinnern uns an die Definition des direkten Produkts von Gruppen:

3.10. **Definition.** Sei $(G_i)_{i\in I}$ eine Familie von Gruppen. Das kartesische Produkt $G = \prod_{i\in I} G_i$ wird zu einer Gruppe, wenn wir die Verknüpfung komponentenweise definieren:

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} = (g_i \cdot h_i)_{i\in I}$$

Die Gruppe G mit dieser Verknüpfung heißt das *direkte Produkt* der Gruppen G_i.

Ist $I = \{1, 2, \ldots, n\}$ endlich, dann schreiben wir auch $G_1 \times G_2 \times \cdots \times G_n$ für das direkte Produkt. ♢

DEF direktes Produkt von Gruppen

3.11. **Lemma.** *Sei G eine endliche Gruppe der Ordnung $\#G = p^e q^f$ mit Primzahlen $p \neq q$ und $e, f \geq 1$. G besitze genau eine p-Sylowgruppe S_p und genau eine q-Sylowgruppe S_q. Dann ist $\phi\colon S_p \times S_q \to G$, $(s, s') \mapsto ss'$ ein Isomorphismus.*

LEMMA Produkt von Sylowgruppen

Beweis. Nach Satz 3.7 sind S_p und S_q Normalteiler von G. Da die Ordnungen von S_p und S_q teilerfremd sind, muss $S_p \cap S_q = \{1_G\}$ gelten. Nach Lemma 3.9 gilt also $ss' = s's$ für alle $s \in S_p$ und $s' \in S_q$. Daraus folgt, dass ϕ ein Gruppenhomomorphismus ist, denn für $s_1, s_2 \in S_p$, $s_1', s_2' \in S_q$ gilt

$$\phi\big((s_1, s_1')(s_2, s_2')\big) = \phi(s_1 s_2, s_1' s_2') = (s_1 s_2)(s_1' s_2') = (s_1 s_1')(s_2 s_2') = \phi(s_1, s_1')\phi(s_2, s_2').$$

Der Kern von ϕ ist trivial, denn aus $ss' = 1_G$ folgt $s = s'^{-1} \in S_p \cap S_q = \{1_G\}$, also $(s, s') = (1, 1)$. Es folgt, dass ϕ injektiv ist. Da Quelle und Ziel von ϕ dieselbe Mächtigkeit haben, muss ϕ auch surjektiv sein. ❑

Man kann das verallgemeinern:
Sei G eine endliche Gruppe. Gibt es zu jedem Primteiler p von $\#G$ genau eine p-Sylowgruppe S_p von G, dann ist G isomorph zum direkten Produkt der Gruppen S_p.
(Beweis als Übung.)

Es folgt das versprochene Anwendungsbeispiel für die Sätze von Sylow.

3.12. **Satz.** *Seien $p < q$ Primzahlen mit $p \nmid q - 1$. Dann ist jede Gruppe G mit $\#G = pq$ zyklisch.*

SATZ Gruppen der Ordnung pq

Beweis. Seien s_p und s_q die Anzahlen der p- und q-Sylowgruppen von G. Nach Satz 3.8 gilt dann $s_p \mid q$ und $s_p \equiv 1 \bmod p$. Da $q \not\equiv 1 \bmod p$, ist $s_p = 1$ die einzige Möglichkeit. Ebenso gilt $s_q \mid p$ und $s_q \equiv 1 \bmod q$; wegen $q > p$ muss $s_q = 1$ sein. Nach Lemma 3.11 ist G isomorph zum Produkt seiner p- und seiner q-Sylowgruppe. Diese Gruppen sind zyklisch (da von Primzahlordnung); nach dem Chinesischen Restsatz ist die direkte Summe isomorph zur zyklischen Gruppe $\mathbb{Z}/pq\mathbb{Z}$. ❑

Im nächsten Abschnitt werden wir die Gruppen der Ordnung pq vollständig klassifizieren.

4. Semidirekte Produkte

Man kann die Gruppen der Ordnung pq ganz allgemein klassifizieren. Dazu braucht man die Konstruktion des *semidirekten Produkts*.

Aus Ergebnissen des letzten Abschnitts kann man Folgendes schließen:

Ist G eine Gruppe mit Normalteilern N, N', sodass $G = NN'$ und $N \cap N' = \{1_G\}$ gilt, dann ist $G \cong N \times N'$.

Wir schwächen die Voraussetzungen jetzt dahingehend ab, dass nur noch eine der beiden Untergruppen ein Normalteiler sein muss.

LEMMA $G = NU$

4.1. **Lemma.** *Sei G eine Gruppe mit einer Untergruppe U und einem Normalteiler N mit den Eigenschaften $G = NU$ und $N \cap U = \{1_G\}$. Dann ist die Abbildung $\phi\colon N \times U \to G$, $(n, u) \mapsto nu$, bijektiv. Auf $N \times U$ wird durch die Verknüpfung*

$$(n, u) \cdot (n', u') = (n \cdot un'u^{-1}, uu')$$

eine Gruppenstruktur definiert, bezüglich derer ϕ ein Isomorphismus ist.

Beweis. Aus $G = NU = \{nu \mid n \in N, u \in U\}$ folgt, dass ϕ surjektiv ist. Aus $\phi(n, u) = \phi(n', u')$, also $nu = n'u'$, folgt $N \ni n'^{-1}n = u'u^{-1} \in U$; $N \cap U = \{1_G\}$ impliziert dann $n'^{-1}n = u'u^{-1} = 1_G$, was $n = n'$ und $u = u'$ bedeutet. Das zeigt, dass ϕ auch injektiv ist.

Wegen $nu \cdot n'u' = n(un'u^{-1}) \cdot uu'$ ist $(n, u) \cdot (n', u') = \phi^{-1}\big(\phi(n, u) \cdot \phi(n', u')\big)$. Dass dies eine Gruppenstruktur auf $N \times U$ definiert, folgt daraus, dass ϕ bijektiv und G eine Gruppe ist; es ergibt sich auch unmittelbar, dass ϕ ein Isomorphismus ist. (Beachte, dass $un'u^{-1} \in N$ ist wegen $N \triangleleft G$.) ❑

Umgekehrt kann man zu Gruppen N und U und einer Operation von U auf N durch Gruppenautomorphismen (wie eben durch $u * n = unu^{-1}$) auf $N \times U$ eine Gruppenstruktur definieren, sodass die resultierende Gruppe G zu N und U isomorphe Untergruppen $N' = N \times \{1_U\}$ und $U' = \{1_N\} \times U$ hat, wobei N' ein Normalteiler ist und die Operation durch Konjugation von U' auf N' der gegebenen Operation von U auf N entspricht.

LEMMA semidirektes Produkt

4.2. **Lemma.** *Seien N und U Gruppen und $\varphi\colon U \times N \to N$, $(u, n) \mapsto u * n$, sei eine Operation von U auf N durch Gruppenautomorphismen. Dann definiert*

$$(n, u) \cdot (n', u') = (n \cdot (u * n'), uu')$$

eine Gruppenstruktur auf $N \times U$. Sei G die resultierende Gruppe. Dann sind $\phi_N\colon N \to G$, $n \mapsto (n, 1_U)$, und $\phi_U\colon U \to G$, $u \mapsto (1_N, u)$, injektive Gruppenhomomorphismen, sodass $N' = \operatorname{im}(\phi_N) = N \times \{1_U\}$ ein Normalteiler von G ist und $\phi_U(u)\phi_N(n)\phi_U(u)^{-1} = \phi_N(u * n)$ für alle $n \in N$ und $u \in U$ gilt.

Beweis. Wir prüfen die Gruppenaxiome nach. Die Assoziativität ergibt sich aus

$$\begin{aligned}
(n_1, u_1) \cdot \big((n_2, u_2) \cdot (n_3, u_3)\big) &= (n_1, u_1) \cdot \big(n_2 \cdot (u_2 * n_3), u_2u_3\big) \\
&= \big(n_1 \cdot u_1 * (n_2 \cdot (u_2 * n_3)), u_1(u_2u_3)\big) \\
&= \big(n_1 \cdot ((u_1 * n_2) \cdot (u_1 * (u_2 * n_3))), u_1(u_2u_3)\big) \\
&= \big((n_1 \cdot (u_1 * n_2)) \cdot ((u_1u_2) * n_3), (u_1u_2)u_3\big) \\
&= \big(n_1 \cdot (u_1 * n_2), u_1u_2\big) \cdot (n_3, u_3) \\
&= \big((n_1, u_1) \cdot (n_2, u_2)\big) \cdot (n_3, u_3)\,.
\end{aligned}$$

Das neutrale Element ist $(1_N, 1_U)$, denn

$$(1_N, 1_U) \cdot (n, u) = (1_N \cdot (1_U * n), 1_U u) = (n, u)$$

und

$$(n, u) \cdot (1_N, 1_U) = (n \cdot (u * 1_N), u 1_U) = (n, u)\,.$$

Das Inverse zu (n, u) ist $(u^{-1} * n^{-1}, u^{-1})$, denn

$$(n,u)\cdot(u^{-1}*n^{-1},u^{-1}) = \big(n\cdot(u*(u^{-1}*n^{-1})),uu^{-1}\big) = (n\cdot(1_U*n^{-1}),1_U) = (1_N,1_U)$$

und

$$(u^{-1}*n^{-1},u^{-1})\cdot(n,u) = \big((u^{-1}*n^{-1})\cdot(u^{-1}*n),u^{-1}u\big) = (u^{-1}*(n^{-1}n),1_U) = (1_N,1_U)\,.$$

Dass ϕ_N und ϕ_U injektiv sind, ist klar. Dass es Gruppenhomomorphismen sind, rechnet man leicht nach. $N' = N \times \{1_U\}$ ist ein Normalteiler, denn es gilt

$$(n, u) \cdot (n', 1) \cdot (n, u)^{-1} = (n'', u^{-1}u) = (n'', 1_U)$$

für ein $n'' \in N$. Das Element $\phi_U(u) = (1_N, u)$ operiert durch Konjugation auf $\phi_N(n) = (n, 1_U)$ via

$$(1_N, u) \cdot (n, 1_U) \cdot (1_N, u)^{-1} = \big(1_N \cdot (u * n) \cdot (u * 1_N), uu^{-1}\big) = (u * n, 1_U)$$

wie behauptet. ❑

* 4.3. **Definition.** In der Situation von Lemma 4.2 heißt G das *semidirekte Produkt* von N und U bezüglich φ und wird $G = N \rtimes_\varphi U$ geschrieben. Ist aus dem Kontext klar, welche Operation φ gemeint ist, schreibt man auch einfach $N \rtimes U$. ♢ **DEF** semidirektes Produkt

Damit lässt sich Lemma 4.1 auch so formulieren:

4.4. **Lemma.** *Sei G eine Gruppe mit einem Normalteiler N und einer Untergruppe U mit den Eigenschaften $G = NU$ und $N \cap U = \{1_G\}$. Dann ist G isomorph zum semidirekten Produkt von N und U bezüglich der Operation von U auf N durch Konjugation.* **LEMMA** $G \cong N \rtimes U$

4.5. **Beispiel.** Die Diedergruppe D_n der Ordnung $2n$ ist isomorph zum semidirekten Produkt $\mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$, wobei ± 1 auf $\mathbb{Z}/n\mathbb{Z}$ durch Multiplikation operiert. Denn D_n enthält eine zyklische Untergruppe C_n der Ordnung n (die Drehungen), die Index 2 hat und deshalb ein Normalteiler ist, und ein Element τ (jede Spiegelung an einer Geraden) der Ordnung 2 mit $\tau \notin C_n$. Es folgt $C_n \cap \langle\tau\rangle = \{\mathrm{id}\}$ und damit auch (wegen $\#C_n \cdot \#\langle\tau\rangle = \#D_n$) $C_n\langle\tau\rangle = D_n$. Für eine Drehung $\sigma \in C_n$ gilt $\tau\sigma\tau^{-1} = \sigma^{-1}$ (das ist äquivalent zu $(\tau\sigma)^2 = \mathrm{id}$, was daraus folgt, dass $\tau\sigma$ eine Spiegelung ist), also ist die Operation von τ auf C_n durch Inversion gegeben. In der zu C_n isomorphen Gruppe $\mathbb{Z}/n\mathbb{Z}$ entspricht das der Negation $[a] \mapsto [-a]$. ♣ **BSP** Diedergruppe

Wann ist $N \rtimes U$ abelsch?

LEMMA $N \rtimes U$ abelsch

4.6. **Lemma.** *Ein semidirektes Produkt $N \rtimes_\varphi U$ ist genau dann abelsch, wenn N und U beide abelsch sind und die Operation von U auf N trivial ist. In diesem Fall ist $N \rtimes_\varphi U = N \times U$.*

Beweis. Ist φ trivial, dann ist $N \rtimes_\varphi U = N \times U$. Es ist dann klar, dass das Produkt genau dann abelsch ist, wenn beide Faktoren abelsch sind. Ist φ nicht trivial, dann gilt $\phi_U(u)\phi_N(n)\phi_U(u)^{-1} \neq \phi_N(n)$ für geeignete $u \in U$ und $n \in N$, damit ist das semidirekte Produkt nicht abelsch. ❑

Die Operation φ von U auf N entspricht nach Lemma 2.2 (und dem folgenden Text) einem Gruppenhomomorphismus $U \to \mathrm{Aut}(N)$. Für Anwendungen ist es daher wichtig, die Struktur von $\mathrm{Aut}(N)$ zu kennen. Wir bestimmen hier die Automorphismengruppe einer zyklischen Gruppe.

LEMMA $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

4.7. **Lemma.** *Sei $G = \langle g \rangle$ zyklisch der Ordnung n. Dann ist*

$$\psi\colon (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(G), \quad [a] \longmapsto (\gamma \mapsto \gamma^a)$$

ein Gruppenisomorphismus.

Beweis. Zunächst einmal ist ψ wohldefiniert, denn $\gamma \mapsto \gamma^a$ definiert einen Endomorphismus von G (weil G abelsch ist, gilt $(\gamma_1\gamma_2)^a = \gamma_1^a\gamma_2^a$), der nur von der Restklasse $[a]$ abhängt (denn $\gamma^n = 1_G$) und bijektiv ist (wegen $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ gibt es $b \in \mathbb{Z}$ mit $ab \equiv 1 \bmod n$; dann ist $\gamma \mapsto \gamma^b$ die inverse Abbildung). Wegen $\big(\psi([ab])\big)(\gamma) = \gamma^{ab} = (\gamma^b)^a = \big(\psi([a]) \circ \psi([b])\big)(\gamma)$ ist ψ ein Homomorphismus. Außerdem ist ψ surjektiv, denn jeder Automorphismus ϕ von G muss g auf einen Erzeuger von G abbilden; dieser hat die Form $\phi(g) = g^a$ mit $a \perp n$, siehe Lemma 3.1. Es folgt $\phi(g^k) = \phi(g)^k = (g^a)^k = (g^k)^a$, also $\phi = \psi([a])$. Für $[a] \neq [1]$ gilt $(\psi([a]))(g) = g^a \neq g$, also $\psi([a]) \neq \mathrm{id}_G$; damit ist ψ auch injektiv. ❑

BSP nicht-abelsche Gruppe

4.8. **Beispiel.** Es gibt eine nicht-abelsche Gruppe der Ordnung 2019.

Es ist $2019 = 3 \cdot 673$. Die Automorphismengruppe von $\mathbb{Z}/673\mathbb{Z}$ hat Ordnung $\varphi(673) = 672$ und enthält eine Untergruppe der Ordnung 3. Es gibt also eine nichttriviale Operation ϕ von $\mathbb{Z}/3\mathbb{Z}$ auf $\mathbb{Z}/673\mathbb{Z}$; damit ist $\mathbb{Z}/673\mathbb{Z} \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$ eine nicht abelsche Gruppe der Ordnung 2019. ♣

Wir beweisen hier gleich noch eine allgemeine Aussage über multiplikative Gruppen von Körpern, die uns unter anderem zeigt, dass $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ für Primzahlen p zyklisch ist.

SATZ endliche Untergruppen von $K^\times$

∗ 4.9. **Satz.** *Seien K ein Körper und $G \leq K^\times$ endlich. Dann ist G zyklisch. Insbesondere ist für jede Primzahl p die Gruppe $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ zyklisch.*

Beweis. Sei $\#G = n$. Dann gilt $g^n = 1$ für jedes $g \in G$. Damit besteht G genau aus den Nullstellen des Polynoms $X^n - 1$ in K (das Polynom hat höchstens n Nullstellen und alle Elemente von G sind Nullstellen). Ist d ein Teiler von n und U eine Untergruppe von G der Ordnung d, dann folgt analog, dass U die Menge der Nullstellen von $X^d - 1$ ist. Es gibt also höchstens eine Untergruppe der Ordnung d. Lemma 3.3 zeigt dann, dass G zyklisch ist.

Ist p eine Primzahl, dann ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper. Die Gruppe $\mathbb{F}_p^\times$ ist selbst endlich und damit zyklisch. ❑

Jetzt können wir die Klassifikation der Gruppen der Ordnung pq abschließen.

SATZ Gruppen der Ordnung pq

4.10. **Satz.** *Seien $p < q$ Primzahlen und G eine Gruppe der Ordnung pq. Gilt $q \not\equiv 1 \bmod p$, dann ist G zyklisch. Anderenfalls ist G entweder zyklisch oder isomorph zum semidirekten Produkt $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ und nicht abelsch, wobei die Operation von $\mathbb{Z}/p\mathbb{Z}$ auf $\mathbb{Z}/q\mathbb{Z}$ nichttrivial ist. Alle diese semidirekten Produkte sind isomorph.*

Beweis. Den Fall $q \not\equiv 1 \bmod p$ hatten wir bereits in Satz 3.12 behandelt. Wir können also $q \equiv 1 \bmod p$ voraussetzen. Wie im Beweis von Satz 3.12 hat G genau eine Untergruppe N der Ordnung q, die also ein Normalteiler ist. Die Anzahl der Untergruppen von G der Ordnung p ist ein Teiler von q, also entweder 1 oder q. Im ersten Fall ist G wie im Beweis von Satz 3.12 zyklisch. Im zweiten Fall sei U eine Untergruppe der Ordnung p. Da die Ordnungen von N und U teilerfremd sind, muss $N \cap U = \{1_G\}$ sein. Dann ist die Abbildung $N \times U \to G$, $(n, u) \mapsto nu$, injektiv, und weil beide Seiten dieselbe Kardinalität pq haben auch surjektiv, also gilt auch $NU = G$. Damit ist G isomorph zu $N \rtimes_\varphi U$ mit einer nichttrivialen Operation φ (denn U ist kein Normalteiler, also ist G nicht abelsch). Die Operation ist gegeben durch $\Phi\colon U \to \mathrm{Aut}(N) \cong \mathbb{F}_q^\times$. Die Gruppe $\mathbb{F}_q^\times$ ist nach Satz 4.9 zyklisch, hat also genau eine Untergruppe A der Ordnung p. Ist Φ nichttrivial, dann muss Φ injektiv sein mit $\Phi(U) = A$. Je zwei solche Homomorphismen Φ, Φ' erfüllen $\Phi' = \Phi \circ \alpha$ mit $\alpha \in \mathrm{Aut}(U)$; die zugehörigen semidirekten Produkte sind dann isomorph vermöge

$$N \rtimes_{\varphi'} U \xrightarrow{\mathrm{id} \times \alpha} N \rtimes_\varphi U\,.$$

Denn diese Abbildung ist offensichtlich bijektiv und auch ein Homomorphismus:

$$\begin{aligned}(\mathrm{id} \times\alpha)\big((n,u) \underset{\varphi'}{\cdot} (n',u')\big) &= (\mathrm{id} \times\alpha)\big(n \cdot (\Phi'(u))(n'), uu'\big)\\ &= \big(n \cdot (\Phi(\alpha(u)))(n'), \alpha(uu')\big) = (n, \alpha(u)) \underset{\varphi}{\cdot} (n', \alpha(u'))\\ &= (\mathrm{id} \times\alpha)(n,u) \underset{\varphi}{\cdot} (\mathrm{id} \times\alpha)(n',u')\,.\end{aligned}$$

❑

Der Satz besagt also im Fall $q \equiv 1 \bmod p$, dass es genau zwei Isomorphieklassen von Gruppen der Ordnung pq gibt, nämlich die zyklische Gruppe und eine nicht-abelsche Gruppe. Insbesondere sind je zwei nicht-abelsche Gruppen der Ordnung pq isomorph.

FOLG $\#G = 2p$

4.11. **Folgerung.** *Seien p eine ungerade Primzahl und G eine Gruppe der Ordnung $2p$. Dann ist G entweder zyklisch oder isomorph zur Diedergruppe D_p.*

Beweis. Nach Satz 4.10 (mit $(p,q) := (2,p)$) sind alle nicht-zyklischen Gruppen der Ordnung $2p$ isomorph. Da die Diedergruppe D_p nicht zyklisch ist, folgt die Behauptung. ❑

BSP Gruppen kleiner Ordnung

4.12. **Beispiel.** Damit sind die Gruppen G mit $\#G \leq 15$, $\#G \neq 8, 12$ bis auf Isomorphie klassifiziert:

- Für $\#G = 1$ gibt es nur die triviale Gruppe.
- Für $\#G = p$ prim (also $\#G \in \{2, 3, 5, 7, 11, 13\}$) gibt es nur die zyklische Gruppe $\mathbb{Z}/p\mathbb{Z}$.

- Für $\#G = p^2$ mit $p \in \{2, 3\}$ muss G abelsch sein (siehe Folgerung 2.19), also ist entweder $G \cong \mathbb{Z}/p^2\mathbb{Z}$ zyklisch oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Die für $p = 2$ auftretende Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong D_2$ heißt die *Kleinsche Vierergruppe*. (Manchmal wird dieser Name auch spezifischer für den zu dieser Gruppe isomorphen Normalteiler $V = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ der A_4 und S_4 verwendet.)

DEF Kleinsche Vierergruppe

- Für $\#G = 2p$ mit $p \in \{3, 5, 7\}$ gilt nach Folgerung 4.11, dass G entweder zyklisch oder G isomorph zur Diedergruppe D_p ist. Im Fall $p = 3$ gilt $D_3 \cong S_3$; somit ist die symmetrische Gruppe S_3 die kleinste nicht-abelsche Gruppe.
- Für $\#G = 15$ gilt nach Satz 4.10, dass G zyklisch ist. ♣

Beispiel. Die Klassifikation der Gruppen G der Ordnung 8 ist etwas komplizierter. Ist G abelsch, dann gibt es die drei Möglichkeiten

BSP $\#G = 8$

$$G \cong \mathbb{Z}/8\mathbb{Z}\,, \qquad G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{und} \quad G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

(vergleiche den Klassifikationssatz für endliche abelsche Gruppen).

Ist G nicht abelsch, dann wissen wir, dass das Zentrum $Z(G)$ nichttrivial ist (Folgerung 2.17) und dass $Z(G) \neq G$ gilt. Wäre $\#Z(G) = 4$, dann würde wie im Beweis von Folgerung 4.11 folgen, dass G doch abelsch wäre; dieser Fall kann also nicht eintreten. Es folgt $Z(G) = \{1, z\}$ mit einem $1_G \neq z \in G$.

G muss Elemente der Ordnung 4 enthalten (denn eine Gruppe, deren nichttriviale Elemente allesamt Ordnung 2 haben, ist abelsch — Übung). Sei $g \in G$ ein solches Element. Dann muss gelten $Z(G) \subset \langle g \rangle$, also $g^2 = z$, denn sonst wäre nach Lemma 3.9 G abelsch. Jetzt gibt es zwei Möglichkeiten. Die erste ist, dass ein Element von $G \setminus \langle g \rangle$ Ordnung 2 hat. Sei h ein solches Element. Da $\langle g \rangle$ ein Normalteiler ist, gilt $hgh = hgh^{-1} = g^{\pm 1}$. Es kann nicht $hgh^{-1} = g$ sein, da dann G abelsch wäre. Also ist $hgh^{-1} = g^{-1}$ und G ist isomorph zur Diedergruppe D_4. In diesem Fall haben dann *alle* Elemente von $G \setminus \langle g \rangle$ die Ordnung 2.

Die andere Möglichkeit ist, dass alle Elemente von $G \setminus \langle g \rangle$ die Ordnung 4 haben. Es gibt dann insgesamt sechs Elemente g der Ordnung 4 und g^2 ist stets das einzige Element der Ordnung 2, nämlich z. Wenn wir $-1 := z$ schreiben und Erzeuger von zwei verschiedenen Untergruppen der Ordnung 4 mit i und j bezeichnen, dann gilt $i^2 = j^2 = -1$. Das Element $k = ij$ muss ebenfalls Ordnung 4 haben und kann nicht in $\langle i \rangle$ oder $\langle j \rangle$ liegen. Für ji gilt das Gleiche; außerdem muss ji von ij verschieden sein (denn sonst wäre $G = \langle i, j \rangle$ abelsch). Das einzig verbleibende Element für ji ist dann $-k := (-1)k = k^{-1}$. Wir sehen, dass G isomorph zur *Quaternionengruppe*

DEF Quaternionengruppe

$$Q = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}^\times$$

ist.

Es gibt also insgesamt fünf verschiedene Isomorphietypen von Gruppen der Ordnung 8, nämlich die drei abelschen und dazu D_4 und Q. ♣

Auch für ungerade Primzahlen p gilt, dass es drei abelsche und zwei nicht-abelsche Isomorphietypen von Gruppen der Ordnung p^3 gibt. Diese beiden nicht-abelschen Gruppen haben aber eine andere Struktur als D_4 und Q; der Beweis ist daher etwas anders (Bonus-Aufgabe). Eine solche Gruppe ist

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F}_p \right\} \leq \mathrm{SL}(3, \mathbb{F}_p)\,;$$

das ist eine p-Sylowgruppe in $\mathrm{SL}(3, \mathbb{F}_p)$. Für $p = 2$ gilt $H_2 \cong D_4$, denn H_2 ist nicht abelsch und enthält genau zwei Elemente der Ordnung 4 (nämlich die mit $a = c = 1$).

Man kann die Sätze von Sylow auch benutzen, um zum Beispiel die Gruppen der Ordnung 12 zu klassifizieren (Übungsaufgabe). Neben den beiden Typen $\mathbb{Z}/12\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ von abelschen Gruppen gibt es drei Typen von nicht-abelschen Gruppen, nämlich die Diedergruppe D_6, die alternierende Gruppe A_4 und eine weitere Gruppe $G = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, wobei ein Erzeuger von $\mathbb{Z}/4\mathbb{Z}$ durch Negation auf $\mathbb{Z}/3\mathbb{Z}$ operiert. Man kann die Gruppe daher auch beschreiben als $G = \langle a, b \rangle$ mit $\mathrm{ord}(a) = 3$, $\mathrm{ord}(b) = 4$, $bab^{-1} = a^{-1}$.

Im Allgemeinen kann die Klassifikation der Gruppen der Ordnung n allerdings recht kompliziert werden, besonders wenn n durch eine hohe Zweierpotenz teilbar ist.

Als weitere Anwendung der Sylowschen Sätze kann man beweisen, dass die A_5 (mit $\#A_5 = 60$) die kleinste nicht-abelsche einfache Gruppe ist. Dazu ist zu zeigen, dass jede Gruppe G der Ordnung $n = \#G < 60$, sodass $n > 1$ keine Primzahl ist, einen nichttrivialen Normalteiler hat. Für $n = pq$ mit Primzahlen p, q folgt das aus Folgerung 2.19 (für den Fall $p = q$) und Satz 4.10. Es bleiben

$$n = 8, 12, 16, 18, 20, 24, 27, 28, 30, 32, 36, 40, 42, 44, 45, 48, 50, 52, 54, 56\,.$$

Ist n eine Primzahlpotenz, dann ist G abelsch oder $Z(G)$ ist ein nichttrivialer Normalteiler; in beiden Fällen ist G nicht einfach. Ist $n = kp^e$ mit p prim und $p \nmid k$, sodass $1 < k < p$ ist, dann erfüllt die Anzahl s_p der p-Sylowgruppen von G die Bedingungen $s_p \equiv 1 \bmod p$ und $s_p \mid k$, was hier $s_p = 1$ bedeutet. Damit hat G einen Normalteiler der Ordnung p^e und ist nicht einfach. Damit sind $n = 8$, 16, 18, 20, 27, 28, 32, 42, 44, 50, 52 und 54 erledigt. Es bleiben $n = 12, 24, 30, 36, 40, 45, 48$ und 56. Die Fälle $n = 40$ und 45 werden durch die Überlegung erledigt, dass es jeweils nur eine 5-Sylowgruppe geben kann.

Wir beweisen eine Hilfsaussage.

Lemma. *Sei G eine endliche Gruppe mit einer Untergruppe U, deren Konjugationsklasse $\{gUg^{-1} \mid g \in G\}$ genau $m > 1$ Elemente habe. Ist $\#G > m!$, dann ist G nicht einfach.* **LEMMA**

Beweis. Sei X die Konjugationsklasse von U. G operiert auf X transitiv durch Konjugation; das liefert einen Homomorphismus $\phi\colon G \to S(X) \cong S_m$. Da die Operation transitiv ist, kann das Bild von ϕ nicht trivial sein, also ist $\ker(\phi)$ eine echte Untergruppe. Da $\#G > \#S_m$ ist, kann ϕ nicht injektiv sein, also ist $\ker(\phi)$ ein nichttrivialer Normalteiler von G. ❑

Das lässt sich auf Gruppen mit $\#G = kp^e$ anwenden, wenn $\#G > k!$ ist: Es gibt höchstens k p-Sylowgruppen in G, die eine Konjugationsklasse bilden. Entweder gibt es nur eine p-Sylowgruppe in G, dann ist sie ein Normalteiler und G ist nicht einfach, oder das Lemma ist anwendbar. Das erledigt $n = 12$, 24, 36, 48. Es bleiben $n = 30$ und 56. Hierfür braucht man noch eine andere Überlegung.

Im Fall $n = 56$ gilt für die Anzahl s_7 der 7-Sylowgruppen $s_7 \in \{1, 8\}$. Im Fall $s_7 = 1$ ist die 7-Sylowgruppe ein Normalteiler. Im Fall $s_7 = 8$ gibt es $8 \cdot 6 = 48$ Elemente der Ordnung 7 in G (zwei verschiedene Untergruppen der Ordnung 7 können nur das neutrale Element gemeinsam haben). Neben dem neutralen Element bleiben also noch sieben Elemente übrig, was gerade für eine 2-Sylowgruppe (der Ordnung 8) reicht. Also ist die 2-Sylowgruppe ein Normalteiler.

Im Fall $n = 30$ ist $s_5 = 1$ oder $s_5 = 6$. Im ersten Fall ist die 5-Sylowgruppe ein Normalteiler. Im zweiten Fall gibt es $6 \cdot 4 = 24$ Elemente der Ordnung 5. Es bleiben fünf Elemente $\neq 1_G$ mit anderen Ordnungen übrig. Entweder gibt es genau ein Element g der Ordnung 2, dann ist $\langle g\rangle$ ein nichttrivialer Normalteiler. Oder es gibt mindestens drei solche Elemente (die Anzahl muss ungerade sein). Weil es auch mindestens zwei Elemente der Ordnung 3 geben muss, gibt es dann genau zwei solche Elemente, h und h^{-1}, und $\langle h\rangle$ ist ein nichttrivialer Normalteiler.

Damit ist gezeigt, dass es keine nicht-abelsche einfache Gruppe G mit $\#G < 60$ gibt. Es bleibt nachzuweisen, dass jede einfache Gruppe G der Ordnung 60 zur A_5 isomorph ist. So ein G hat $s_5 = 6$; die Konstruktion im Beweis des Lemmas oben liefert einen Homomorphismus $G \to S_6$, der injektiv sein muss. G ist also isomorph zu einer Untergruppe der S_6, die Ordnung 60 hat und transitiv operiert. Man stellt dann fest, dass diese Untergruppen alle zur A_5 isomorph sind. Alternativ kann man durch ähnliche (aber deutlich aufwändigere) Überlegungen wie oben für den Fall $\#G = 30$ zeigen, dass G genau fünf 2-Sylowgruppen haben muss. Man erhält dann analog wie eben eine Einbettung $G \to S_5$, deren Bild wegen $\#G = 60$ die A_5 sein muss (Bonus-Aufgabe).

5. Körpererweiterungen

Das zweite große Thema dieser Vorlesung nach der Gruppentheorie ist die Theorie der Körpererweiterungen.

* 5.1. **Definition.** Sei K ein Körper. Ein *Teilkörper* von K ist ein Unterring $k \subset K$, der ein Körper ist (d.h., sodass für alle $a \in k \setminus \{0\}$ auch $a^{-1} \in k$ ist). In diesem Fall heißt $k \subset K$ (auch K/k oder $K|k$ geschrieben) eine *Körpererweiterung* von k.

Ist L ein weiterer Teilkörper von K mit $k \subset L \subset K$, dann heißt L ein *Zwischenkörper* der Körpererweiterung $k \subset K$. ♢

DEF
Teilkörper
Körpererweiterung
Zwischenkörper

5.2. **Beispiele.** $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}(\boldsymbol{i}) \subset \mathbb{C}$ sind Körpererweiterungen. $\mathbb{Q}(\boldsymbol{i})$ und $\mathbb{R}$ sind Zwischenkörper von $\mathbb{Q} \subset \mathbb{C}$. ♣

BSP
Körpererweiterungen

Ein Homomorphismus $\phi\colon K \to L$ zwischen Körpern ist dasselbe wie ein Ringhomomorphismus. Man beachte, dass ein Körperhomomorphismus stets injektiv ist: Der Kern von ϕ ist ein Ideal von K, muss also entweder trivial sein oder ganz K. Der zweite Fall ist wegen $\phi(1) = 1 \neq 0$ nicht möglich. Man identifiziert daher häufig K mit seinem Bild unter der Einbettung ϕ und erhält eine Körpererweiterung $K = \phi(K) \subset L$.

Man sieht ganz genauso wie bei Unterringen oder Untergruppen, dass beliebige Durchschnitte (und aufsteigende Vereinigungen) von Teilkörpern wieder Teilkörper sind. Wir können also wieder folgende Definition formulieren:

5.3. **Definition.** Seien $k \subset K$ eine Körpererweiterung und $A \subset K$ eine Teilmenge. Wir schreiben

$$k(A) = \bigcap \{L \mid k \subset L \subset K \text{ Zwischenkörper mit } A \subset L\}$$

für den kleinsten Teilkörper von K, der k und A enthält. Man sagt auch, $k(A)$ entstehe durch *(Körper-)Adjunktion* von A zu k. Ist $A = \{a_1, \ldots, a_n\}$ endlich, dann schreiben wir wie üblich $k(a_1, \ldots, a_n)$. Gilt $K = k(a)$ für geeignetes $a \in K$, dann heißt die Körpererweiterung $k \subset K$ *einfach*, und a heißt ein *primitives Element* der Körpererweiterung.

Sind $k_1, k_2 \subset K$ zwei Teilkörper, dann schreibt man auch k_1k_2 für den kleinsten Teilkörper $k_1(k_2) = k_2(k_1)$ von K, der sowohl k_1 als auch k_2 enthält, und nennt ihn das *Kompositum* von k_1 und k_2. ♢

DEF
Adjunktion
einfache Körpererw.
primitives Element
Kompositum

Man vergleiche die Definition von $k[A]$ als dem kleinsten Unter*ring* von K, der k und A enthält. In diesem Fall spricht man auch von *Ringadjunktion* von A zu k. Man kann $k(A)$ mit dem Quotientenkörper von $k[A]$ identifizieren.

Wir hatten schon Beispiele wie $\mathbb{Q}(\boldsymbol{i})$ oder $\mathbb{Q}(\sqrt{2})$ gesehen. Ein anderes Beispiel ist $\mathbb{C} = \mathbb{R}(\boldsymbol{i})$; $\mathbb{C}$ ist also eine einfache Erweiterung von $\mathbb{R}$.

5.4. **Definition.** Man kann auch den Durchschnitt *aller* Teilkörper eines Körpers K betrachten. Dies ist offenbar der kleinste Körper, der in K enthalten ist und heißt der *Primkörper* von K. ♢ **DEF** Primkörper

Bevor wir uns ansehen, wie diese Primkörper aussehen können, führen wir einen weiteren Begriff ein. Wir erinnern uns daran, dass es für jeden Ring R einen eindeutig bestimmten Ringhomomorphismus $\phi_R\colon \mathbb{Z} \to R$ gibt (denn $1_\mathbb{Z}$ muss auf 1_R abgebildet werden; alles andere ergibt sich daraus). Der Kern von ϕ_R ist ein Ideal von $\mathbb{Z}$, kann also als $\ker(\phi_R) = n\mathbb{Z}$ mit $n \in \mathbb{Z}_{\geq 0}$ geschrieben werden.

* 5.5. **Definition.** Sei R ein Ring. Der nichtnegative Erzeuger des Ideals $\ker(\phi_R)$ von $\mathbb{Z}$ heißt die *Charakteristik* von R, $\mathrm{char}(R)$. ♢ **DEF** Charakteristik

5.6. **Lemma.** *Ist R ein Integritätsbereich (z.B. ein Körper), dann ist* $\mathrm{char}(R)$ *entweder null oder eine Primzahl.* **LEMMA** Charakteristik

Beweis. Wir müssen den Fall ausschließen, dass $n = \mathrm{char}(R) > 0$ eine zusammengesetzte Zahl oder $n = 1$ ist. Im Fall $n = 1$ wäre $1 \in \ker(\phi_R)$, also $1_R = \phi_R(1) = 0_R$, was der Voraussetzung widerspricht (in einem Integritätsbereich sind 0 und 1 verschieden).

Sei also n zusammengesetzt und $n = n_1 n_2$ eine nichttriviale Faktorisierung. Dann gilt $\phi_R(n_1), \phi_R(n_2) \neq 0$, aber $\phi_R(n_1)\phi_R(n_2) = \phi_R(n_1 n_2) = \phi_R(n) = 0$, also hat R Nullteiler; das ist ein Widerspruch. ❑

5.7. **Lemma.** *Sei K ein Körper. Gilt* $\mathrm{char}(K) = 0$*, dann ist der Primkörper von K isomorph zu $\mathbb{Q}$; insbesondere ist K unendlich. Anderenfalls ist* $\mathrm{char}(K) = p$ *eine Primzahl, und der Primkörper von K ist isomorph zu $\mathbb{F}_p$.* **LEMMA** Primkörper

Ein Körper der Charakteristik p kann endlich sein (wie etwa $\mathbb{F}_p$ selbst), kann aber auch unendlich sein (wie etwa der Quotientenkörper $\mathbb{F}_p(X)$ des Polynomrings $\mathbb{F}_p[X]$).

Beweis. Sei P der Primkörper von K. Dann ist (wegen der Eindeutigkeit von ϕ_R) $\phi_P = \phi_K$ mit Ziel eingeschränkt auf P, also ist $\mathrm{im}(\phi_K) \subset P$. Im Fall $\mathrm{char}(K) = 0$ ist ϕ_K injektiv, also ist $\mathrm{im}(\phi_K) \cong \mathbb{Z}$. Nach der Definition des Quotientenkörpers (Satz 8.1 im Skript zur „Einführung in die Zahlentheorie und algebraische Strukturen“) gibt es eine Fortsetzung von ϕ_K zu einem Homomorphismus $\tilde{\phi}_K\colon \mathbb{Q} \to P \subset K$. Als Homomorphismus zwischen Körpern ist $\tilde{\phi}_K$ injektiv, und sein Bild ist ein in P enthaltener Teilkörper von K; es folgt $P = \mathrm{im}(\tilde{\phi}_K) \cong \mathbb{Q}$.

Im Fall $\mathrm{char}(K) = p > 0$ ist $\ker(\phi_K) = p\mathbb{Z}$, also ist $\mathrm{im}(\phi_K) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ bereits ein Körper und es folgt $P = \mathrm{im}(\phi_K)$. ❑

Man sieht, dass $\mathrm{char}(K)$ nur vom Primkörper von K abhängt (und umgekehrt). Insbesondere gilt in einer Körpererweiterung $k \subset K$ stets $\mathrm{char}(k) = \mathrm{char}(K)$.

Wir kommen jetzt zu einer einfachen Beobachtung, die für die Körpertheorie jedoch sehr wichtig ist, weil sie eine Verbindung zur Linearen Algebra aufzeigt.

Sei $k \subset K$ eine Körpererweiterung. Indem wir die Multiplikation von K auf $k \times K$ einschränken, erhalten wir eine skalare Multiplikation von k auf K. Aus den Körperaxiomen folgt dann sofort, dass K ein *k-Vektorraum* ist. Zum Beispiel ist $\mathbb{C}$ ein zweidimensionaler $\mathbb{R}$-Vektorraum und $\mathbb{R}$ ist ein unendlichdimensionaler

$\mathbb{Q}$-Vektorraum (denn jeder endlichdimensionale $\mathbb{Q}$-Vektorraum ist abzählbar). Das ermöglicht die folgende Definition.

5.8. **Definition.** Sei $k \subset K$ eine Körpererweiterung. Dann heißt die Dimension von K als k-Vektorraum, **DEF** Grad (un)endliche Körpererw.

$$[K : k] = \dim_k K \in \{1, 2, 3, \ldots, \infty\},$$

der *Grad* der Körpererweiterung $k \subset K$ oder auch der *Körpergrad* von K über k. Ist $[K : k] < \infty$, dann heißt die Körpererweiterung $k \subset K$ *endlich*, sonst *unendlich*. Im Fall $[K : k] = 1$ ist $k = K$ und die Körpererweiterung heißt *trivial*. Im Fall $[K : k] = 2$ heißt die Körpererweiterung auch *quadratisch*, im Fall $[K : k] = 3$ *kubisch*. ♢

5.9. **Beispiele.** Es ist $[\mathbb{C} : \mathbb{R}] = 2$ und $[\mathbb{R} : \mathbb{Q}] = \infty$. Ist F ein endlicher Körper, dann ist $\mathrm{char}(F) = p$ eine Primzahl (nach Lemma 5.7), also $\mathbb{F}_p \subset F$, wenn wir den Primkörper mit $\mathbb{F}_p$ identifizieren; außerdem $[F : \mathbb{F}_p] = n < \infty$. Es folgt $\#F = p^n$, denn F ist ein n-dimensionaler Vektorraum über $\mathbb{F}_p$. Wir werden später zeigen, dass es zu jeder Primzahlpotenz p^n auch einen Körper mit p^n Elementen gibt. ♣ **BSP** Körpergrad

* 5.10. **Satz.** *Sei $k \subset L \subset K$ ein Zwischenkörper. Dann gilt* **SATZ** Gradsatz

$$[K : k] = [K : L] \cdot [L : k]$$

(mit der üblichen Rechenregel $n \cdot \infty = \infty \cdot n = \infty$ für $n \in \{1, 2, 3, \ldots, \infty\}$).

Beweis. Ist einer der Grade $[K : L]$ oder $[L : k]$ unendlich, dann gilt das auch für $[K : k]$, denn K enthält dann eine unendliche Menge über k (oder sogar über L) linear unabhängiger Elemente. Wir können also annehmen, dass $n = [K : L]$ und $m = [L : k]$ beide endlich sind. Wir wählen Basen $(x_1, \ldots, x_m)$ von L über k und $(y_1, \ldots, y_n)$ von K über L. Dann ist $B = (x_i y_j)_{1 \le i \le m, 1 \le j \le n}$ eine Basis von K über k: B ist ein Erzeugendensystem, denn jedes $\alpha \in K$ kann in der Form $\alpha = \sum_{j=1}^{n} a_j y_j$ mit $a_j \in L$ geschrieben werden, und jedes a_j kann wiederum als $a_j = \sum_{i=1}^{m} b_{ij} x_i$ mit $b_{ij} \in k$ geschrieben werden, also ist $\alpha = \sum_{i,j} b_{ij} x_i y_j$. B ist auch k-linear unabhängig, denn aus $\sum_{i,j} b_{ij} x_i y_j = 0$ mit $b_{ij} \in k$ folgt zunächst wegen der linearen Unabhängigkeit der y_j über L, dass $\sum_i b_{ij} x_i = 0$ sein muss für alle $1 \le j \le n$, und dann wegen der linearen Unabhängigkeit der x_i über k, dass alle $b_{ij} = 0$ sind.

Es folgt $[K : k] = \dim_k K = \#B = nm = [K : L] \cdot [L : k]$. ❑

5.11. **Folgerung.** *Sei $k \subset L \subset K$ ein Zwischenkörper und $[K : k] < \infty$. Dann ist $[L : k]$ ein Teiler von $[K : k]$, und $L = k$ gilt genau dann, wenn $[K : L] = [K : k]$ ist.* **FOLG** Grad eines Zwischenkörpers

Beweis. Die erste Aussage folgt unmittelbar aus Satz 5.10. Die zweite ergibt sich aus $L = k \iff [L : k] = 1 \iff [K : L] = [K : k]$. ❑

5.12. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung mit Zwischenkörpern L_1 und L_2. Dann gilt:* **LEMMA** Körpergrade

(1) $[L_1L_2 : L_1] \leq [L_2 : k]$.

(2) $[L_1L_2 : k] \leq [L_1 : k] \cdot [L_2 : k]$. *Ist die rechte Seite endlich und gilt Gleichheit, dann folgt $L_1 \cap L_2 = k$.*

(3) *Sind $[L_1 : k]$ und $[L_2 : k]$ endlich und teilerfremd, dann gilt Gleichheit in* (2).

(4) *Gilt $L_1 \cap L_2 = k$ und sind $[L_1 : k]$ und $[L_2 : k]$ endlich, dann folgt im Allgemeinen nicht, dass $[L_1L_2 : k] = [L_1 : k] \cdot [L_2 : k]$ ist.*

Beweis. Im Fall $[L_2 : k] = \infty$ ist nichts zu zeigen. Sei also $[L_2 : k] = n < \infty$ und $(b_1, b_2, \ldots, b_n)$ eine k-Basis von L_2 mit $b_1 = 1$. Sei $M = \langle b_1, \ldots, b_n \rangle_{L_1} \subset K$. Es ist klar, dass M sowohl L_1 als auch L_2 enthält. Außerdem muss jeder Teilkörper von K, der L_1 und L_2 enthält, auch M enthalten (denn alle Elemente von M sind Linearkombinationen von $b_1, \ldots, b_n \in L_2$ mit Koeffizienten in L_1). Wir zeigen, dass M ein Körper ist, dann ist M der *kleinste* Teilkörper von K, der L_1 und L_2 enthält, also folgt $M = L_1L_2$.

Zunächst ist klar, dass M unter Addition und Subtraktion abgeschlossen ist und 0 und 1 enthält. Da alle Produkte $b_ib_j \in L_2$ wieder als (k-)Linearkombinationen der b_i geschrieben werden können, ist M auch unter der Multiplikation abgeschlossen, also jedenfalls ein Unterring von K. Sei $0 \neq a \in M$. Dann ist die Abbildung $m_a : M \to M$, $x \mapsto ax$, L_1-linear und injektiv. Da M ein endlichdimensionaler L_1-Vektorraum ist, muss m_a auch surjektiv sein, also gibt es $x \in M$ mit $ax = 1$; damit ist $a^{-1} \in M$.

Der Rest des Beweises ist eine Übungsaufgabe. ❑

6. Algebraische Elemente und Erweiterungen

Wir kommen nun zu einer wichtigen Begriffsbildung in der Körpertheorie.

* 6.1. **Definition.** Sei $k \subset K$ eine Körpererweiterung.

DEF
algebraisch
transzendent
algebraisch abgeschlossen

(1) Ein Element $a \in K$ heißt *algebraisch über* k, wenn es ein normiertes Polynom $f \in k[X]$ gibt mit $f(a) = 0$. Ist a nicht algebraisch über k, dann heißt a *transzendent über* k. Im Fall $k = \mathbb{Q}$ und $K = \mathbb{R}$ oder $\mathbb{C}$ spricht man von *algebraischen* bzw. *transzendenten Zahlen*.

(2) Die Körpererweiterung $k \subset K$ heißt *algebraisch* und K heißt *algebraisch über* k, wenn alle Elemente von K über k algebraisch sind. Anderenfalls heißt die Körpererweiterung *transzendent*.

(3) k heißt *algebraisch abgeschlossen in* K, wenn jedes Element von K, das über k algebraisch ist, bereits in k liegt. In diesem Fall heißt die Körpererweiterung $k \subset K$ auch *rein transzendent*.

(4) Ein Körper k heißt *algebraisch abgeschlossen*, wenn jedes nicht konstante Polynom $f \in k[X]$ eine Nullstelle in k hat. ♢

Durch Induktion folgt leicht, dass über einem algebraisch abgeschlossenen Körper k jedes Polynom in Linearfaktoren zerfällt. Daraus folgt wiederum, dass k in jedem Erweiterungskörper algebraisch abgeschlossen ist.

6.2. **Beispiele.**

BSP
algebraische und transzendente Zahlen und Körpererweiterungen

(1) Die Zahlen $\sqrt{2}$, $\boldsymbol{i}$, $\sqrt[3]{2}$ sind algebraisch als Nullstellen von $X^2 - 2$, $X^2 + 1$, $X^3 - 2$. Ebenso sind alle Zahlen der Form $\zeta = e^{2\pi \boldsymbol{i} q}$ mit $q \in \mathbb{Q}$ algebraisch, denn ist $q = a/b$ mit $a, b \in \mathbb{Z}$ (und $b \neq 0$), dann ist ζ Nullstelle von $X^b - 1$.

(2) Die Zahlen e und π sind transzendent (Hermite 1873, Lindemann 1882). Demgegenüber ist unbekannt, ob $e + \pi$ und $e \cdot \pi$ beide transzendent sind. (Sie können jedenfalls nicht beide algebraisch sein, wie sich noch zeigen wird)

(3) $\mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn jede (echt) komplexe Zahl $z = a + b\boldsymbol{i}$ ist Nullstelle des reellen Polynoms $X^2 - 2aX + a^2 + b^2$. Insbesondere ist $\mathbb{R}$ nicht algebraisch abgeschlossen.

(4) Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen. Da $\mathbb{R}$ und $\mathbb{C}$ unter anderem durch topologische Eigenschaften definiert sind, kann es dafür keinen rein algebraischen Beweis geben. Der einfachste Beweis kann mit Hilfsmitteln der Funktionentheorie geführt werden (Satz von Liouville). ♣

C. Hermite
1822–1901

F. v. Lindemann
1852–1939

Im Folgenden wird mehrfach auf das Skript „Einführung in die Zahlentheorie und algebraische Strukturen“ vom Wintersemester 2017/18 verwiesen. Dies geschieht in der Form „EZAS.a.b“, wobei „a.b“ die Nummer der betreffenden Aussage ist.

Ist $k \subset K$ eine Körpererweiterung und $a \in K$, dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\phi_a \colon k[X] \longrightarrow K \qquad \text{mit } \phi_a|_k = \mathrm{id}_k \text{ und } \phi_a(X) = a,$$

vergleiche Satz EZAS.9.2 (universelle Eigenschaft des Polynomrings). (Wir schreiben hier der Kürze halber id_k auch für den Inklusionshomomorphismus $k \to K$.) Dies ist der Einsetzungshomomorphismus $f \mapsto f(a)$; es gilt $k[a] = \mathrm{im}(\phi_a)$. Wir haben dann folgende Charakterisierung.

SATZ Charakterisierung von „algebraisch“

6.3. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und $a \in K$. Sei ϕ_a wie oben. Dann sind folgende Aussagen äquivalent:*

(1) *a ist algebraisch über k.*

(2) *ϕ_a ist nicht injektiv.*

(3) *$k[a] = k(a)$.*

(4) *$k \subset k(a)$ ist eine endliche Körpererweiterung.*

In diesem Fall ist $\ker(\phi_a) = \langle f \rangle_{k[X]}$ *mit einem eindeutig bestimmten normierten irreduziblen Polynom $f \in k[X]$, und es gilt $[k(a) : k] = \deg(f)$.*

Beweis. „(1)⇒(2)“: Ist a algebraisch über k, dann gibt es ein normiertes Polynom $h \in k[X]$ mit $h(a) = 0$. Dann ist $0 \neq h \in \ker(\phi_a)$, also ist ϕ_a nicht injektiv.

„(2)⇒(3)“: Ist ϕ_a nicht injektiv, dann ist der Kern $\ker(\phi_a)$ ein von null verschiedenes Ideal von $k[X]$. Da $k[X]$ ein Hauptidealring ist, ist $\ker(\phi_a) = \langle f \rangle_{k[X]}$ mit einem Polynom $f \neq 0$, das bis auf Multiplikation mit einem Element aus $k^\times$ eindeutig bestimmt ist. Wenn wir zusätzlich fordern, dass f normiert ist, dann ist f eindeutig bestimmt. Nach dem Homomorphiesatz für Ringe EZAS.6.13 ist $k[a] = \mathrm{im}(\phi_a) \cong k[X]/\langle f \rangle_{k[X]}$. Da $k[a] \subset K$ ein Integritätsbereich ist, ist f ein Primelement und damit irreduzibel. Damit ist das von f erzeugte Ideal maximal, also ist $k[a]$ sogar ein Körper und damit gleich $k(a)$ (vgl. EZAS.6.18).

„(3)⇒(4)“: Gilt $k[a] = k(a)$, dann ist $\mathrm{im}(\phi_a)$ ein Körper, also ist $\ker(\phi_a)$ ein maximales Ideal und damit nicht das Nullideal; es gilt also $\ker(\phi_a) = \langle f \rangle_{k[X]}$ mit einem normierten Polynom f. Sei $n = \deg(f)$. Dann ist $1, a, a^2, \ldots, a^{n-1}$ eine Basis von $k[a] = k(a)$: Sei $b \in k[a]$ und $h \in k[X]$ ein Urbild von b unter ϕ_a. Dann gibt es $q, r \in k[X]$ mit $\deg(r) < n$ und $h = qf + r$, also ist

$$b = h(a) = q(a)f(a) + r(a) = r(a) \in \langle 1, a, a^2, \ldots, a^{n-1} \rangle_k \,.$$

Ist $r(a) = r_0 + r_1 a + \ldots + r_{n-1}a^{n-1} = 0$ mit $r_j \in k$, dann ist das zugehörige Polynom r im Kern von ϕ_a, also durch f teilbar. Wegen $\deg(r) < n = \deg(f)$ ist das nur für $r = 0$ möglich. Damit ist gezeigt, dass $1, a, \ldots, a^{n-1}$ ein linear unabhängiges Erzeugendensystem des k-Vektorraums $k[a]$ ist. Insbesondere ist $k(a) = k[a]$ eine endliche Erweiterung von k, und $[k(a) : k] = n = \deg(f)$.

„(4)⇒(1)“: Ist $k \subset k(a)$ eine endliche Körpererweiterung, dann müssen die unendlich vielen Elemente $1, a, a^2, \ldots \in k(a)$ über k linear abhängig sein. Es gibt also eine Relation

$$h_0 + h_1 a + h_2 a^2 + \ldots + h_n a^n = 0$$

mit $h_j \in k$ und $h_n \neq 0$. Nach Skalieren können wir annehmen, dass $h_n = 1$ ist. Dann ist a eine Nullstelle des normierten Polynoms

$$h = X^n + h_{n-1}X^{n-1} + \ldots + h_2 X^2 + h_1 X + h_0 \in k[X] \,,$$

also ist a algebraisch über k. ❑

Man sieht, dass Algebraizität eine *Endlichkeitsbedingung* ist (wie zum Beispiel auch Kompaktheit in der Topologie): Aus dem Beweis folgt die Äquivalenz

$$a \text{ algebraisch} \iff \dim_k k[a] < \infty \,.$$

Das in Satz 6.3 auftretende Polynom f hat einen Namen:

∗ 6.4. **Definition.** Sei $k \subset K$ eine Körpererweiterung und sei $a \in K$ algebraisch über k. Dann heißt das (nach Satz 6.3 existierende und eindeutig bestimmte) normierte und irreduzible Polynom $f \in k[X]$ mit $f(a) = 0$ das *Minimalpolynom* von a über k, und der Grad $[k(a) : k] = \deg(f)$ heißt der *Grad* von a über k. ♢

DEF Minimalpolynom

Dieser Begriff ist analog zum Minimalpolynom einer Matrix, das wir in der Linearen Algebra eingeführt haben.

Da der Kern von ϕ_a vom Minimalpolynom f von a erzeugt wird, folgt für ein Polynom $h \in k[X]$: $h(a) = 0$ gilt genau dann, wenn h ein Vielfaches von f ist.

Satz 6.3 hat einige wichtige Konsequenzen.

6.5. **Folgerung.** *Sei $k \subset K$ eine Körpererweiterung und sei $a \in K$. Ist a Nullstelle eines normierten irreduziblen Polynoms $f \in k[X]$, dann ist f das Minimalpolynom von a. Insbesondere gilt $[k(a) : k] = \deg(f)$ und a ist algebraisch über k.*

FOLG Minimalpolynom

Beweis. Da a Nullstelle eines normierten Polynoms mit Koeffizienten in k ist, ist a algebraisch über k. Sei $m \in k[X]$ das Minimalpolynom von a über k. Aus $f(a) = 0$ folgt $m \mid f$, und da f irreduzibel und normiert ist, muss $f = m$ gelten. Die Aussage über den Grad von a über k war Teil von Satz 6.3. ❑

6.6. **Beispiel.** Zum Beispiel ist $[\mathbb{Q}(\sqrt[7]{5}) : \mathbb{Q}] = 7$, weil $\sqrt[7]{5}$ Nullstelle des (nach Eisenstein) irreduziblen Polynoms $X^7 - 5$ ist. ♣

BSP Grad über Minimalpolynom

6.7. **Folgerung.** *Sei $k \subset K$ eine Körpererweiterung. Sind $a, b \in K$ algebraisch über k, dann sind auch $a \pm b$, ab und (falls $b \neq 0$) a/b algebraisch über k. Insbesondere ist die Menge aller über k algebraischen Elemente von K ein Körper.*

FOLG algebraische Elemente bilden Körper

6.8. **Definition.** Dieser Teilkörper von K heißt der *algebraische Abschluss* von k in K. ♢

DEF algebraischer Abschluss in K

Beweis. Sind a und b algebraisch über k, dann gilt $[k(a) : k], [k(b) : k] < \infty$ nach Satz 6.3. Aus Lemma 5.12 ergibt sich, dass dann $k(a, b)$ ebenfalls eine endliche Erweiterung von k ist. Da $a \pm b$, ab und a/b Elemente von $k(a, b)$ sind, müssen die von ihnen erzeugten Körpererweiterungen von k ebenfalls endlich sein. Wiederum nach Satz 6.3 müssen diese Elemente algebraisch über k sein. ❑

Das bedeutet also, dass, wenn a und b Nullstellen von normierten Polynomen über k sind, dies auch für $a \pm b$, ab und a/b gilt. Wie man aus den Minimalpolynomen von a und b geeignete Polynome für $a \pm b$ usw. bestimmen kann, ist eine andere Frage. Eine Möglichkeit dafür liefert die *Resultante* von zwei Polynomen (das ist eine gewisse aus den Koeffizienten der Polynome gebildete Determinante).

BSP $\cos 2\pi/n$, $\sin 2\pi/n$ sind algebraisch

6.9. **Beispiel.** Für jedes $n \in \mathbb{Z}_{\geq 1}$ sind $\cos\frac{2\pi}{n}$ und $\sin\frac{2\pi}{n}$ algebraisch. Denn es ist $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ algebraisch (als Nullstelle von X^n-1), also ist $\cos\frac{2\pi}{n} = \frac{1}{2}(\zeta_n+\zeta_n^{-1})$ algebraisch. Weil $\boldsymbol{i} = \zeta_4$ ebenfalls algebraisch ist, ist auch $\sin\frac{2\pi}{n} = \frac{1}{2i}(\zeta_n - \zeta_n^{-1})$ algebraisch.

Sei $K_n = \mathbb{Q}(\cos\frac{2\pi}{n}) \subset \mathbb{Q}(\zeta_n)$. Für $n > 2$ gilt $[\mathbb{Q}(\zeta_n) : K_n] = 2$, denn ζ_n ist Nullstelle des Polynoms $X^2 - 2\cos\frac{2\pi}{n}X + 1 \in K_n[X]$, und $\mathbb{Q}(\zeta_n) \neq K_n$, denn $K_n \subset \mathbb{R}$, während ζ_n echt komplex ist. Man kann zeigen (wir werden das später tun), dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \boldsymbol{\varphi}(n)$ ist; es folgt $[K_n : \mathbb{Q}] = \frac{1}{2}\boldsymbol{\varphi}(n)$. Für $n = 7$ und $n = 9$ ist $\boldsymbol{\varphi}(n) = 6$, also haben die Minimalpolynome von $\cos\frac{2\pi}{7}$ und $\cos\frac{2\pi}{9}$ beide den Grad 3. (Bestimmung dieser Minimalpolynome als Übungsaufgabe.) ♣

FOLG endliche KE sind algebraisch

6.10. **Folgerung.** *Jede endliche Körpererweiterung $k \subset K$ ist algebraisch.*

Beweis. Ist $a \in K$, dann ist $k(a) \subset K$ endlich über k, also ist a nach Satz 6.3 algebraisch über k. ❑

BSP Umkehrung gilt nicht

6.11. **Beispiel.** Die Umkehrung von Folgerung 6.10 gilt nicht: Sei $\mathbb{A}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Dann ist $\mathbb{A}$ eine algebraische Erweiterung von $\mathbb{Q}$ von unendlichem Grad. Das kann man zum Beispiel so sehen: Für jedes $n \geq 1$ ist das Polynom $X^n - 2 \in \mathbb{Q}[X]$ irreduzibel (Eisenstein-Kriterium EZAS.10.13). Es gilt $\mathbb{Q}(\sqrt[n]{2}) \subset \mathbb{A} \cap \mathbb{R} \subset \mathbb{A}$, also auch $n = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \leq [\mathbb{A} \cap \mathbb{R} : \mathbb{Q}] \leq [\mathbb{A} : \mathbb{Q}]$. Der Körper $\mathbb{A}$ besteht aus allen algebraischen komplexen Zahlen. Dass er selbst algebraisch abgeschlossen ist, folgt aus dem folgenden Ergebnis. ♣

SATZ Transitivität der Algebraizität

6.12. **Satz.** *Seien $k \subset L \subset K$ Körpererweiterungen. K ist genau dann algebraisch über k, wenn sowohl L algebraisch über k als auch K algebraisch über L ist.*

Beweis. Wir nehmen zunächst an, dass $k \subset K$ algebraisch ist. Dann ist jedes Element $a \in K$ algebraisch über k, also ist jedes solche a auch algebraisch über L (denn jedes Polynom in $k[X]$ ist auch in $L[X]$), also ist $L \subset K$ algebraisch. Außerdem ist natürlich insbesondere jedes $a \in L$ algebraisch über k; damit ist auch $k \subset L$ algebraisch.

Seien jetzt $k \subset L$ und $L \subset K$ algebraisch, und sei $a \in K$. Da a nach Annahme algebraisch ist über L, gibt es ein normiertes Polynom $h \in L[X]$ mit $h(a) = 0$; sei $n = \deg(h)$. Seien $h_0, h_1, \ldots, h_{n-1} \in L$ die Koeffizienten von h (ohne $h_n = 1$). Da $k \subset L$ algebraisch ist, gilt mit Satz 6.3 und wiederholter Anwendung von Lemma 5.12, dass $L' = k(h_0, h_1, \ldots, h_{n-1})$ über k endlich ist. Wegen $h \in L'[X]$ gilt immer noch $[L'(a) : L'] < \infty$. Es folgt

$$[k(a) : k] \leq [L'(a) : k] = [L'(a) : L'] \cdot [L' : k] < \infty\,,$$

also ist a algebraisch über k. ❑

FOLG algebraischer Abschluss

6.13. **Folgerung.** *Sei $k \subset K$ eine Körpererweiterung, sei K ein algebraisch abgeschlossener Körper und sei $\bar{k} \subset K$ der algebraische Abschluss von k in K. Dann ist $\bar{k}$ ebenfalls algebraisch abgeschlossen.*

Beweis. Wir müssen zeigen, dass jedes nicht konstante Polynom $f \in \bar{k}[X]$ eine Nullstelle in $\bar{k}$ hat. Da K algebraisch abgeschlossen ist, hat f jedenfalls eine Nullstelle $a \in K$. Als Nullstelle eines Polynoms in $\bar{k}[X]$ ist a algebraisch über $\bar{k}$. Nach Satz 6.12 ist a dann auch algebraisch über k, also liegt a in $\bar{k}$. ❑

DEF algebraischer Abschluss

∗ 6.14. **Definition.** Ist k ein Körper und $k \subset K$ eine algebraische Körpererweiterung, sodass K algebraisch abgeschlossen ist, dann heißt K ein *algebraischer Abschluss* von k. ♢

Man kann zeigen, dass es für jeden Körper einen algebraischen Abschluss gibt, und dass dieser bis auf Isomorphie „über k“ eindeutig bestimmt ist, siehe zum Beispiel [Fi, § III.2.5] oder [KM, § 23].

Wir sehen jedenfalls, dass der in Beispiel 6.11 eingeführte Körper $\mathbb{A}$ der algebraischen Zahlen ein algebraischer Abschluss von $\mathbb{Q}$ ist.

7. Zerfällungskörper

Bisher haben wir stets „bereits vorhandene“ Körpererweiterungen $k \subset K$ betrachtet und (zum Beispiel) Elemente von K studiert. Man kann sich jedoch auch fragen, ob es zu gegebenem Körper k eine Körpererweiterung mit bestimmten gewünschten Eigenschaften gibt (etwa eine, die Nullstellen gewisser Polynome enthält) und wie man eine solche gegebenenfalls konstruiert. Der Beweis von Satz 6.3 weist dazu den Weg.

SATZ Existenz von Körpererweiterungen

7.1. **Satz.** *Sei k ein Körper und sei $f \in k[X]$ normiert und irreduzibel. Dann gibt es eine Körpererweiterung $k \subset K$ mit $[K : k] = \deg(f)$, sodass f in K eine Nullstelle hat.*

Eine solche Körpererweiterung kann konstruiert werden als $K = k[X]/\langle f \rangle_{k[X]}$.

Beweis. Wir definieren $K = k[X]/\langle f \rangle_{k[X]}$ wie angegeben. Weil f irreduzibel ist, ist $\langle f \rangle_{k[X]}$ ein maximales Ideal im Hauptidealring $k[X]$; deshalb ist K ein Körper. Die Aussage $[K : k] = \deg(f)$ folgt wie im Beweis von Satz 6.3. Wir schreiben den kanonischen Epimorphismus $\phi\colon k[X] \to K$ als $h \mapsto [h]$. Sei $a = [X]$ das Bild von X in K, dann gilt $f(a) = f([X]) = f(\phi(X)) = \phi(f) = [f] = [0]$, also hat f in K eine Nullstelle. ❑

Man sieht hieran die Mächtigkeit algebraischer Konstruktionen, die es einem erlaubt, sich algebraische Strukturen fast „nach Wunsch“ zu basteln.

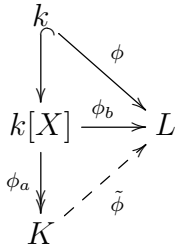
Für den Vergleich von Körpererweiterungen, in denen ein gegebenes irreduzibles Polynom eine Nullstelle hat, ist folgende Aussage nützlich.

SATZ Fortsetzung von Homomorphismen

7.2. **Satz.** *Sei k ein Körper und sei $f \in k[X]$ normiert und irreduzibel. Seien $k \subset K$ eine Körpererweiterung und $a \in K$ mit $f(a) = 0$ und $K = k(a)$ (zum Beispiel wie in Satz 7.1 mit $a = [X]$). Sei L ein weiterer Körper, $\phi\colon k \to L$ ein Homomorphismus und $b \in L$ eine Nullstelle von $\tilde{f}$, wobei $\tilde{f} \in L[X]$ durch Anwendung von ϕ auf die Koeffizienten von f entsteht. Dann gibt es einen eindeutig bestimmten Homomorphismus $\tilde{\phi}\colon K \to L$ mit $\tilde{\phi}|_k = \phi$ und $\tilde{\phi}(a) = b$.*

Insbesondere gibt es genau $\#\{b \in L \mid \tilde{f}(b) = 0\}$ Homomorphismen $\tilde{\phi}\colon K \to L$ mit $\tilde{\phi}|_k = \phi$.

Beweis. Der durch $X \mapsto a \in K$ gegebene Einsetzungshomomorphismus ϕ_a ist surjektiv. Wir betrachten folgendes Diagramm:



Nach der universellen Eigenschaft des Polynomrings gibt es genau einen Ringhomomorphismus $\phi_b\colon k[X] \to L$ mit $\phi_b|_k = \phi$ und $\phi_b(X) = b$. Da $\phi_b(f) = \tilde{f}(b) = 0$ ist, gilt $\ker(\phi_b) \supset \langle f \rangle_{k[X]}$. Also induziert ϕ_b einen eindeutig bestimmten Homomorphismus $\tilde{\phi}$ mit den gewünschten Eigenschaften.

Für jedes solche $\tilde{\phi}$ muss gelten $\tilde{f}\big(\tilde{\phi}(a)\big) = \tilde{\phi}\big(f(a)\big) = \tilde{\phi}(0) = 0$, a muss also auf eine Nullstelle von $\tilde{f}$ in L abgebildet werden. Nach dem bereits Bewiesenen gibt es zu jeder solchen Nullstelle genau ein passendes $\tilde{\phi}$. ❑

BSP isomorphe Körpererweiterungen

7.3. **Beispiel.** Man kann zum Beispiel mit diesem Ergebnis leicht sehen, dass $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}(\omega\sqrt[3]{2})$ mit $\omega = e^{2\pi i/3}$ isomorph sind (obwohl der erste Körper in $\mathbb{R}$ enthalten ist und der zweite nicht). Dazu wenden wir Satz 7.2 an mit $k = \mathbb{Q}$, $f = X^3 - 2$, $K = \mathbb{Q}(\sqrt[3]{2})$, $a = \sqrt[3]{2}$, $L = \mathbb{Q}(\omega\sqrt[3]{2})$, $b = \omega\sqrt[3]{2}$ und $\phi\colon \mathbb{Q} \hookrightarrow \mathbb{Q}(\omega\sqrt[3]{2})$. Da ϕ auf $\mathbb{Q}$ die Identität ist, ist hier $\tilde{f} = f$. Wir erhalten einen Homomorphismus $\tilde{\phi}\colon \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\omega\sqrt[3]{2})$. Da $\tilde{\phi}$ eine injektive $\mathbb{Q}$-lineare Abbildung zwischen $\mathbb{Q}$-Vektorräumen gleicher endlicher Dimension (hier 3) ist, muss $\tilde{\phi}$ auch bijektiv und damit ein Isomorphismus sein. ♣

Durch Iteration der Konstruktion von Satz 7.1 können wir erreichen, dass ein gegebenes Polynom in Linearfaktoren zerfällt.

DEF Zerfällungskörper

* 7.4. **Definition.** Seien k ein Körper und $f \in k[X]$ ein normiertes Polynom. Ist $k \subset K$ eine Körpererweiterung, sodass f in $K[X]$ in Linearfaktoren zerfällt und K über k von den Nullstellen von f erzeugt wird, dann heißt K ein *Zerfällungskörper* von f über k. ♢

SATZ Existenz und Eindeutigkeit des Zerfällungskörpers

7.5. **Satz.** *Seien k ein Körper und $f \in k[X]$ ein normiertes Polynom. Dann gibt es einen Zerfällungskörper K von f über k. Es gilt $[K : k] \leq \deg(f)!$.*

Ist K' ein weiterer Zerfällungskörper von f über k, dann gibt es einen Isomorphismus $\psi\colon K \to K'$ mit $\psi|_k = \mathrm{id}_k$.

Wegen der Eindeutigkeit bis auf Isomorphie spricht man auch gerne von „dem“ Zerfällungskörper von f über k.

Beweis. Der Existenzbeweis geht durch Induktion über den Grad n von f (jeweils gleichzeitig für alle Körper k). Im Fall $n = 0$ ist nichts zu zeigen, denn $K = k$ ist der einzige Zerfällungskörper. Sei also $n > 0$. Wir schreiben $f = gh$ mit einem normierten irreduziblen Polynom $g \in k[X]$. Nach Satz 7.1 gibt es eine Körpererweiterung $k \subset k' = k(a)$, sodass wir in $k'[X]$ die Zerlegung $g = (X - a)g_1$ haben. Das Polynom $f_1 = g_1 h \in k'[X]$ hat Grad $n-1$. Nach Induktionsannahme gibt es einen Zerfällungskörper K von f_1 über k'. Dann ist K auch ein Zerfällungskörper von f über k, denn die Nullstellen von f, nämlich a und die Nullstellen von f_1, liegen alle in K, und K wird über $k' = k(a)$ von den Nullstellen von f_1 erzeugt, also wird K über k von den Nullstellen von f erzeugt. Ebenfalls nach Induktionsannahme haben wir $[K : k'] \leq (n-1)!$, also $[K : k] = [K : k'] \cdot [k' : k] \leq (n-1)! \cdot n = n!$.

Zur Eindeutigkeit: Seien K und K' zwei Zerfällungskörper von f über k. Wir zeigen, dass es einen Homomorphismus $\psi\colon K \to K'$ gibt mit $\psi|_k = \mathrm{id}_k$. Dann folgt ebenso, dass es einen Homomorphismus $\psi'\colon K' \to K$ gibt mit $\psi'|_k = \mathrm{id}_k$. Als Homomorphismen zwischen Körpern sind ψ und ψ' injektiv. Also sind auch die Kompositionen $\psi' \circ \psi\colon K \to K$ und $\psi \circ \psi'\colon K' \to K'$ injektiv und k-linear. Da K und K' endlich-dimensionale k-Vektorräume sind, sind sowohl $\psi' \circ \psi$ als auch $\psi \circ \psi'$ bijektiv. Dann muss ψ ein Isomorphismus sein.

Der Homomorphismus ψ wird schrittweise konstruiert. Sei ψ schon auf dem Zwischenkörper L von $k \subset K$ definiert (zu Beginn ist $L = k$); wir haben also

$\psi_L\colon L \to K'$ mit $\psi_L|_k = \mathrm{id}_k$. Wir faktorisieren f in $L[X]$ in normierte irreduzible Faktoren. Sind diese alle linear, dann muss $L = K$ sein, und wir sind fertig. Anderenfalls sei h ein irreduzibler Faktor vom Grad ≥ 2. Sei $\tilde{h} \in K'[X]$ das Polynom, das durch Anwendung von ϕ_L auf die Koeffizienten von h entsteht. Sei a eine Nullstelle von h in K und b eine Nullstelle von $\tilde{h}$ in K', und sei $L' = L(a)$. Dann gibt es nach Satz 7.2 eine (eindeutig bestimmte) Fortsetzung $\psi_{L'}\colon L' \to K'$ von ψ_L mit $\psi_{L'}(a) = b$. Da $L' \neq L$, gilt $[L' : k] > [L : k]$. Weil $[K : k]$ endlich ist, müssen wir nach endlich vielen Schritten $L = K$ erreichen. ❑

Man kann sich vorstellen, dass man durch „unendliche Iteration“ der Konstruktion von Zerfällungskörpern einen algebraischen Abschluss von k erzeugen kann. Die technischen Details dieser Konstruktion sind allerdings recht kompliziert.

Aus der zweiten Aussage in Satz 7.2 folgt im Fall, dass f keine mehrfachen Nullstellen (in K') hat, dass es genau $[K : k] = [K' : k]$ Isomorphismen $\psi\colon K \to K'$ mit $\psi|_k = \mathrm{id}_k$ gibt. (Im Beweis oben gibt es beim Schritt von L zu L' genau $[L' : L]$ Möglichkeiten, den Homomorphismus fortzusetzen; die Behauptung folgt durch Induktion.) Man kann das auf $K' = K$ anwenden und erhält die Aussage, dass die Körpererweiterung $k \subset K$ genau $[K : k]$ Automorphismen hat (das sind Körperautomorphismen von K, die auf k die Identität induzieren). Das ist die maximal mögliche Anzahl. Körpererweiterungen mit der Eigenschaft, dass sie diese Maximalzahl an Automorphismen haben, heißen *Galois-Erweiterungen*; wir werden sie noch genauer studieren.

7.6. **Beispiele.**

BSP Zerfällungskörper

DEF Kreisteilungs-Körper

(1) Ein Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ ist $\mathbb{Q}(\zeta_n) \subset \mathbb{C}$ mit $\zeta_n = e^{2\pi i/n}$. Denn die Nullstellen von $X^n - 1$ sind ζ_n^j mit $j = 0, 1, \ldots, n-1$; sie liegen also alle in $\mathbb{Q}(\zeta_n)$. Auf der anderen Seite wird $\mathbb{Q}(\zeta_n)$ von den Nullstellen (sogar schon von einer Nullstelle) erzeugt. Der Körper $\mathbb{Q}(\zeta_n)$ heißt der *n-te Kreisteilungskörper* (weil die Nullstellen von $X^n - 1$ den Einheitskreis in $\mathbb{C}$ in n gleiche Teile teilen).

(2) Ein Zerfällungskörper von $X^5 - 7$ über $\mathbb{Q}$ ist $K = \mathbb{Q}(\sqrt[5]{7}, \zeta_5)$. Die Nullstellen sind von der Form $\alpha_j = \zeta_5^j \sqrt[5]{7}$ für $j = 0, 1, 2, 3, 4$; sie sind also alle in K enthalten. Da K wegen $\zeta_5 = \alpha_1/\alpha_0$ von den Nullstellen erzeugt wird, ist K ein Zerfällungskörper.

(3) Allgemeiner gilt: Ist $k \subset \bar{k}$ mit $\bar{k}$ algebraisch abgeschlossen und ist $f \in k[X]$ normiert, dann ist $K = k(\{\alpha \in \bar{k} \mid f(\alpha) = 0\}) \subset \bar{k}$ ein Zerfällungskörper von f über k. Denn da (nach Definition von „algebraisch abgeschlossen“) f über $\bar{k}$ in Linearfaktoren zerfällt, gilt dies auch über K (jeder Linearfaktor hat die Form $X - \alpha$ mit einer Nullstelle α von f in $\bar{k}$), und K wird offensichtlich von den Nullstellen von f über k erzeugt. ♣

8. Endliche Körper

Wir wollen uns jetzt etwas ausführlicher mit endlichen Körpern beschäftigen. Endliche Körper sind einerseits innerhalb der Mathematik wichtige Objekte, spielen andererseits aber auch für Anwendungen etwa in der Codierungstheorie und der Kryptographie eine große Rolle.

Wir wiederholen erst einmal kurz, was wir bereits über endliche Körper wissen.

8.1. **Erinnerung.** *Sei F ein endlicher Körper.*

(1) *Für jede Primzahl p ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen.*

(2) $\mathrm{char}(F) = p$ *ist eine Primzahl und F enthält (eine Kopie von) $\mathbb{F}_p$ (Lemma 5.7).*

(3) $\#F = p^e$ *mit $e \geq 1$ (Beispiel 5.9).*

(4) *In F gilt $(x+y)^p = x^p + y^p$ („Freshman's Dream"[1]) (und natürlich auch $(xy)^p = x^p y^p$).*

(5) *Die multiplikative Gruppe $F^\times$ von F ist zyklisch (Satz 4.9).*

F.G. Frobenius
1849–1915

Die vorletzte Aussage gilt für jeden Körper F mit $\mathrm{char}(F) = p$. Sie ergibt sich wie folgt: Es ist nach dem Binomialsatz

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \ldots + \binom{p}{p-1}xy^{p-1} + y^p\,,$$

und die Binomialkoeffizienten $\binom{p}{m} = \frac{p!}{m!(p-m)!}$ sind für $0 < m < p$ durch p teilbar (denn p teilt den Zähler $p!$, aber nicht den Nenner $m!(p-m)!$). In einem Körper der Charakteristik p ist $p \cdot a = 0$ für alle a, also verschwinden oben alle Terme außer x^p und y^p.

Das legt folgende Definition nahe:

8.2. **Definition.** Sei F ein Körper der Charakteristik $p > 0$. Dann ist die Abbildung $\phi_F \colon F \to F$, $x \mapsto x^p$, ein Endomorphismus von F; ϕ_F heißt der *Frobenius-Endomorphismus* von F. Ist F endlich, dann ist ϕ_F ein Automorphismus von F und heißt der *Frobenius-Automorphismus* von F. ♢

DEF Frobenius-Automorphismus

Dass ϕ_F ein Ringhomomorphismus ist, folgt aus Aussage (4) in 8.1. Als Homomorphismus zwischen Körpern ist ϕ_F injektiv. Ist F endlich, dann muss $\phi_F \colon F \to F$ sogar bijektiv sein.

Wir bezeichnen die Iterierten von ϕ_F mit ϕ_F^n, also $\phi_F^0 = \mathrm{id}_F$ und $\phi_F^{n+1} = \phi_F^n \circ \phi_F$.

8.3. **Lemma.** *Sei F ein endlicher Körper der Charakteristik p, $\#F = p^e$. Dann ist $\phi_F^e = \mathrm{id}_F$, und für jeden Teiler f von e ist die Teilmenge*

$$K_f = \{x \in F \mid \phi_F^f(x) = x\} \subset F$$

ein Teilkörper von F mit p^f Elementen. Jeder Teilkörper von F hat die Form K_f für einen Teiler f von e.

LEMMA Teilkörper endlicher Körper

[1] Freshman = Studienanfänger

Beweis. Die multiplikative Gruppe $F^\times$ von F hat $p^e - 1$ Elemente, also gilt für alle $x \in F^\times$, dass $x^{p^e-1} = 1$ ist. Daraus folgt $x^{p^e} = x$, also $\phi_F^e(x) = \mathrm{id}_F(x)$ für alle $x \in F$. (Vergleiche den kleinen Satz von Fermat, das ist der Spezialfall $F = \mathbb{F}_p$.)

Sei jetzt f ein Teiler von e. Dann ist K_f ein Teilkörper von F — das gilt für die Menge der Fixpunkte jedes Körperautomorphismus (Übung). Die Elemente von K_f sind genau die Nullstellen von $X^{p^f} - X$. Es gilt $p^f - 1 \mid p^e - 1$ (denn mit $e = fg$ ist $p^e - 1 = (p^f)^g - 1 \equiv 1^g - 1 = 0 \bmod p^f - 1$); daraus folgt $X^{p^f-1}-1 \mid X^{p^e-1}-1$, also ist auch $X^{p^f}-X$ ein Teiler von $X^{p^e}-X$ im Polynomring $F[X]$. Da $X^{p^e} - X$ p^e verschiedene Nullstellen in F hat, muss auch $X^{p^f} - X$ p^f verschiedene Nullstellen in F haben, also ist $\#K_f = p^f$.

Sei schließlich $K \subset F$ ein Teilkörper. Dann gilt $\#K = p^f$ mit geeignetem f; wegen $f \cdot [F : K] = e$ muss f ein Teiler von e sein. Die erste Aussage dieses Lemmas zeigt dann, dass $\phi_K^f = \phi_F^f|_K$ die Identität von K ist. Das bedeutet $K \subset K_f$, und weil beide Seiten die gleiche Anzahl von Elementen haben, muss $K = K_f$ gelten. ❑

Wir haben uns jetzt zwar schon einmal einen Überblick über die Teilkörper eines endlichen Körpers verschafft, aber wir wissen immer noch nicht, ob es auch zu jeder Primzahlpotenz p^e einen endlichen Körper mit p^e Elementen gibt. (Aus dem eben bewiesenen Lemma folgt nur, dass mit dem Exponenten e auch jeder Teiler von e vorkommen muss.) Um diese Frage zu beantworten, verwenden wir die Existenz von Zerfällungskörpern und lassen uns von der Beschreibung der Teilkörper in Lemma 8.3 inspirieren.

SATZ Existenz von Erweiterungen endlicher Körper

8.4. **Satz.** *Sei F ein endlicher Körper mit $\#F = q = p^e$ und sei $n \geq 1$. Dann gibt es eine Körpererweiterung $F \subset F'$ mit $[F' : F] = n$. Jeder solche Körper ist ein Zerfällungskörper von $X^{q^n} - X$ über F; insbesondere sind alle solche Körpererweiterungen von F isomorph (d.h., es gibt einen Isomorphismus, der auf F die Identität ist).*

Beweis. Ist $F \subset F'$ eine beliebige Körpererweiterung mit $[F' : F] = n$, dann ist $\phi_{F'}^{en} = \mathrm{id}_{F'}$ nach Lemma 8.3, also sind die Elemente von F' genau die Nullstellen von $f = X^{q^n} - X = X^{p^{en}} - X$. Insbesondere ist F' ein Zerfällungskörper von f über F. Die Eindeutigkeitsaussage folgt aus Satz 7.5.

Sei F' ein Zerfällungskörper von f über F; so ein F' existiert nach Satz 7.5. Dann ist F' von endlichem Grad über F, also ebenfalls endlich. Die Menge der Fixpunkte von $\phi_{F'}^{en}$ bildet einen Teilkörper F'' von F'. Diese Fixpunkte sind gerade die Nullstellen von f in F', wovon es genau q^n gibt (denn f hat wegen $f' = -1$ keine mehrfachen Nullstellen). Es folgt $F'' = F'$ und $[F' : F] = n$. ❑

* **FOLG** Existenz endlicher Körper

8.5. **Folgerung.** *Seien p eine Primzahl und $e \geq 1$. Dann gibt es Körper F mit $\#F = p^e$. Jeder solche Körper ist ein Zerfällungskörper von $X^{p^e} - X$ über $\mathbb{F}_p$; insbesondere sind alle Körper mit p^e Elementen isomorph.*

Beweis. Wir wenden Satz 8.4 auf $F = \mathbb{F}_p$ an. ❑

Man schreibt daher gerne $\mathbb{F}_q$ für „den“ Körper mit $q = p^e$ Elementen.

LEMMA Erweiterungen endlicher Körper sind einfach

8.6. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung mit K endlich. Dann ist diese Erweiterung einfach (d.h., es gibt $\alpha \in K$ mit $K = k(\alpha)$).*

Beweis. Die Gruppe $K^\times$ ist zyklisch; sei $\alpha \in K^\times$ ein Erzeuger. Dann ist $K = k(\alpha)$, denn $K = \{0\} \cup \{\alpha^n \mid 0 \le n < \#K - 1\}$. ❑

Aus Satz 8.4 und Lemma 8.6 können wir nun Schlüsse über die Existenz von irreduziblen Polynomen vorgegebenen Grades über einem endlichen Körper ziehen.

SATZ Existenz irreduzibler Polynome

8.7. **Satz.** *Seien F ein endlicher Körper und $n \ge 1$. Dann gibt es mindestens ein normiertes irreduzibles Polynom $f \in F[X]$ vom Grad n.*

Beweis. Sei $q = \#F = p^e$. Nach Satz 8.4 gibt es eine Körpererweiterung F' von F vom Grad n. Nach Lemma 8.6 ist F' eine einfache Erweiterung von F. Sei $\alpha \in F'$ ein primitives Element (also $F' = F(\alpha)$) und sei $f \in F[X]$ das Minimalpolynom von α. Dann gilt $\deg(f) = [F(\alpha) : F] = [F' : F] = n$ und f ist irreduzibel und normiert. ❑

Für $F = \mathbb{F}_2$ und $n = 2$ gibt es tatsächlich nur ein (normiertes) irreduzibles Polynom vom Grad n, nämlich $X^2 + X + 1$. Im Allgemeinen gibt es jedoch mehr. Wir wollen im Rest dieses Abschnitts eine Formel für ihre Anzahl herleiten.

Dazu beweisen wir erst noch zwei vorbereitende Aussagen.

LEMMA irred. Polynom vom Grad n zerfällt in Erweiterung vom Grad n

8.8. **Lemma.** *Seien F ein endlicher Körper, $q = p^e = \#F$ und $f \in F[X]$ normiert und irreduzibel mit $\deg(f) = n$. Sei F' eine Körpererweiterung von F vom Grad n. Dann hat f in F' eine Nullstelle α und in $F'[X]$ gilt*

$$f = (X - \alpha)(X - \alpha^q)(X - \alpha^{q^2}) \cdots (X - \alpha^{q^{n-1}}) .$$

Insbesondere ist F' ein Zerfällungskörper von f über F.

Beweis. Nach Satz 7.1 gibt es eine Körpererweiterung F'' von F vom Grad n, in der f eine Nullstelle hat. Nach Satz 8.4 sind F' und F'' isomorph als Körpererweiterungen von F. Es folgt, dass f in F' eine Nullstelle α hat. Sei jetzt $\beta \in F'$ irgendeine Nullstelle von f. Dann gilt

$$0 = \phi^e_{F'}(0) = \phi^e_{F'}\big(f(\beta)\big) = f\big(\phi^e_{F'}(\beta)\big) = f(\beta^q) ,$$

denn $\phi^e_{F'}$ ist nach Lemma 8.3 auf F, also auf den Koeffizienten von f, die Identität. Also ist auch β^q eine Nullstelle von f. Induktiv erhalten wir also, dass alle α^{q^m} für $m = 0, 1, 2, \ldots$ Nullstellen von f sind.

Da $\phi^e_{F'} \colon x \mapsto x^q$ bijektiv und F' endlich ist, muss die Folge $(\alpha, \alpha^q, \alpha^{q^2}, \ldots)$ von Beginn an periodisch sein. Da $\phi^{en}_{F'}$ nach Lemma 8.3 die Identität auf F' ist, ist die (minimale) Periode ein Teiler von n. Wäre sie ein echter Teiler m von n, dann wäre α in der Fixpunktmenge von $\phi^{em}_{F'}$ enthalten, also in einer Körpererweiterung vom Grad m von F. Das wäre aber ein Widerspruch dazu, dass das Minimalpolynom von α Grad n hat, vergleiche Folgerung 6.5. Also ist die Periode genau n; damit sind die ersten n Glieder der Folge paarweise verschieden. Da diese n Elemente allesamt Nullstellen von f sind, müssen es alle Nullstellen von f sein, und die behauptete Faktorisierung folgt. Da $F' = F(\alpha)$ von den Nullstellen von f erzeugt wird, ist F' ein Zerfällungskörper von f über F. ❑

LEMMA Faktorisierung von $X^{q^n} - X$

8.9. **Lemma.** *Seien F ein endlicher Körper, $q = \#F$ und $n \geq 1$. Dann gilt*

$$X^{q^n} - X = \prod_f f$$

in $F[X]$, wobei das Produkt über alle normierten irreduziblen Polynome $f \in F[X]$ mit $\deg(f) \mid n$ läuft.

Beweis. Wir haben bereits gesehen, dass $h = X^{q^n} - X$ insgesamt q^n verschiedene Nullstellen in F' hat, wobei F' der Zerfällungskörper von h über F ist. Außerdem gilt $[F' : F] = n$. Da alle Elemente von F' Nullstellen von h sind, gilt in $F'[X]$ die Faktorisierung

$$h = X^{q^n} - X = \prod_{\alpha \in F'} (X - \alpha)\,.$$

Sei $\alpha \in F'$. Dann ist $[F(\alpha) : F]$ ein Teiler von n, also ist der Grad des Minimalpolynoms f von α ein Teiler von n. Damit ist f ein Faktor im Produkt auf der rechten Seite. Dieses Argument zeigt, dass jede Nullstelle von h auch Nullstelle des Produkts ist, also teilt h das Produkt. Sei jetzt umgekehrt $f \in F[X]$ ein normiertes irreduzibles Polynom mit $m = \deg(f) \mid n$. Es gibt einen Zwischenkörper $F \subset K \subset F'$ mit $[K : F] = m$. Nach Lemma 8.8 ist K ein Zerfällungskörper von f über F, also zerfällt f auch über F' in (paarweise verschiedene) Linearfaktoren. Das zeigt, dass f ein Teiler von h ist. Da verschiedene normierte irreduzible Polynome paarweise teilerfremd sind, folgt, dass das Produkt auf der rechten Seite ein Teiler von h ist. Da beide Seiten normiert sind und sich gegenseitig teilen, müssen sie gleich sein. ❑

Aus dieser Faktorisierung können wir nun leicht folgende Rekursion herleiten.

SATZ Anzahl irreduzibler Polynome

8.10. **Satz.** *Sei F ein endlicher Körper mit $\#F = q$. Wir schreiben $a_n(q)$ für die Anzahl der normierten irreduziblen Polynome vom Grad n in $F[X]$. Dann gilt für alle $n \geq 1$*

$$\sum_{d \mid n} d a_d(q) = q^n\,.$$

Beweis. Die linke Seite ergibt den Grad des Produkts auf der rechten Seite der Formel in Lemma 8.9, die rechte Seite ist der Grad des Polynoms $X^{q^n} - X$ auf der linken Seite. ❑

BSP Anzahlen irreduzibler Polynome

8.11. **Beispiele.** Für kleine Grade n erhalten wir:

$$\begin{aligned}
a_1(q) &= q \\
a_2(q) &= \frac{q^2 - a_1(q)}{2} = \tfrac{1}{2}(q^2 - q) \\
a_3(q) &= \frac{q^3 - a_1(q)}{3} = \tfrac{1}{3}(q^3 - q) \\
a_4(q) &= \frac{q^4 - 2a_2(q) - a_1(q)}{4} = \tfrac{1}{4}(q^4 - q^2)
\end{aligned}$$

Für $q = 2$ haben wir also $a_1(2) = 2$, $a_2(2) = 1$, $a_3(2) = 2$, $a_4(2) = 3$, vergleiche die Tabelle von irreduziblen Polynomen über $\mathbb{F}_2$ in EZAS.10.10. ♣

Es gibt eine allgemeine Formel für $a_n(q)$. Dafür brauchen wir noch eine Definition und ein Lemma.

8.12. **Definition.** Die *Möbiusfunktion* $\mu\colon \mathbb{Z}_{>0} \to \{-1,0,1\}$ ist definiert durch **DEF** Möbius-funktion

$$\mu(n) = \begin{cases} (-1)^m & \text{falls } n = p_1 p_2 \cdots p_m \text{ mit paarweise verschiedenen Primzahlen } p_j, \\ 0 & \text{falls } n \text{ nicht quadratfrei.} \end{cases} \qquad \diamondsuit$$

Hier ist eine kleine Tabelle:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0	−1	1	1	0

Aus der Definition ergibt sich, dass aus $m \perp n$ die Beziehung $\mu(mn) = \mu(m)\mu(n)$ folgt.

8.13. **Lemma.** *Sei R ein Ring und seien $(a_n)_{n\geq 1}$ und $(b_n)_{n\geq 1}$ zwei Folgen von Elementen von R. Dann gilt* **LEMMA** Möbius-Inversion

$$\forall n \geq 1\colon \sum_{d|n} a_d = b_n \iff \forall n \geq 1\colon \sum_{d|n} \mu\big(\frac{n}{d}\big) b_d = a_n\,.$$

Beweis. Wir zeigen zunächst

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n > 1. \end{cases}$$

Der Fall $n = 1$ ist klar. Seien also $n > 1$ und p ein Primteiler von n; sei $n = mp^e$ mit $p \nmid m$. Dann sind die Teiler von n gegeben durch $d = lp^f$ mit $l \mid m$ und $0 \leq f \leq e$, und wir haben

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{l|m} \sum_{f=0}^{e} \mu(lp^f) = \sum_{l|m} \sum_{f=0}^{e} \mu(l)\mu(p^f) \\ &= \Big(\sum_{l|m} \mu(l)\Big)\Big(\sum_{f=0}^{e} \mu(p^f)\Big) = \Big(\sum_{l|m} \mu(l)\Big)(1-1) = 0\,. \end{aligned}$$

Für die Implikation „⇒“ setzen wir die Definition von b_n ein:

$$\begin{aligned} \sum_{d|n} \mu\big(\frac{n}{d}\big) b_d &= \sum_{d|n} \mu\big(\frac{n}{d}\big) \sum_{l|d} a_l = \sum_{l|n} a_l \sum_{d\colon l|d|n} \mu\big(\frac{n}{d}\big) \\ &= \sum_{l|n} a_l \sum_{m|\frac{n}{l}} \mu(m) = a_n \end{aligned}$$

(wir benutzen, dass die n/d genau die Teiler von n/l durchlaufen). Der Beweis von „⇐“ ist ähnlich. ❑

8.14. **Folgerung.** *Es gilt* **FOLG** Formel für $a_n(q)$

$$a_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}\,.$$

Beweis. Anwendung von Lemma 8.13 auf $a_n := n a_n(q)$ und $b_n := q^n$. ❑

Zum Beispiel gilt

$$a_6(q) = \tfrac{1}{6}(q^6 - q^3 - q^2 + q)\,.$$

Es gibt also genau $a_6(2) = 9$ verschiedene irreduzible Polynome vom Grad 6 über $\mathbb{F}_2$. (Über $\mathbb{F}_2$ ist jedes Polynom $\neq 0$ normiert.)

9. Konstruktionen mit Zirkel und Lineal

In diesem Abschnitt werden wir sehen, dass sich die Theorie der Körpererweiterungen auf ein geometrisches Problem anwenden lässt; man kann sie nämlich dazu benutzen, um zu entscheiden, ob gewisse Konstruktionen mit Zirkel und Lineal möglich sind oder nicht.

Dazu erinnern wir uns daran, was bei einer „Konstruktion mit Zirkel und Lineal“ erlaubt ist. Wir beginnen mit einer Menge S gegebener Punkte in der Ebene. Wir können dann schrittweise weitere Punkte und dazu Geraden und Kreise konstruieren:

- Die Gerade durch zwei (verschiedene) bereits konstruierte Punkte.
- Der Kreis um einen bereits konstruierten Punkt mit Radius gleich dem Abstand zweier bereits konstruierter Punkte.
- Die Schnittpunkte von zwei bereits konstruierten Geraden oder Kreisen.

Als ersten Schritt zur „Algebraisierung“ führen wir (kartesische) Koordinaten der Ebene ein. Wenn wir davon ausgehen, dass wir mit mindestens zwei gegebenen Punkten starten, können wir die Koordinaten so wählen, dass einer der Punkte der Ursprung und ein anderer der Punkt $(1,0)$ auf der x-Achse ist, dass also S die Punkte $(0,0)$ und $(1,0)$ enthält.

Wir überlegen jetzt, wie sich die Konstruktion von Punkten algebraisch niederschlägt. Eine erste Beobachtung ist, dass sich ein Punkt (x,y) genau dann ausgehend von S konstruieren lässt, wenn das für die Punkte $(x,0)$ und $(y,0)$ gilt. Wir können also ohne Einschränkung annehmen, dass $S = S' \times \{0\}$ ist mit einer Teilmenge $S' \subset \mathbb{R}$ (bestehend aus den x- und y-Koordinaten der Punkte aus S). Im Folgenden schreiben wir der Einfachheit halber S für die Menge S'.

* 9.1. **Definition.** Wir nennen eine reelle Zahl α *konstruierbar aus* $S \subset \mathbb{R}$, wenn sich $(\alpha, 0)$ ausgehend von $S \times \{0\}$ konstruieren lässt. Wir sagen, α sei *konstruierbar*, wenn α aus $\{0,1\}$ konstruierbar ist. ♢

DEF konstruierbar

9.2. **Lemma.** *Sei $\alpha \in \mathbb{R}$ aus $S \subset \mathbb{R}$ (mit $0,1 \in S$) konstruierbar. Dann kann α als Ausdruck in den Elementen von S geschrieben werden, der nur die vier Grundrechenarten und Quadratwurzeln enthält.*

LEMMA notwendige Bedingung für Konstruierbarkeit

Formaler ausgedrückt: Es gibt einen Körperturm

$$\mathbb{Q}(S) = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset \mathbb{R}$$

mit $\alpha \in K_n$ und $[K_m : K_{m-1}] = 2$ für alle $m = 1, \ldots, n$. Insbesondere ist α algebraisch über $\mathbb{Q}(S)$ und $[\mathbb{Q}(S,\alpha) : \mathbb{Q}(S)]$ ist eine Zweierpotenz.

Die Umkehrung der letzten Aussage gilt nicht: Daraus, dass $[\mathbb{Q}(S,\alpha) : \mathbb{Q}(S)]$ eine Zweierpotenz ist, folgt im Allgemeinen nicht, dass α aus S konstruierbar ist.

Beweis. Wir müssen zeigen, dass die Koordinaten der Schnittpunkte von Geraden und/oder Kreisen, die durch bereits konstruierte Punkte P_j definiert sind, sich in der geforderten Weise durch die Koordinaten (x_j, y_j) der P_j ausdrücken lassen. Die Aussage folgt dann durch Induktion über die Anzahl der Konstruktionsschritte. Wir müssen drei Fälle betrachten:

(1) Schnitt zweier Geraden. Die Geraden seien die Geraden durch die Punkte P_1 und P_2 und durch die Punkte P_3 und P_4. Ein Punkt $P = (x, y)$ liegt genau dann auf der Geraden durch P_1 und P_2, wenn

$$\det \begin{pmatrix} x_1 & x_2 & x \\ y_1 & y_2 & y \\ 1 & 1 & 1 \end{pmatrix} = 0\,,$$

und analog für die Gerade durch P_3 und P_4. Dies ergibt ein lineares Gleichungssystem für x und y, dessen (eindeutige, denn die Geraden sind verschieden) Lösung durch rationale Ausdrücke in den Koeffizienten gegeben ist. Diese Koeffizienten sind wiederum Polynome in den x_j und y_j. Somit sind die Koordinaten des Schnittpunkts mittels der vier Grundrechenarten aus den Koordinaten der P_j zu berechnen.

(2) Schnitt von Gerade und Kreis. Die Gerade sei durch P_1 und P_2 gegeben, der Kreis habe Mittelpunkt P_3 und Radius $|P_4P_5|$. Wir erhalten das folgende Gleichungssystem:

$$\begin{aligned}(y_1 - y_2)x - (x_1 - x_2)y + x_1y_2 - x_2y_1 &= 0\\ (x - x_3)^2 + (y - y_3)^2 - (x_4 - x_5)^2 - (y_4 - y_5)^2 &= 0\end{aligned}$$

Es hat die Form

$$ax + by + c = x^2 + y^2 + dx + ey + f = 0\,,$$

wobei a, b, c, d, e, f rationale Ausdrücke in den Koordinaten der P_j sind. Wir können die erste Gleichung nach x oder y auflösen (denn a und b können nicht beide null sein) und dann in die zweite einsetzen. Das liefert eine quadratische Gleichung in y oder x, deren Lösungen (soweit existent) sich nach der bekannten Lösungsformel für quadratische Gleichungen durch rationale Ausdrücke und das Ziehen einer (reellen) Quadratwurzel erhalten lassen.

(3) Schnitt zweier Kreise. Wir erhalten zwei Gleichungen der Form

$$x^2 + y^2 + ax + by + c = x^2 + y^2 + a'x + b'y + c' = 0\,.$$

Wir können annehmen, dass die Kreise nicht konzentrisch sind (sonst gibt es keinen Schnittpunkt oder die Kreise sind identisch); das bedeutet $(a, b) \neq (a', b')$. Durch Subtraktion erhalten wir die *lineare* Gleichung

$$(a - a')x + (b - b')y + c - c' = 0\,.$$

(Sie beschreibt die Gerade durch die beiden Schnittpunkte der Kreise.) Den resultierenden Fall (eine lineare und eine quadratische Gleichung) haben wir aber bereits behandelt.

Sei K der von den bisher konstruierten Zahlen erzeugte Teilkörper von $\mathbb{R}$. Zu Beginn der Konstruktion ist $K = \mathbb{Q}(S)$. Rationale Operationen ergeben wieder Elemente von K. Wenn wir eine Quadratwurzel ziehen, dann adjungieren wir eine Nullstelle von $X^2 - \beta$ für ein Element $\beta \in K$. Der resultierende Körper $K' = K(\sqrt{\beta})$ ist entweder gleich K (wenn β ein Quadrat in K ist) oder hat Grad 2 über K. So erhalten wir schrittweise den Turm von quadratischen Erweiterungen, sodass der letzte Körper das Element α enthält.

Da $\mathbb{Q}(S, \alpha) \subset K_n$ und

$$[K_n : \mathbb{Q}(S)] = [K_1 : K_0] \cdot [K_2 : K_1] \cdots [K_n : K_{n-1}] = 2^n < \infty$$

ist, folgt, dass α als Element einer endlichen Körpererweiterung von $\mathbb{Q}(S)$ über $\mathbb{Q}(S)$ algebraisch ist. Außerdem gilt $[\mathbb{Q}(S,\alpha) : \mathbb{Q}(S)] \mid [K_n : \mathbb{Q}(S)] = 2^n$, also ist der Grad von $\mathbb{Q}(S,\alpha)$ über $\mathbb{Q}(S)$ eine Zweierpotenz. ❑

Damit können wir bereits die Unlösbarkeit mehrerer klassischer Probleme zeigen.

9.3. **Folgerung.** *Die Zahl $\sqrt[3]{2}$ ist nicht konstruierbar.*

FOLG Würfelverdopplung

Beweis. $X^3-2 \in \mathbb{Q}[X]$ ist irreduzibel nach Eisenstein, also ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und damit keine Zweierpotenz. Nach Lemma 9.2 ist $\sqrt[3]{2}$ also nicht konstruierbar. ❑

Dahinter steht das sogenannte „Delische Problem“ der Würfelverdopplung. Der Name geht auf eine Legende zurück: Die Insel Delos wurde von einer Pestepidemie heimgesucht. In ihrer Verzweiflung befragten die Bewohner das Orakel von Delphi. Die Auskunft war, dass die Epidemie enden würde, wenn sie den würfelförmigen Altar im Tempel des Apollon im Volumen verdoppelten. Die antiken Mathematiker interpretierten das so, dass die Seitenlänge eines Würfels mit dem doppelten Volumen mit Zirkel und Lineal konstruiert werden sollte. Das Verhältnis der Seitenlängen ist gerade $\sqrt[3]{2}$. Besonders hilfreich kann der Orakelspruch also nicht gewesen sein...

9.4. **Definition.** Wir sagen, ein Winkel φ sei *konstruierbar*, wenn sein Cosinus (oder sein Sinus, beides ist äquivalent) konstruierbar ist. ♢

DEF konstruierbar für Winkel

Durch Errichten des Lots auf die x-Achse im Punkt $(\cos\varphi, 0)$ und Schneiden mit dem Einheitskreis kann man leicht eine Gerade durch den Ursprung konstruieren, die mit der x-Achse den Winkel φ einschließt.

Offenbar ist ein reguläres n-Eck genau dann konstruierbar, wenn der Winkel $\frac{2\pi}{n}$ konstruierbar ist.

9.5. **Folgerung.** *Der Winkel $\frac{2\pi}{9}$ (das entspricht $40°$) ist nicht konstruierbar. Also ist das reguläre Neuneck nicht konstruierbar.*

FOLG Neuneck nicht konstruierbar

Beweis. Sei $\zeta = e^{2\pi i/9} = \cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$. Dann ist ζ^3 eine primitive dritte Einheitswurzel, also gilt $\zeta^6+\zeta^3+1 = (\zeta^3)^2+\zeta^3+1 = 0$. Sei $\alpha = \zeta+\zeta^{-1} = 2\cos\frac{2\pi}{9}$. Dann gilt

$$\alpha^3 - 3\alpha + 1 = (\zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}) - 3(\zeta+\zeta^{-1}) + 1 = \zeta^{-3}(\zeta^6+\zeta^3+1) = 0\,.$$

Das Polynom $f = X^3-3X+1$ ist irreduzibel, denn es hat keine rationale Nullstelle (nur ±1 kämen in Frage). Es folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$. Nach Lemma 9.2 ist also α (und damit natürlich auch $\alpha/2 = \cos\frac{2\pi}{9}$) nicht konstruierbar. ❑

Da der Winkel $\frac{2\pi}{3}$ sehr leicht konstruierbar ist, folgt daraus auch:

9.6. **Folgerung.** *Es gibt keine allgemeine Konstruktion mit Zirkel und Lineal, die einen Winkel in drei gleiche Teile teilt.*

FOLG Unmöglichkeit der Winkeldreiteilung

Genauer heißt das: Es gilt nicht, dass für beliebige φ die Zahl $\cos\frac{\varphi}{3}$ aus $\{0, 1, \cos\varphi\}$ konstruierbar ist.

Beweis. Wegen $\cos\frac{2\pi}{3} = -\frac{1}{2}$ müsste $\cos\frac{2\pi}{9}$ (aus $\{0,1\}$) konstruierbar sein, was aber nach Folgerung 9.5 nicht der Fall ist. ❑

FOLG Konstruierbarkeit des regulären p-Ecks

9.7. **Folgerung.** *Sei p eine ungerade Primzahl. Dann ist das reguläre p-Eck höchstens dann konstruierbar, wenn p eine Fermatsche Primzahl ist: $p = 2^{2^m} + 1$ für ein $m \geq 0$.*

Beweis. Die p-te Einheitswurzel $\zeta = e^{2\pi i/p}$ ist Nullstelle von

$$f = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Q}[X]$$

und f ist irreduzibel (Eisenstein für $f(X+1)$, siehe Beispiel EZAS.10.14). Es gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos\frac{2\pi}{p})] = 2$ (siehe Beispiel 6.9). Wenn das reguläre p-Eck konstruierbar ist, dann muss $[\mathbb{Q}(\cos\frac{2\pi}{p}) : \mathbb{Q}]$ eine Zweierpotenz sein, und damit ist auch

$$p - 1 = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2\,[\mathbb{Q}(\cos\tfrac{2\pi}{p}) : \mathbb{Q}]$$

eine Zweierpotenz. p hat also die Form 2^n+1. Wenn $n = kl$ ist mit $k > 1$ ungerade, dann ist

$$2^n + 1 = (2^l)^k + 1 = (2^l + 1)((2^l)^{k-1} - (2^l)^{k-2} + \ldots - 2^l + 1)$$

keine Primzahl. Also ist $n = 2^m$ selbst eine Zweierpotenz. ❑

C.F. Gauß (1777–1855)

Zum Beispiel kann man keine regulären 7-, 11- oder 13-Ecke mit Zirkel und Lineal konstruieren. Umgekehrt kann man zeigen, dass reguläre p-Ecke für Fermatsche Primzahlen p tatsächlich konstruierbar sind (Gauß 1796). Für $p = 3$ und $p = 5$ ist das seit der Antike bekannt. Gauß fand 1796 eine Konstruktion für das reguläre 17-Eck (mit neunzehn Jahren!) — daran erinnert ein siebzehnzackiger Stern an seinem Denkmal in Braunschweig. Richelot gab 1832 eine Konstruktion des regulären 257-Ecks an. „Im Jahr 1894 fand Johann Gustav Hermes nach mehr als zehnjähriger Anstrengung eine Konstruktionsvorschrift für das regelmäßige 65 537-Eck und beschrieb diese in einem Manuskript von mehr als 200 Seiten, welches sich heute in einem speziell dafür angefertigten Koffer in der Mathematischen Bibliothek der Universität Göttingen befindet.“ (Wikipedia zum 65 537-Eck)

Weitere Fermatsche Primzahlen sind nicht bekannt. Fermat hatte einmal behauptet, alle Zahlen $2^{2^m} + 1$ seien prim. Schon Euler zeigte, dass $2^{32} + 1$ durch 641 teilbar ist. Das lässt sich wie folgt sehr schnell nachprüfen: Es ist

$$641 = 640 + 1 = 5 \cdot 2^7 + 1 \qquad \text{und} \qquad 641 = 625 + 16 = 5^4 + 2^4\,,$$

also gilt

$$2^4 \equiv -5^4 \bmod 641 \qquad \text{und} \qquad 5 \cdot 2^7 \equiv -1 \bmod 641\,.$$

Daraus folgt

$$2^{32} = 2^4 \cdot 2^{28} \equiv -5^4 \cdot 2^{28} = -(5 \cdot 2^7)^4 \equiv -(-1)^4 = -1 \bmod 641\,,$$

was gerade $641 \mid 2^{32} + 1$ bedeutet.

Wie kam Euler auf 641? Wenn p ein Primteiler von $2^{2^m} + 1$ ist, dann muss gelten $2^{2^m} \equiv -1 \bmod p$; die Ordnung der Restklasse $[2]$ in der multiplikativen Gruppe $\mathbb{F}_p^\times$ ist dann 2^{m+1}. (Denn $[2]^{2^{m+1}} = \big([2]^{2^m}\big)^2 = [-1]^2 = [1]$, also ist die Ordnung ein Teiler von 2^{m+1}. Wegen $[2]^{2^m} = [-1] \neq [1]$ ist die Ordnung kein Teiler von 2^m. Es bleibt nur 2^{m+1}.) Da die Ordnung jedes Elements die Gruppenordnung $\#\mathbb{F}_p^\times = p-1$ teilen muss, folgt $p \equiv 1 \bmod 2^{m+1}$. Im konkreten Fall ist $m = 5$, also muss ein Primteiler p die Form $p = 64k + 1$ haben. 641 ist die fünfte Primzahl dieser Form (nach 193, 257, 449 und 577).

Tatsächlich gilt noch ein wenig mehr: Für $m \geq 2$ folgt $p \equiv 1 \bmod 8$; nach dem 2. Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz ist dann 2 ein quadratischer Rest mod p. Sei $a \in \mathbb{Z}$ mit $a^2 \equiv 2 \bmod p$. Dann hat $[a]$ in $\mathbb{F}_p^\times$ die

Ordnung 2^{m+2}, da $[a]^2 = [2]$ die Ordnung 2^{m+1} hat. Es folgt $p \equiv 1 \bmod 2^{m+2}$. Für $m = 5$ ist 641 sogar die kleinste solche Primzahl.

Sei $F_m = 2^{2^m} + 1$. Man weiß, dass F_m nicht prim ist für $5 \leq m \leq 32$ (und für etliche weitere m); ob F_{33} prim ist, ist eine offene Frage (Stand 2018).

Die Unmöglichkeit eines anderen klassischen Problems zeigt die nächste Folgerung.

FOLG Quadratur des Kreises

9.8. **Folgerung.** *Die Zahl $\sqrt{\pi}$ ist nicht konstruierbar.*

Beweis. Wäre $\sqrt{\pi}$ konstruierbar, dann wäre $\sqrt{\pi}$ und damit auch π nach Lemma 9.2 algebraisch. π ist aber transzendent (Lindemann 1882). ❑

Für die „Quadratur des Kreises“ wird verlangt, zu einem Kreis mit gegebenem Radius (den wir ohne Einschränkung $= 1$ annehmen können) die Seitenlänge eines Quadrats mit demselben Flächeninhalt zu konstruieren. Diese Seitenlänge ist gerade $\sqrt{\pi}$, also ist eine Konstruktion mit Zirkel und Lineal nicht möglich.

Wenn man zeigen will, dass gewisse Konstruktionen *möglich* sind, dann braucht man eine Umkehrung von Lemma 9.2. Tatsächlich ist es so, dass die vier Grundrechenarten und das Ziehen von Quadratwurzel durch Konstruktionen mit Zirkel und Lineal ausgeführt werden können. Für Addition und Subtraktion ist das klar. Für Multiplikation und Division verwendet man den Strahlensatz: Die Parallele durch den Punkt $(b, 0)$ zur Geraden durch $(1, 0)$ und $(0, a)$ schneidet die y-Achse im Punkt $(0, ab)$. Und analog schneidet die Parallele durch den Punkt $(1, 0)$ zur Geraden durch $(0, a)$ und $(b, 0)$ die y-Achse im Punkt $(0, a/b)$. Für Quadratwurzeln konstruiert man einen Kreis mit Durchmesser $1 + x$ und trägt 1 auf dem Durchmesser ab. Das Lot in diesem Punkt trifft den Kreis im Abstand $\sqrt{x}$, wie man mit dem Satz des Pythagoras, angewandt auf die drei entstehenden rechtwinkligen Dreiecke, leicht nachrechnet. Daraus ergibt sich:

* **SATZ** Kriterium für Konstruierbarkeit

9.9. **Satz.** *Seien $S \subset \mathbb{R}$ (mit $0, 1 \in S$) und $\alpha \in \mathbb{R}$. α ist genau dann aus S konstruierbar, wenn es einen Körperturm*

$$\mathbb{Q}(S) = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset \mathbb{R}$$

gibt, sodass $\alpha \in K_n$ ist und $[K_m : K_{m-1}] = 2$ gilt für alle $m = 1, \ldots, n$.

Die Konstruierbarkeit des regulären Siebzehnecks folgt dann zum Beispiel aus der Formel von Gauß

$$-1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}$$

für $16 \cos \frac{2\pi}{17}$.

10. Separable Körpererweiterungen

In diesem Abschnitt werden wir separable Elemente und Erweiterungen einführen und untersuchen und insbesondere auch den „Satz vom primitiven Element“ beweisen. Wir orientieren uns hier an [KM, Kap. 24].

∗ 10.1. **Definition.** Seien K ein Körper und $0 \neq f \in K[X]$ ein Polynom. f heißt *separabel*, wenn für jeden irreduziblen normierten Teiler h von f gilt, dass h in einem Zerfällungskörper von h (oder f) nur einfache Nullstellen hat. ♢

DEF separables Polynom

Häufig wird einfach gefordert, dass f selbst in seinem Zerfällungskörper nur einfache Nullstellen hat, was eine stärkere Einschränkung ist. Für irreduzible Polynome stimmen beide Versionen überein, und wir werden den Begriff „separabel“ fast ausschließlich im Zusammenhang mit irreduziblen Polynomen verwenden. In diesem Fall können wir Separabilität auf einfache Weise charakterisieren.

10.2. **Lemma.** *Seien K ein Körper und $f \in K[X]$ irreduzibel. f ist genau dann separabel, wenn die Ableitung $f' \neq 0$ ist.*

LEMMA Kriterium für separabel

Beweis. Wir können ohne Einschränkung annehmen, dass f normiert ist. Sei L ein Zerfällungskörper von f über K. Ist f nicht separabel, dann hat f eine mehrfache Nullstelle α in L. Damit ist α eine Nullstelle von $f' \in K[X]$ (denn $f = (X-\alpha)^2 g$ impliziert $f' = (X-\alpha)(2g + (X-\alpha)g')$), also muss das Minimalpolynom f von α über K ein Teiler von f' sein. Auf der anderen Seite ist $\deg(f') < \deg(f)$, daher bleibt nur die Möglichkeit, dass $f' = 0$ ist. Damit ist „$\Leftarrow$“ gezeigt.

Ist umgekehrt f separabel, dann sei $\alpha \in L$ eine einfache Nullstelle von f; wir schreiben $f = (X-\alpha)g$ in $L[X]$; es ist dann $g(\alpha) \neq 0$. Dann gilt

$$f' = g + (X-\alpha)g', \qquad \text{also} \qquad f'(\alpha) = g(\alpha) \neq 0\,.$$

Das zeigt $f' \neq 0$. ❑

Aus dem Beweis ergibt sich auch, dass entweder *alle* Nullstellen von f in L einfach sind oder *keine*.

10.3. **Folgerung.** *Ist K ein Körper der Charakteristik 0, dann ist jedes irreduzible Polynom über K separabel.*

FOLG Char. 0: immer separabel

Beweis. In Charakteristik 0 gilt für f nicht konstant, dass $\deg(f') = \deg(f) - 1$ ist; es folgt $f' \neq 0$, also ist f nach Lemma 10.2 separabel. ❑

10.4. **Beispiel.** Nicht separable Polynome sind also nicht so einfach zu finden. Das Standardbeispiel sieht so aus: Sei $K = \mathbb{F}_p(y)$ der Quotientenkörper des Polynomrings $\mathbb{F}_p[y]$ und sei $f = X^p - y \in K[X]$. Nach dem Eisenstein-Kriterium (mit dem Primelement $y \in \mathbb{F}_p[y]$) ist f irreduzibel. Auf der anderen Seite ist $f' = pX^{p-1} = 0$, da K Charakteristik p hat. Also ist f nicht separabel. Sei L ein Zerfällungskörper von f über K und sei $\alpha \in L$ eine Nullstelle von f. Dann ist $\alpha^p = y$ und es gilt

BSP nicht separabel

$$(X-\alpha)^p = X^p - \alpha^p = X^p - y = f\,,$$

also hat f die p-fache Nullstelle α in L. ♣

Das lässt sich verallgemeinern:

LEMMA Separabilität in Char. p

10.5. **Lemma.** *Seien K ein Körper der Charakteristik $p > 0$ und $f \in K[X]$ irreduzibel. f ist genau dann nicht separabel, wenn es ein Polynom $g \in K[X]$ gibt mit $f = g(X^p)$.*

Beweis. Nach Lemma 10.2 genügt es, die Äquivalenz

$$f' = 0 \iff \exists g \in K[X]\colon f = g(X^p)$$

zu zeigen. Aus $f = g(X^p)$ folgt $f' = pX^{p-1}g'(X^p) = 0$. Für die Gegenrichtung sei $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. Dann ist

$$f' = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1\,.$$

Aus $f' = 0$ folgt $ma_m = 0$ für alle $0 \le m \le n$. Ist m kein Vielfaches von p, dann ist $m \neq 0$ in K, und es folgt $a_m = 0$. Also hat f die Form

$$a_{pn'}X^{pn'} + a_{p(n'-1)}X^{p(n'-1)} + \ldots + a_pX^p + a_0 = g(X^p)$$

mit

$$g = a_{pn'}X^{n'} + a_{p(n'-1)}X^{n'-1} + \ldots + a_pX + a_0\,. \qquad \square$$

Wir erweitern den Begriff „separabel“ auf Elemente und Körpererweiterungen.

DEF (in)separable Körpererweiterung

$*$ 10.6. **Definition.** Sei $k \subset K$ eine Körpererweiterung. Ein Element $a \in K$ heißt *separabel über k*, wenn es algebraisch über k ist und sein Minimalpolynom über k separabel ist. Die Körpererweiterung $k \subset K$ heißt *separabel*, wenn jedes Element $a \in K$ separabel über k ist. Anderenfalls heißt sie *inseparabel*. $\diamondsuit$

LEMMA Charakterisierung separabler Elemente

10.7. **Lemma.** *Seien $k \subset K$ eine Körpererweiterung und $a \in K$ algebraisch über k.*

(1) *Ist $\mathrm{char}(k) = 0$, dann ist a separabel über k.*

(2) *Im Fall $\mathrm{char}(k) = p > 0$ ist a genau dann separabel über k, wenn $k(a^p) = k(a)$ ist.*

(3) *a ist genau dann separabel über k, wenn die Körpererweiterung $k \subset k(a)$ separabel ist.*

Beweis. Der Fall von Charakteristik 0 folgt aus Folgerung 10.3.

Sei also $\mathrm{char}(k) = p > 0$. Wir haben den Zwischenkörper $k \subset k(a^p) \subset k(a)$. Ist a separabel über k, dann ist a auch separabel über $k(a^p)$ (denn das Minimalpolynom von a über $k(a^p)$ teilt das Minimalpolynom von a über k). Sei f das Minimalpolynom von a über $k(a^p)$, dann ist f ein Teiler von $X^p - a^p \in k(a^p)[X]$, denn a ist eine Nullstelle dieses Polynoms. Auf der anderen Seite gilt in $k(a)[X]$, dass $X^p - a^p = (X-a)^p$ ist. Da f nach Annahme keine mehrfachen Nullstellen hat, folgt $f = X - a$, also $a \in k(a^p)$ und damit $k(a) = k(a^p)$. Ist a nicht separabel über k, dann hat das Minimalpolynom h von a über k die Form $h = g(X^p)$ nach Lemma 10.5. Da h irreduzibel ist, muss auch g irreduzibel sein (eine Faktorisierung von g würde sich auf h übertragen), und da $g(a^p) = h(a) = 0$ ist, ist g das Minimalpolynom von a^p über k. Es folgt

$$[k(a) : k(a^p)] = \frac{[k(a) : k]}{[k(a^p) : k]} = \frac{\deg(h)}{\deg(g)} = p\,,$$

also gilt hier $k(a^p) \subsetneq k(a)$.

In der dritten Aussage gilt „$\Leftarrow$“ nach Definition. Für die Gegenrichtung ist nur im Fall $\mathrm{char}(k) = p > 0$ etwas zu zeigen. Sei $b \in k(a)$; es ist zu zeigen, dass b separabel über k ist. Nach Teil (2) genügt es zu zeigen, dass $k(b^p) = k(b)$ ist, wobei wir verwenden können, dass $k(a^p) = k(a)$ ist. Wir schreiben $\phi\colon K \to K$ für den Frobenius-Endomorphismus $\lambda \mapsto \lambda^p$. Es ist dann $\phi(k(a)) = \phi(k)(a^p)$ und $\phi(k(b)) = \phi(k)(b^p)$. Da ϕ injektiv ist, folgt $[\phi(k)(a^p) : \phi(k)(b^p)] = [k(a) : k(b)]$. Da $\phi(k) \subset k$, ist $k(a^p)$ das Kompositum von $k(b^p)$ und $\phi(k)(a^p)$. Nach Lemma 5.12 (1) folgt

$$[k(a) : k(b^p)] = [k(a^p) : k(b^p)] \leq [\phi(k)(a^p) : \phi(k)(b^p)] = [k(a) : k(b)]$$

und damit

$$[k(b) : k(b^p)] = \frac{[k(a) : k(b^p)]}{[k(a) : k(b)]} \leq 1\,,$$

woraus wie gewünscht $k(b^p) = k(b)$ folgt. ❑

Körper mit der Eigenschaft, dass jede algebraische Erweiterung separabel ist, haben einen besonderen Namen.

* 10.8. **Definition.** Ein Körper K heißt *vollkommen* oder *perfekt*, wenn jedes irreduzible Polynom in $K[X]$ separabel ist. Dann ist auch jede algebraische Körpererweiterung von K separabel. ♢

DEF
vollkommen
perfekt

* 10.9. **Satz.** *Sei K ein Körper.*

SATZ
Satz von Steinitz

(1) *Ist* $\mathrm{char}(K) = 0$*, dann ist K vollkommen.*

(2) *Im Fall* $\mathrm{char}(K) = p > 0$ *ist K genau dann vollkommen, wenn $\{a^p \mid a \in K\} = K$ gilt, wenn also der Frobenius-Endomorphismus $\phi\colon K \to K$, $a \mapsto a^p$, surjektiv (und damit ein Automorphismus) ist.*

(3) *Ist K endlich, dann ist K vollkommen.*

Beweis. Der Fall von Charakteristik 0 folgt wieder aus Folgerung 10.3.

Wir betrachten den Fall $\mathrm{char}(K) = p > 0$. Wir nehmen zunächst an, dass ϕ nicht surjektiv ist. Dann gibt es $a \in K$ mit $a \neq b^p$ für alle $b \in K$. Wir betrachten eine Körpererweiterung L von K, in der $X^p - a$ eine Nullstelle α hat. Es gilt dann $\alpha \notin K$, aber $\alpha^p = a \in K$, also ist $K(\alpha^p) = K \subsetneq K(\alpha)$ und damit ist α nicht separabel über K nach Lemma 10.7. Jetzt nehmen wir an, dass ϕ surjektiv ist. Sei $f \in K[X]$ ein irreduzibles Polynom. Wenn f nicht separabel wäre, dann gäbe es $g \in K[X]$ mit $f = g(X^p)$. Wir schreiben $g = a_n X^n + \ldots + a_1 X + a_0$, dann ist $f = a_n X^{pn} + \ldots + a_1 X^p + a_0$. Da ϕ surjektiv ist, gibt es $b_0, b_1, \ldots, b_n \in K$ mit $b_j^p = a_j$ für $0 \leq j \leq n$. Dann ist

$$f = b_n^p X^{np} + b_{n-1}^p X^{(n-1)p} + \ldots + b_1^p X^p + b_0^p = (b_n X^n + b_{n-1} X^{n-1} + \ldots + b_1 X + b_0)^p\,,$$

und kann f nicht irreduzibel sein, ein Widerspruch. Also muss f separabel sein, und K ist vollkommen.

Ist K endlich, dann gilt $\mathrm{char}(K) = p$ für eine Primzahl p. Der Frobenius-Endomorphismus ϕ ist in diesem Fall bijektiv (siehe die Diskussion nach Definition 8.2), also ist K nach Teil (2) vollkommen. ❑

10.10. **Beispiel.** Ein unvollkommener Körper ist also nicht so leicht zu finden. Wie Beispiel 10.4 zeigt, ist $\mathbb{F}_p(y)$ ein solcher. In jedem Fall muss es ein unendlicher Körper von Primzahlcharakteristik sein. ♣

BSP unvollkommener Körper

Wir kommen zum Satz vom primitiven Element; er besagt, dass jede endliche separable Erweiterung einfach ist. Wir behandeln den wesentlichen Schritt als Lemma vorneweg.

10.11. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung und seien $a, b \in K$ algebraisch über k mit b separabel über k. Dann gibt es $c \in k(a,b)$ mit $k(c) = k(a,b)$.*

LEMMA $k(a,b) = k(c)$

Beweis. $k(a,b)$ ist eine endliche Erweiterung von k. Ist k ein endlicher Körper, dann ist auch $k(a,b)$ endlich. Nach Lemma 8.6 ist die Erweiterung $k \subset k(a,b)$ einfach. Wir können ab jetzt also annehmen, dass k unendlich ist.

Seien f das Minimalpolynom von a und g das Minimalpolynom von b über k und sei $k(a,b) \subset L$ ein Zerfällungskörper von fg über k. Wir bezeichnen die verschiedenen Nullstellen von f in L mit $a = a_1, a_2, \ldots, a_m$ und die verschiedenen Nullstellen von g in L mit $b = b_1, b_2, \ldots, b_n$. Die Menge der $\lambda \in k$, für die es ein Paar $(i,j) \neq (1,1)$ gibt mit

$$a + \lambda b = a_i + \lambda b_j \,,$$

ist endlich (jedes Paar (i,j) schließt höchstens ein λ aus). Da k unendlich ist, gibt es also ein $\lambda \in k$ mit $c := a + \lambda b \neq a_i + \lambda b_j$ für alle $(i,j) \neq (1,1)$. Wir wollen jetzt $k(c) = k(a,b)$ zeigen. Die Inklusion „$\subset$“ ist klar; es bleibt also $a, b \in k(c)$ zu zeigen. Wir zeigen $b \in k(c)$, dann folgt $a = c - \lambda b \in k(c)$. Dazu betrachten wir $h = \mathrm{ggT}(g, f(c - \lambda X))$ in $k(c)[X]$. Da b eine gemeinsame Nullstelle von g und $f(c - \lambda X)$ ist, muss $X - b$ ein Teiler von h sein (in $k(a,b)[X]$). Wäre b_j mit $j > 1$ eine Nullstelle von h, dann wäre b_j auch eine Nullstelle von $f(c - \lambda X)$, also wäre $c - \lambda b_j = a_i$ für ein $1 \leq i \leq m$, im Widerspruch zur Wahl von λ. Da h ein Teiler von g sein muss und da g nur einfache Nullstellen hat (denn b ist separabel über k — hier wird diese wichtige Voraussetzung verwendet!), folgt $h = X - b$. Da der ggT aber durch den Euklidischen Algorithmus in $k(c)[X]$ berechnet werden kann, folgt $b \in k(c)$. ❑

10.12. **Beispiel.** Wir betrachten $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$, den Zerfällungskörper von $X^4 - 17$ über $\mathbb{Q}$. Mit $\lambda = 1$ sehen wir, dass alle Elemente $\boldsymbol{i}^m \sqrt[4]{17} \pm \boldsymbol{i}$ (mit $0 \leq m \leq 3$) paarweise verschieden sind. Da wir uns in Charakteristik 0 befinden, sind alle Elemente separabel. Es folgt $K = \mathbb{Q}(\sqrt[4]{17} + \boldsymbol{i})$. ♣

BSP primitives Element

* 10.13. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und seien $a, b_1, \ldots, b_n \in K$ algebraisch über k mit $b_1, \ldots, b_n$ separabel über k. Dann gibt es $c \in k(a, b_1, \ldots, b_n)$ mit $k(c) = k(a, b_1, \ldots, b_n)$.*

SATZ Satz vom primitiven Element

Insbesondere ist jede endliche separable Körpererweiterung $k \subset K$ einfach, hat also ein primitives Element c (d.h., es ist $K = k(c)$).

Beweis. Wir beweisen die Aussage durch Induktion nach n. Für $n = 0$ gilt die Behauptung trivialerweise mit $c = a$. Sei also $n \geq 1$. Nach Induktionsvoraussetzung gibt es $c' \in k(a, b_1, \ldots, b_{n-1})$ mit $k(a, b_1, \ldots, b_{n-1}) = k(c')$; insbesondere ist c' algebraisch über k. Dann haben wir

$$k(a, b_1, \ldots, b_{n-1}, b_n) = k(a, b_1, \ldots, b_{n-1})(b_n) = k(c')(b_n) = k(c', b_n) \,.$$

Nach Lemma 10.11 gibt es $c \in k(c', b_n)$ mit $k(c', b_n) = k(c)$.

Ist $k \subset K$ endlich und separabel, dann wird K von endlich vielen separablen Elementen über k erzeugt; damit ist der erste Teil des Satzes anwendbar. ❑

Wie Algebraizität ist auch Separabilität transitiv:

SATZ
Transitivität der Separabilität

10.14. **Satz.** *Sei $k \subset K$ eine Körpererweiterung.*

(1) *Sind $a, b \in K$, sodass a separabel ist über k und b separabel ist über $k(a)$, dann ist b auch separabel über k.*

(2) *Ist $K \subset L$ eine weitere Körpererweiterung und sind die Erweiterungen $k \subset K$ und $K \subset L$ separabel, dann ist auch $k \subset L$ separabel.*

Beweis. Es ist nur im Fall positiver Charakteristik p etwas zu zeigen. Zum Beweis der ersten Aussage benutzen wir Lemma 10.7. Aus den Voraussetzungen folgt dann $k(a^p) = k(a)$ und $k(a)(b^p) = k(a)(b)$; damit ist $k(a^p, b^p) = k(a, b^p) = k(a, b)$. Wie im Beweis von Lemma 10.7 (3) haben wir $[k(a^p, b^p) : k(b^p)] \leq [k(a, b) : k(b)]$, und wie dort folgt $k(b^p) = k(b)$, also ist b separabel über k.

Zum Beweis der zweiten Aussage sei $b \in L$; wir müssen zeigen, dass b separabel über k ist. Sei dazu f das Minimalpolynom von b über K und K' der von den Koeffizienten von f über k erzeugte Zwischenkörper. Dann ist K' eine von endlich vielen separablen Elementen erzeugte Erweiterung von k; nach dem Satz vom primitiven Element 10.13 ist also $K' = k(a)$ mit einem $a \in K' \subset K$; a ist separabel über k, da die Körpererweiterung $k \subset K$ separabel ist. Nach Teil (1) folgt, dass auch b separabel über k ist. ❑

Die Umkehrung „$k \subset L$ separabel $\implies$ $k \subset K$ separabel und $K \subset L$ separabel“ gilt auch, wie man sich sehr leicht überlegt.

11. Automorphismen von Körpererweiterungen

Wir betrachten jetzt Automorphismen von Körpererweiterungen genauer.

* 11.1. **Definition.** Seien $k \subset K$ und $k \subset L$ zwei Körpererweiterungen. Ein *Homomorphismus* $K \to L$ von Körpererweiterungen von k oder *Homomorphismus über* k ist ein Körperhomomorphismus $\phi\colon K \to L$ mit $\phi|_k = \mathrm{id}_k$. ϕ ist ein *Isomorphismus* von Körpererweiterungen, wenn ϕ bijektiv ist. Im Fall $L = K$ heißt ϕ dann ein *Automorphismus* der Körpererweiterung $k \subset K$. Diese Automorphismen bilden eine Gruppe, die *Automorphismengruppe* $\mathrm{Aut}(K/k)$ von $k \subset K$. ♢

DEF Automorphismus einer Körpererweiterung

Es ist klar, dass $\mathrm{Aut}(K/k)$ in natürlicher Weise auf K operiert.

Ein Homomorphismus ϕ über k ist stets k-linear bezüglich der natürlichen k-Vektorraumstruktur der Erweiterungskörper (denn $\phi(x+y) = \phi(x)+\phi(y)$, weil ϕ ein Ringhomomorphismus ist, und für $\lambda \in k$ ist auch $\phi(\lambda x) = \phi(\lambda)\phi(x) = \lambda\phi(x)$ wegen $\phi|_k = \mathrm{id}_k$). Wir erinnern uns auch daran, dass jeder Körperhomomorphismus injektiv ist.

11.2. **Lemma.** *Ist $k \subset K$ eine endliche Körpererweiterung und $\phi\colon K \to K$ ein Homomorphismus über k, dann ist $\phi \in \mathrm{Aut}(K/k)$.*

LEMMA Automorphismen von endlichen KE

Beweis. Als Homomorphismus von Körpern ist ϕ injektiv. Außerdem ist ϕ k-linear. Als injektiver Endomorphismus eines endlich-dimensionalen Vektorraums ist ϕ dann auch bijektiv. ❑

Im Fall von endlichen *separablen* Körpererweiterungen können wir eine recht genaue Aussage über die mögliche Anzahl von Homomorphismen machen.

11.3. **Satz.** *Sei $k \subset K$ eine endliche separable Körpererweiterung und sei $k \subset L$ eine weitere Körpererweiterung. Dann gibt es höchstens $[K : k]$ Homomorphismen $K \to L$ über k. Außerdem gibt es eine Körpererweiterung $L \subset L'$, sodass es genau $[K : k]$ solcher Homomorphismen $K \to L'$ über k gibt.*

SATZ Homomorphismen von separablen KE

Beweis. Da $k \subset K$ separabel ist, gibt es nach dem Satz vom primitiven Element 10.13 ein Element $\alpha \in K$, sodass $K = k(\alpha)$ ist. Sei f das Minimalpolynom von α über k und sei $\deg(f) = n$; dann ist $[K : k] = n$.

Nach Satz 7.2 gibt es dann genau so viele Homomorphismen $K \to L$ über k, wie f Nullstellen in L hat. Wegen $\deg(f) = n$ sind das in jedem Fall höchstens $n = [K : k]$.

Sei $L \subset L'$ eine Körpererweiterung, sodass L' einen Zerfällungskörper von f über k enthält. (Zum Beispiel können wir für L' einen Zerfällungskörper von f über L nehmen.) Da $k \subset K$ separabel ist, ist α separabel; damit hat f in L' nur einfache Nullstellen. Da f in $L'[x]$ nach Annahme in Linearfaktoren zerfällt, hat f in L' *genau* n Nullstellen, und es gibt demnach auch $n = [K : k]$ Homomorphismen $K \to L'$ über k. ❑

Wir werden uns bald genauer mit Untergruppen von $\mathrm{Aut}(K/k)$ und Zwischenkörpern der Körpererweiterung $k \subset K$ befassen. Es gibt eine enge Beziehung zwischen diesen beiden Arten von Objekten:

DEF
Fixkörper
Fixgruppe

11.4. **Definition.** Sei $k \subset K$ eine Körpererweiterung.

(1) Sei $U \leq \mathrm{Aut}(K/k)$ eine Untergruppe. Dann heißt der Zwischenkörper(!)
$$\mathcal{F}(U) = \{\alpha \in K \mid \forall \sigma \in U \colon \sigma(\alpha) = \alpha\}$$
von $k \subset K$ der *Fixkörper* von U.

(2) Sei $k \subset L \subset K$ ein Zwischenkörper. Dann heißt die Untergruppe
$$\mathcal{U}(L) = \{\sigma \in \mathrm{Aut}(K/k) \mid \forall \alpha \in L \colon \sigma(\alpha) = \alpha\}$$
von $\mathrm{Aut}(K/k)$ die *Fixgruppe* von L. ♢

Die Schreibweise für Fixkörper und -gruppen variiert in der Literatur.

Da $\mathrm{Aut}(K) = \mathrm{Aut}(K/P)$ ist, wobei P der Primkörper von K ist, können wir diese Begriffe auch für Untergruppen von $\mathrm{Aut}(K)$ und beliebige Teilkörper von K verwenden. Für später wichtig ist dann das folgende Ergebnis.

LEMMA
Fixkörper einer Untergruppe von $\mathrm{Aut}(K)$

11.5. **Lemma.** *Sei K ein Körper und sei $G \leq \mathrm{Aut}(K)$ eine endliche Untergruppe der Automorphismengruppe von K. Wir setzen $k = \mathcal{F}(G)$.*

(1) *Sei $\alpha \in K$ und seien $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ die verschiedenen Elemente der Bahn von α unter G. Dann ist*
$$f = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) \in k[x]$$
ein normiertes irreduzibles Polynom mit Koeffizienten in k. Insbesondere ist α algebraisch über k mit Minimalpolynom f.

(2) *$k \subset K$ ist separabel; es gilt $G = \mathrm{Aut}(K/k)$ und $[K : k] = \#G$.*

Beweis.

(1) Es ist zunächst zu zeigen, dass f Koeffizienten in k hat. Wir können die Automorphismen von K zu Automorphismen des Polynomrings $K[x]$ fortsetzen, indem wir sie auf die Koeffizienten der Polynome anwenden. Für $\gamma \in G$ gilt dann $\gamma(f) = f$, denn γ permutiert die Elemente der Bahn von α und damit die Faktoren in der Produktdarstellung von f. Das bedeutet, dass alle Koeffizienten Fixpunkte der Operation von G sind; nach Definition des Fixkörpers sind sie also in $k = \mathcal{F}(G)$. Dass f normiert ist, ist klar. Als Nullstelle eines normierten Polynoms in $k[x]$ ist α dann algebraisch über k. Es bleibt zu zeigen, dass f irreduzibel ist. Das liegt daran, dass G auf der Bahn von α (wie auf jeder Bahn) transitiv operiert: Haben wir eine Faktorisierung $f = f_1 f_2$ in $k[x]$, wobei wir annehmen können, dass $f_1(\alpha) = 0$ ist, dann muss jeder Automorphismus von K α auf eine Nullstelle von f_1 abbilden. Also hat f_1 schon alle Elemente der Bahn von α als Nullstellen; damit muss f_2 konstant sein. Da $f \in k[x]$ irreduzibel und normiert ist und α als Nullstelle hat, muss f das Minimalpolynom von α über k sein.

(2) Sei $\alpha \in K$ und f wie in Teil (1) das Minimalpolynom von α über k. Da f offensichtlich nur einfache Nullstellen hat, ist α separabel über k. Da $\alpha \in K$ beliebig war, folgt, dass die Körpererweiterung $k \subset K$ separabel ist. Wir zeigen, dass die Körpererweiterung auch endlich ist: Nach Teil (1) gilt für jedes $\alpha \in K$
$$[k(\alpha) : k] = \deg(f) = \#(G \cdot \alpha) \leq \#G\,.$$

Nach dem Satz vom primitiven Element 10.13 ist jeder Zwischenkörper $k \subset L \subset K$, der über k endlich ist, von der Form $L = k(\alpha)$, also gilt $[L : k] \leq \#G$. Sei jetzt L ein Zwischenkörper mit $[L : k]$ endlich und maximal. Gäbe es $\beta \in K \setminus L$, dann wäre $L \subsetneq L(\beta) \subset K$ und β algebraisch über k. Dann wäre aber $[L : k] < [L(\beta) : k] < \infty$, im Widerspruch zur Wahl von L. Es folgt $K = L$, also ist $k \subset K$ endlich, und $[K : k] \leq \#G$. Auf der anderen Seite gilt nach Satz 11.3 $\#G \leq \# \operatorname{Aut}(K/k) \leq [K : k]$ (nach Definition von k ist $G \leq \operatorname{Aut}(K/k)$), also ist $[K : k] = \#G = \# \operatorname{Aut}(K/k)$, woraus auch $G = \operatorname{Aut}(K/k)$ folgt. ❑

11.6. **Folgerung.** *Sei $k \subset K$ eine endliche separable Körpererweiterung. Dann gilt $\# \operatorname{Aut}(K/k) \leq [K : k]$ mit Gleichheit genau dann, wenn jedes normierte irreduzible Polynom $f \in k[x]$, das in K eine Nullstelle hat, in $K[x]$ bereits in Linearfaktoren zerfällt.*

FOLG Kriterium für $\# \operatorname{Aut}(K/k) = [K : k]$

Beweis. Die Aussage „$\# \operatorname{Aut}(K/k) \leq [K : k]$“ ist als Spezialfall $L = K$ in Satz 11.3 enthalten. Hat K die angegebene Eigenschaft, dann ist $L' = K$ eine mögliche Wahl in Satz 11.3, also folgt Gleichheit. Jetzt nehmen wir umgekehrt an, dass $\# \operatorname{Aut}(K/k) = [K : k]$ gilt. Dann ist $k = \mathcal{F}(\operatorname{Aut}(K/k))$, denn

$$k \subset \mathcal{F}(\operatorname{Aut}(K/k)) \qquad \text{und} \qquad [K : k] = \# \operatorname{Aut}(K/k) = [K : \mathcal{F}(\operatorname{Aut}(K/k))]$$

nach Lemma 11.5 (2). Sei $f \in k[x]$ normiert und irreduzibel und $\beta \in K$ mit $f(\beta) = 0$. Wir betrachten die Bahn $\{\phi(\beta) \mid \phi \in \operatorname{Aut}(K/k)\}$ von β unter der Automorphismengruppe von $k \subset K$; ihre Elemente seien $\beta = \beta_1, \beta_2, \ldots, \beta_m$. Nach Lemma 11.5 ist dann $\tilde{f} = \prod_{j=1}^{m} (x - \beta_j) \in k[x]$ das Minimalpolynom von β, also ist $f = \tilde{f}$, und f zerfällt in $K[x]$ in Linearfaktoren. ❑

Die Eigenschaft der Körpererweiterung, die die Gleichheit von $[K : k]$ und $\# \operatorname{Aut}(K/k)$ garantiert, ist wichtig genug, dass sie einen eigenen Namen hat:

$*$ 11.7. **Definition.** Eine Körpererweiterung $k \subset K$ mit der Eigenschaft, dass jedes normierte irreduzible Polynom $f \in k[x]$, das in K eine Nullstelle hat, in $K[x]$ in Linearfaktoren zerfällt, heißt *normal*. ♢

DEF normale KE

(Wir werden später sehen, wo diese zunächst einmal wenig erhellende Bezeichnung herkommt.)

11.8. **Beispiele.**

BSP (nicht) normale KE

(1) Sei $k \subset K$ eine Körpererweiterung vom Grad $[K : k] = 2$. Dann ist $k \subset K$ normal. Denn sei $f \in k[x]$ ein normiertes irreduzibles Polynom, das in K eine Nullstelle α hat. Dann folgt $\deg(f) \leq 2$. Jedes Polynom vom Grad 1 „zerfällt“ trivialerweise in Linearfaktoren. Wir können demnach $\deg(f) = 2$ annehmen, also $f = x^2 + ax + b$ mit $a, b \in K$. Dann ist aber $f = (x - \alpha)(x + a + \alpha)$ in $K[x]$; damit zerfällt f in $K[x]$ in Linearfaktoren.

(2) Eine Körpererweiterung vom Grad 3 braucht dagegen nicht normal zu sein. Zum Beispiel hat $f = x^3 - 2$ in $K = \mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle, zerfällt aber über K nicht in Linearfaktoren, da die anderen beiden Nullstellen nicht in K liegen. Also ist $\mathbb{Q} \subset K$ nicht normal.

(3) Ist K algebraisch abgeschlossen, dann ist $k \subset K$ normal, weil *jedes* Polynom in $K[x]$ in Linearfaktoren zerfällt. ♣

BSP Normalität nicht transitiv

11.9. **Beispiel.** Im Gegensatz zu Algebraizität und Separabilität ist Normalität *nicht* transitiv. Zum Beispiel ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{17})$ nicht normal, denn $L = \mathbb{Q}(\sqrt[4]{17})$ enthält nur zwei der vier Nullstellen von $x^4 - 17$. Auf der anderen Seite sind aber die beiden Körpererweiterungen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{17})$ und $\mathbb{Q}(\sqrt{17}) \subset \mathbb{Q}(\sqrt[4]{17})$ normal, da sie Grad 2 haben. ♣

12. Galois-Erweiterungen

Im verbleibenden Teil der Vorlesung werden wir uns mit der sogenannten *Galois-Theorie* befassen. Kurz gesagt, handelt es sich um das Studium der Struktur von Zerfällungskörpern; insbesondere um die Beschreibung der Zwischenkörper zwischen dem Grundkörper k und dem Zerfällungskörper K eines Polynoms $f \in k[X]$. Eine entscheidende Rolle spielt dabei die Automorphismengruppe der Körpererweiterung $k \subset K$, die wir im letzten Abschnitt studiert haben.

É. Galois (1811–1832)

Die Bezeichnung „Galois-Theorie“ verweist auf Évariste Galois, der die grundlegenden Zusammenhänge Anfang der 1830er Jahre erkannte und kurz darauf nach einem Duell im Alter von 20 Jahren starb.

* 12.1. **Definition.** Eine Körpererweiterung $k \subset K$ heißt *galoissch* oder *Galois-Erweiterung*, wenn $k = \mathcal{F}(\mathrm{Aut}(K/k))$ ist. In diesem Fall heißt $\mathrm{Aut}(K/k)$ die *Galois-Gruppe* der Körpererweiterung $k \subset K$; sie wird häufig $\mathrm{Gal}(K/k)$ geschrieben. ♢

DEF Galois-Erweiterung

Galois-Gruppe

Beachte: $k \subset \mathcal{F}(\mathrm{Aut}(K/k))$ gilt immer nach Definition von $\mathrm{Aut}(K/k)$. Die Bedingung ist also, dass jedes unter $\mathrm{Aut}(K/k)$ festgehaltene Element von K bereits in k liegt.

Man beachte auch die zwei „s“ in „galoissch“!

12.2. **Beispiel.** Die Körpererweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[3]{17})$ ist nicht galoissch, denn K hat keine nichttrivialen Automorphismen (jeder Automorphismus muss $\sqrt[3]{17}$ auf eine Nullstelle von $X^3 - 17$ abbilden; in K gibt es aber keine andere Nullstelle); damit ist $\mathcal{F}(\mathrm{Aut}(K/\mathbb{Q})) = K \neq \mathbb{Q}$. ♣

BSP keine Galois-Erweiterung

Wir können endliche Galois-Erweiterungen charakterisieren:

* 12.3. **Satz.** *Sei $k \subset K$ eine endliche Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

SATZ Galois-Erweiterungen

(1) *$k \subset K$ ist galoissch.*

(2) *$k \subset K$ ist separabel und normal.*

(3) *$\#\,\mathrm{Aut}(K/k) = [K : k]$.*

(4) *K ist Zerfällungskörper eines normierten separablen irreduziblen Polynoms $f \in k[x]$.*

Beweis. „(1) ⇒ (3)“: Wir wenden Lemma 11.5 an auf $G = \mathrm{Aut}(K/k)$. Nach Voraussetzung ist $k = \mathcal{F}(G)$, also ist $[K : k] = \#G$ (und $k \subset K$ ist separabel).

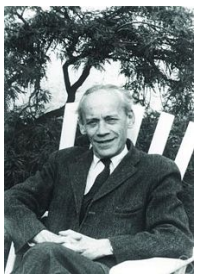
„(3) ⇒ (1)“: Sei wieder $G = \mathrm{Aut}(K/k)$; es gelte $[K : k] = \#G$. Dann haben wir $k \subset \mathcal{F}(G) \subset K$ und nach Lemma 11.5 gilt $[K : \mathcal{F}(G)] = \#G = [K : k]$. Daraus folgt $k = \mathcal{F}(G)$.

„(1) ⇒ (2)“: Wir haben schon gesehen, dass aus (1) die Separabilität folgt. Außerdem folgt (3); nach Folgerung 11.6 bedeutet die Gleichheit $[K : k] = \#\,\mathrm{Aut}(K/k)$ gerade, dass $k \subset K$ normal ist.

„(2) ⇒ (4)“: Da $k \subset K$ endlich und separabel ist, gibt es nach dem Satz vom primitiven Element 10.13 ein $\alpha \in K$ mit $K = k(\alpha)$. Sei f das Minimalpolynom von α über k. Da $k \subset K$ normal ist und f die Nullstelle α in K hat, zerfällt f

in $K[x]$ in Linearfaktoren. Damit ist K ein Zerfällungskörper von f; f ist separabel, da α separabel über k ist (denn $k \subset K$ ist separabel).

„(4) ⇒ (3)“: Das folgt aus dem Beweis von Satz 11.3. ❑



E. Artin (1898–1962)

Da Normalität nicht transitiv in Körpererweiterungen ist, gilt das analog für die Eigenschaft galoissch zu sein (wie dasselbe Beispiel zeigt).

Die Äquivalenz von (1) und (2) gilt auch noch für unendliche algebraische Körpererweiterungen (Satz von Artin, siehe z.B. [KM, Satz 26.7]).

12.4. **Beispiel.** Ist $\mathrm{char}(k) \neq 2$ und ist $k \subset K$ eine quadratische Körpererweiterung (also mit $[K : k] = 2$), dann ist $k \subset K$ galoissch, denn eine quadratische Erweiterung ist stets normal, und sie kann nur dann inseparabel sein, wenn die Charakteristik den Grad teilt. Es gilt dann $\mathrm{Aut}(K/k) = \{\mathrm{id}_K, \tau\}$ für einen Automorphismus $\tau \neq \mathrm{id}_K$. Wegen $\mathrm{char}(k) \neq 2$ können wir die übliche quadratische Ergänzung durchführen. Das zeigt, dass $K = k(\sqrt{a})$ ist für ein $a \in k$ (sodass a kein Quadrat in k ist). Das Minimalpolynom von $\sqrt{a}$ ist $x^2 - a$ und hat $-\sqrt{a}$ als einzige weitere Nullstelle, also muss $\tau(\sqrt{a}) = -\sqrt{a}$ sein.

BSP quadratische Erweiterung

Als konkretes Beispiel haben wir $\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i)$; in diesem Fall ist τ die komplexe Konjugation: $\tau(a + bi) = a - bi$. ♣

12.5. **Folgerung.** *Jede Erweiterung $k \subset K$ von endlichen Körpern ist galoissch mit* $\mathrm{Gal}(K/k) \cong \mathbb{Z}/[K : k]\mathbb{Z}$.

FOLG Erw. endlicher Körper sind galoissch

Beweis. Sei $q = \#k$ (dann ist $q = p^e$ eine Primzahlpotenz und p ist die Charakteristik von k), dann ist $\phi\colon K \to K$, $x \mapsto x^q$ ein Automorphismus von K, der die Elemente von k fest lässt (und nur diese, denn die Fixpunkte sind genau die q Nullstellen von $x^q - x$), also ist $\phi \in \mathrm{Aut}(K/k)$, und es gilt $\mathcal{F}(\mathrm{Aut}(K/k)) \subset \mathcal{F}(\langle\phi\rangle) = k$. Damit ist $k \subset K$ jedenfalls galoissch und es folgt zusätzlich, dass $\mathrm{Aut}(K/k) = \langle\phi\rangle$ ist, denn

$$\#\,\mathrm{Aut}(K/k) = [K : k] = [K : \mathcal{F}(\langle\phi\rangle)] = \#\langle\phi\rangle\,.$$

Die Galois-Gruppe $\mathrm{Aut}(K/k)$ ist also zyklisch und wird von ϕ erzeugt. ❑

12.6. **Beispiel.** Die Automorphismengruppe von $\mathbb{R}$ ist trivial: $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$. (Das zu zeigen war eine Übungsaufgabe.)

BSP $\mathbb{R}$ ist keine Galois-Erweiterung

Als Konsequenz ergibt sich, dass es *keine* Galois-Erweiterung $k \subset \mathbb{R}$ mit $k \neq \mathbb{R}$ geben kann. ♣

12.7. **Folgerung.** *Ist K der Zerfällungskörper über k eines (nicht notwendig irreduziblen) normierten separablen Polynoms $f \in k[x]$, dann ist $k \subset K$ galoissch.*

FOLG Zerfällungskörper sind galoissch

Beweis. Seien $f_1, f_2, \ldots, f_l$ die verschiedenen normierten irreduziblen Faktoren von f. Da f separabel ist, sind auch alle f_j separabel. Dann können wir statt f auch $f_0 = f_1 f_2 \cdots f_l$ betrachten; f_0 hat nur einfache Nullstellen in K.

Ist $k \subset L \subset K$ ein Zwischenkörper, dann schreiben wir $\mathrm{Hom}_k(L, K)$ für die Menge der Homomorphismen $L \to K$ über k. Sei $L_0 = k$. Ist L_n definiert und $L_n \neq K$, dann gibt es eine Nullstelle α_{n+1} von f_0 in K mit $\alpha_{n+1} \notin L_n$; wir setzen $L_{n+1} = L_n(\alpha_{n+1})$. Dann bilden die L_n eine strikt aufsteigende Folge von Zwischenkörpern von $k \subset K$. Da diese Erweiterung als Zerfällungskörper endlich

ist, muss es einen Index m geben mit $L_m = K$. Wir zeigen jetzt durch Induktion, dass $\#\operatorname{Hom}_k(L_n, K) = [L_n : k]$ ist für $n = 0, 1, \ldots, m$. Für $m = n$ erhalten wir

$$\#\operatorname{Aut}(K/k) = \#\operatorname{Hom}_k(K, K) = \#\operatorname{Hom}_k(L_m, K) = [L_m : k] = [K : k]\,,$$

woraus mit Satz 12.3 folgt, dass $k \subset K$ galoissch ist.

Es ist $L_0 = k$, also ist $\#\operatorname{Hom}_k(L_0, k) = 1 = [L_0 : k]$. Für den Schritt von n auf $n+1$ sei h_{n+1} das Minimalpolynom von α_{n+1} über L_n; dann hat h_{n+1} genau $\deg(h_{n+1}) = [L_{n+1} : L_n]$ verschiedene Nullstellen in K, und dasselbe gilt für h_{n+1}^{ϕ} für jeden Homomorphismus $\phi \in \operatorname{Hom}_k(L_n, K)$ (dabei bezeichne h^{ϕ} das Polynom, das man aus h bekommt, indem man ϕ auf die Koeffizienten anwendet), denn h_{n+1} und h_{n+1}^{ϕ} sind Teiler von f_0 in $K[x]$ und zerfallen deshalb über K in Linearfaktoren. Nach Satz 7.2 lässt sich jeder Homomorphismus $\phi \in \operatorname{Hom}_k(L_n, K)$ auf genau $[L_{n+1} : L_n]$ verschiedene Arten zu einem Homomorphismus $L_{n+1} \to K$ fortsetzen. Insgesamt erhalten wir dann

$$\begin{aligned}\#\operatorname{Hom}_k(L_{n+1}, K) &= [L_{n+1} : L_n] \cdot \#\operatorname{Hom}_k(L_n, K) \\ &= [L_{n+1} : L_n] \cdot [L_n : k] = [L_{n+1} : k]\end{aligned}$$

wie gewünscht. ❑

Das im obigen Beweis verwendete Verfahren lässt sich auch dazu benutzen, die Automorphismen einer Galois-Erweiterung zu bestimmen.

12.8. **Beispiel.** Sei $K = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$; das ist der Zerfällungskörper von $f = X^4 - 17$ über $\mathbb{Q}$. Wir betrachten den Körperturm **BSP** $\mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$

$$\mathbb{Q} \subset \mathbb{Q}(\boldsymbol{i}) \subset \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i}) = K\,;$$

es ist $\mathbb{Q}(\boldsymbol{i})$ der Zerfällungskörper von $X^2 + 1$ über $\mathbb{Q}$ und K der Zerfällungskörper von f über $\mathbb{Q}(\boldsymbol{i})$; außerdem bleibt f irreduzibel über $\mathbb{Q}(\boldsymbol{i})$, was man z.B. mit dem Eisenstein-Kriterium, angewendet für den Ring $\mathbb{Z}[\boldsymbol{i}]$ und das Primelement $1 + 4\boldsymbol{i}$, sehen kann.

Nach Beispiel 12.4 ist $\operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\boldsymbol{i}), K) = \operatorname{Aut}(\mathbb{Q}(\boldsymbol{i})/\mathbb{Q}) = \{\mathrm{id}, \tau'\}$ mit $\tau'(\boldsymbol{i}) = -\boldsymbol{i}$. Wir bestimmen jetzt, wie sich diese Homomorphismen auf K fortsetzen lassen. Die Nullstellen von f in K sind $\alpha = \sqrt[4]{17}$, $\boldsymbol{i}\alpha$, $-\alpha$ und $-\boldsymbol{i}\alpha$. Wegen $K = \mathbb{Q}(\boldsymbol{i})(\alpha)$ ist die Fortsetzung jeweils durch ihren Wert an der Stelle α eindeutig bestimmt, und dieser Wert kann jede der vier Nullstellen sein (weil f irreduzibel über $\mathbb{Q}(\boldsymbol{i})$ ist). Sei $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ die Fortsetzung von $\mathrm{id}\colon \mathbb{Q}(\boldsymbol{i}) \hookrightarrow K$ mit $\sigma(\alpha) = \boldsymbol{i}\alpha$, und sei τ die Fortsetzung von τ' mit $\tau(\alpha) = \alpha$. Dann erhalten wir die folgenden Automorphismen:

ρ	$\rho\vert_{\mathbb{Q}(\boldsymbol{i})}$	$\rho(\boldsymbol{i})$	$\rho(\alpha)$	$\rho(\boldsymbol{i}\alpha)$	$\rho(-\alpha)$	$\rho(-\boldsymbol{i}\alpha)$
id	id	$\boldsymbol{i}$	α	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$
σ	id	$\boldsymbol{i}$	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α
σ^2	id	$\boldsymbol{i}$	$-\alpha$	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$
σ^3	id	$\boldsymbol{i}$	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$	$-\alpha$
τ	τ'	$-\boldsymbol{i}$	α	$-\boldsymbol{i}\alpha$	$-\alpha$	$\boldsymbol{i}\alpha$
$\sigma\tau$	τ'	$-\boldsymbol{i}$	$\boldsymbol{i}\alpha$	α	$-\boldsymbol{i}\alpha$	$-\alpha$
$\sigma^2\tau$	τ'	$-\boldsymbol{i}$	$-\alpha$	$\boldsymbol{i}\alpha$	α	$-\boldsymbol{i}\alpha$
$\sigma^3\tau$	τ'	$-\boldsymbol{i}$	$-\boldsymbol{i}\alpha$	$-\alpha$	$\boldsymbol{i}\alpha$	α

An dieser Tabelle liest man ab, dass $\sigma^4 = \tau^2 = \mathrm{id}$ und $\tau\sigma\tau = \sigma^{-1}$ ist; es folgt $\operatorname{Gal}(K/\mathbb{Q}) \cong D_4$. Der Isomorphismus kommt dabei konkret von dem natürlichen Homomorphismus $\operatorname{Gal}(K/\mathbb{Q}) \to S(\{\alpha, \boldsymbol{i}\alpha, -\alpha, -\boldsymbol{i}\alpha\}) \cong S_4$. ♣

Wir betrachten jetzt eine Galois-Erweiterung $k \subset K$ mit einem Zwischenkörper L. Wann sind die beiden Körpererweiterungen $k \subset L$ und $L \subset K$ ebenfalls galoissch?

SATZ galoissch für Zwischenkörper

12.9. **Satz.** *Sei $k \subset K$ eine endliche Galois-Erweiterung und sei $k \subset L \subset K$ ein Zwischenkörper. Dann ist $L \subset K$ galoissch. Die Erweiterung $k \subset L$ ist genau dann galoissch, wenn $\gamma(L) = L$ ist für alle $\gamma \in \mathrm{Gal}(K/k)$. In diesem Fall ist*

$$\Phi\colon \mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(L/k), \quad \gamma \longmapsto \gamma|_L$$

ein surjektiver Gruppenhomomorphismus mit Kern $\mathrm{Gal}(K/L)$*. Insbesondere ist* $\mathrm{Gal}(K/L)$ *ein Normalteiler von* $\mathrm{Gal}(K/k)$ *und* $\mathrm{Gal}(L/k)$ *ist isomorph zur Faktorgruppe* $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$*.*

Die letzte Aussage liefert eine Erklärung für die Bezeichnung „normal“ bei Körpererweiterungen.

Beweis. Wir zeigen erst einmal, dass $L \subset K$ galoissch ist. Nach Satz 12.3 ist K Zerfällungskörper über k eines normierten (sogar irreduziblen) separablen Polynoms $f \in k[x]$. Dann ist K auch Zerfällungskörper von f über L. Nach Folgerung 12.7 ist also $L \subset K$ galoissch.

Da $k \subset K$ nach Satz 12.3 separabel ist, gilt das auch für $k \subset L$. Wiederum nach Satz 12.3 ist $k \subset L$ also genau dann galoissch, wenn $k \subset L$ normal ist. Wir zeigen, dass das äquivalent ist zu $\forall \gamma \in \mathrm{Gal}(K/k)\colon \gamma(L) = L$.

Sei jetzt zunächst $k \subset L$ als normal angenommen; sei $a \in L$ und $\gamma \in \mathrm{Gal}(L/k)$. Wir müssen zeigen, dass $\gamma(a) \in L$ ist. Sei dazu $f \in k[x]$ das Minimalpolynom von a, dann sind alle Nullstellen von f in K bereits in L (denn $k \subset L$ ist normal). Auf der anderen Seite muss $\gamma(a)$ aber eine Nullstelle von f sein, also ist $\gamma(a) \in L$.

Jetzt nehmen wir an, dass $\gamma(L) = L$ ist für alle $\gamma \in \mathrm{Gal}(K/k)$. Wir wollen zeigen, dass dann $k \subset L$ normal ist. Sei also $f \in k[x]$ irreduzibel und normiert und $a \in L$ eine Nullstelle von f. Da $k \subset K$ normal ist, zerfällt f in $K[x]$ in Linearfaktoren. Aus Lemma 11.5 folgt, dass $\mathrm{Gal}(K/k)$ auf den Nullstellen von f in K transitiv operiert. Da $\gamma(L) = L$ ist für alle $\gamma \in \mathrm{Gal}(K/k)$ und eine Nullstelle (nämlich a) in L ist, sind alle Nullstellen in L, also zerfällt f auch schon in $L[x]$ in Linearfaktoren. Wir sehen also, dass jedes irreduzible normierte Polynom $f \in k[x]$, das in L eine Nullstelle hat, in $L[x]$ in Linearfaktoren zerfällt. Damit ist $k \subset L$ normal.

Sei jetzt $k \subset L$ galoissch. Für $\gamma \in \mathrm{Gal}(K/k)$ folgt aus $\gamma(L) = L$, dass die Einschränkung $\gamma|_L \in \mathrm{Gal}(L/k)$ ist; die Abbildung Φ ist also wohldefiniert, und es ist klar, dass Φ ein Gruppenhomomorphismus ist. Die Definition von $\mathrm{Aut}(K/L)$ liefert $\ker(\Phi) = \mathrm{Aut}(K/L) = \mathrm{Gal}(K/L)$, also ist $\mathrm{Gal}(K/L)$ ein Normalteiler von $\mathrm{Gal}(K/k)$. Es bleibt die Surjektivität von Φ zu zeigen. Nach dem Homomorphiesatz für Gruppen ist das Bild von Φ isomorph zu $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$. Es gilt daher

$$\begin{aligned}[L:k] = \#\,\mathrm{Gal}(L/k) \geq \#\,\mathrm{im}(\Phi) &= \#\frac{\mathrm{Gal}(K/k)}{\mathrm{Gal}(K/L)} \\ &= \frac{\#\,\mathrm{Gal}(K/k)}{\#\,\mathrm{Gal}(K/L)} = \frac{[K:k]}{[K:L]} = [L:k]\,,\end{aligned}$$

also folgt Gleichheit. Damit ist Φ surjektiv; die letzte Behauptung folgt dann auch. ❑

DEF Galois-Abschluss

12.10. **Definition.** Ist $k \subset K$ eine endliche separable Körpererweiterung, dann ist $K = k(\alpha)$ eine einfache Körpererweiterung nach dem Satz vom primitiven Element 10.13. Sei $f \in k[x]$ das Minimalpolynom von α über k. Sei L ein Zerfällungskörper von f über K. Dann ist L auch Zerfällungskörper von f über k, also ist $k \subset L$ eine Galois-Erweiterung. Auf der anderen Seite muss jede Galois-Erweiterung von k, die K enthält, einen Zerfällungskörper von f enthalten. Damit ist L (bis auf Isomorphie) die kleinste K enthaltende Galois-Erweiterung von k. Die Erweiterung $k \subset L$ heißt der *Galois-Abschluss* oder die *galoissche Hülle* von $k \subset K$. ♢

Wir kommen jetzt zu einem wichtigen Aspekt der Galois-Theorie, nämlich zur Beschreibung aller Zwischenkörper durch die Untergruppen der Galois-Gruppe. Sei $k \subset K$ galoissch. Wir erinnern uns an die Abbildungen aus Definition 11.4:

$$\begin{aligned} \mathcal{F}\colon \{U \subset \mathrm{Aut}(K/k) \mid U \text{ Untergruppe}\} &\longrightarrow \{L \mid L \text{ Zwischenkörper von } k \subset K\} \\ U &\longmapsto \mathcal{F}(U) = \{a \in K \mid \forall \gamma \in U\colon \gamma(a) = a\} \end{aligned}$$

und

$$\begin{aligned} \mathcal{U}\colon \{L \mid L \text{ Zwischenkörper von } k \subset K\} &\longrightarrow \{U \subset \mathrm{Aut}(K/k) \mid U \text{ Untergruppe}\} \\ L &\longmapsto \mathcal{U}(L) = \mathrm{Aut}(K/L)\,. \end{aligned}$$

Die wesentliche Aussage des nun folgenden Satzes ist, dass diese beiden Abbildungen zueinander invers sind.

SATZ Galois-Korrespondenz

∗ 12.11. **Satz.** *Sei $k \subset K$ eine endliche Galois-Erweiterung. Dann sind die oben definierten Abbildungen $\mathcal{F}$ und $\mathcal{U}$ inklusionsumkehrend und zueinander invers.*

Für einen Zwischenkörper L von $k \subset K$ gilt, dass $k \subset L$ genau dann galoissch ist, wenn $\mathcal{U}(L)$ Normalteiler in $\mathrm{Gal}(K/k)$ *ist.*

Inklusionsumkehrend heißt dabei, dass aus $U_1 \subset U_2$ die umgekehrte Inklusion $\mathcal{F}(U_1) \supset \mathcal{F}(U_2)$ folgt; entsprechend für $\mathcal{U}$.

Beweis. Dass $\mathcal{F}$ und $\mathcal{U}$ inklusionsumkehrend sind, folgt direkt aus den Definitionen. Wir zeigen, dass die Abbildungen zueinander invers sind. Für Untergruppen U und Zwischenkörper L gilt

$$U \subset \mathcal{U}(\mathcal{F}(U)) \qquad \text{und} \qquad L \subset \mathcal{F}(\mathcal{U}(L))$$

(denn jedes Element von U lässt $\mathcal{F}(U)$ elementweise fest und jedes Element von L wird von allen Elementen von $\mathcal{U}(L)$ fest gelassen). Nach Satz 12.9 ist $L \subset K$ für jedes L galoissch, also ist nach Satz 12.3 $\#\mathcal{U}(L) = [K : L]$. Nach Lemma 11.5 gilt $[K : \mathcal{F}(U)] = \#U$. Beides zusammen bedeutet

$$\#U = \#\mathcal{U}(\mathcal{F}(U)) \qquad \text{und} \qquad [K : L] = [K : \mathcal{F}(\mathcal{U}(L))]\,.$$

Zusammen mit der bereits bewiesenen Inklusion folgt

$$U = \mathcal{U}(\mathcal{F}(U)) \qquad \text{und} \qquad L = \mathcal{F}(\mathcal{U}(L))\,,$$

was zu zeigen war.

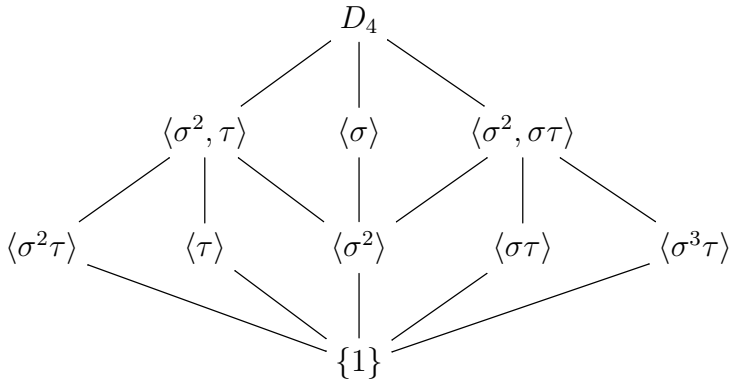
In Satz 12.9 hatten wir schon gesehen, dass aus „$k \subset L$ galoissch“ folgt, dass $\mathcal{U}(L) = \mathrm{Aut}(K/L)$ ein Normalteiler von $\mathrm{Gal}(K/k)$ ist. Für die umgekehrte Implikation überlegen wir Folgendes. Seien $\gamma, \phi \in \mathrm{Gal}(K/k)$. Dann gilt

$$\begin{aligned}
\phi \in \mathrm{Aut}(K/L) &\iff \forall a \in L\colon \phi(a) = a \\
&\iff \forall a \in L\colon \gamma(\phi(a)) = \gamma(a) \\
&\iff \forall a \in L\colon (\gamma\phi\gamma^{-1})(\gamma(a)) = \gamma(a) \\
&\iff \forall b \in \gamma(L)\colon (\gamma\phi\gamma^{-1})(b) = b \\
&\iff \gamma\phi\gamma^{-1} \in \mathrm{Aut}(K/\gamma(L))\,.
\end{aligned}$$

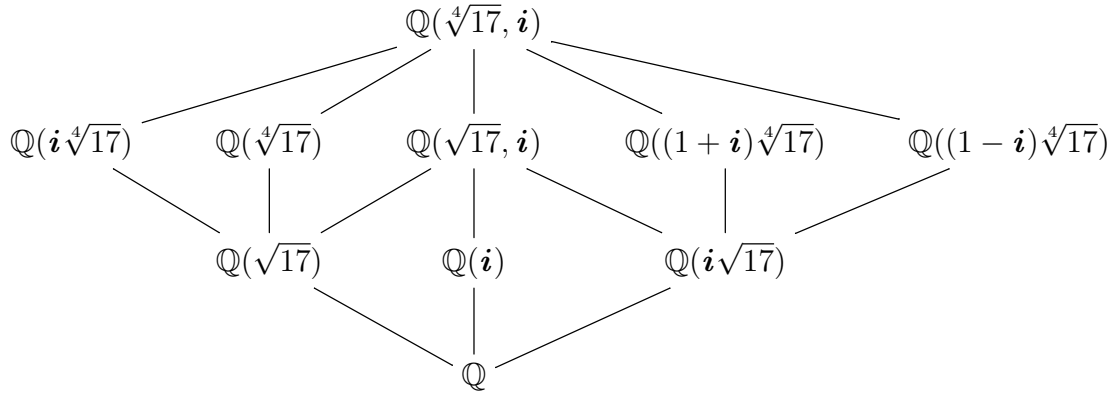
Das bedeutet $\mathrm{Aut}(K/\gamma(L)) = \gamma\,\mathrm{Aut}(K/L)\gamma^{-1} = \mathrm{Aut}(K/L)$, wobei wir benutzen, dass $\mathrm{Aut}(K/L)$ ein Normalteiler ist. Es folgt $\mathcal{U}(L) = \mathcal{U}(\gamma(L))$, nach dem ersten Teil des Satzes also $L = \gamma(L)$ (für alle $\gamma \in \mathrm{Gal}(K/k)$). Nach Satz 12.9 bedeutet das, dass $k \subset L$ galoissch ist. ❑

Da es relativ einfach ist, sich einen Überblick über die Untergruppen einer endlichen Gruppe zu verschaffen, erlaubt es uns dieser Satz, auch alle Zwischenkörper einer endlichen Galois-Erweiterung zu beschreiben.

12.12. **Beispiel.** Für die Galois-Erweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$ hatten wir in Beispiel 12.8 gezeigt, dass $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4$ ist. Die Untergruppen der Diedergruppe D_4 sind wie folgt: **BSP** $\mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$



Aus diesem „Untergruppenverband“ erhalten wir durch Spiegelung an einer horizontalen Achse den „Zwischenkörperverband“ von $\mathbb{Q} \subset K$:



(Um zu sehen, dass die Zwischenkörper wie angegeben sind, prüft man nach, dass die Erzeuger von der jeweiligen Untergruppe fest gelassen werden und dass der Körper den richtigen Grad hat.) Satz 12.11 sagt uns, dass es keine weiteren Zwischenkörper gibt.

Die nichttrivialen Normalteiler von $D_4 = \langle \sigma, \tau \rangle$ sind die Untergruppen $\langle \sigma \rangle$, $\langle \sigma^2, \tau \rangle$ und $\langle \sigma^2, \sigma\tau \rangle$ vom Index 2 und das Zentrum $\langle \sigma^2 \rangle$. Die einzigen (nichttrivialen) Zwischenkörper, die über $\mathbb{Q}$ galoissch sind, sind also $\mathbb{Q}(\boldsymbol{i})$, $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\boldsymbol{i}\sqrt{17})$ und $\mathbb{Q}(\sqrt{17}, \boldsymbol{i})$. ♣

13. Kreisteilungskörper und Kreisteilungspolynome

In diesem Abschnitt studieren wir eine Klasse von Körpererweiterungen (insbesondere von $\mathbb{Q}$), deren Galois-Gruppen wir explizit bestimmen können.

13.1. **Definition.** Seien k ein Körper und $n \in \mathbb{Z}_{>0}$ mit $\operatorname{char}(k) \nmid n$. Dann ist $X^n - 1 \in k[X]$ separabel. Der Zerfällungskörper K_n von $X^n - 1$ über k heißt der *n-te Kreisteilungskörper über k*. ♢

DEF Kreisteilungskörper

Man adjungiert also gerade die n-ten Einheitswurzeln zu k. Der Name „Kreisteilungskörper“ kommt daher, dass die n-ten Einheitswurzeln in $\mathbb{C}$ gerade die Ecken eines regelmäßigen, dem Einheitskreis einbeschriebenen, n-Ecks sind; sie teilen also den Einheitskreis in n gleiche Teile. (Siehe auch Beispiel 7.6.)

$X^n - 1$ ist separabel, weil die Ableitung nX^{n-1} nur bei null verschwindet (denn $n \neq 0$ in k), was aber keine Nullstelle von $X^n - 1$ ist. Also hat $X^n - 1$ nur einfache Nullstellen.

Die Nullstellen von $X^n - 1$ bilden die Untergruppe der n-ten Einheitswurzeln in $K_n^\times$. Sie hat Ordnung n (denn $X^n - 1$ hat n verschiedene Nullstellen in K_n) und ist nach Satz 4.9 zyklisch. Die Erzeuger, das sind also genau die Elemente der Ordnung n in $K_n^\times$, heißen *primitive n-te Einheitswurzeln*. Ein Element $\zeta \in K_n^\times$ ist genau dann eine primitive n-te Einheitswurzel, wenn $\zeta^n = 1$, aber $\zeta^m \neq 1$ für $1 \leq m < n$ ist. Alle primitiven n-ten Einheitswurzeln sind dann gegeben durch ζ^m mit $0 \leq m < n$ und $m \perp n$; es gibt also genau $\varphi(n)$ davon.

DEF primitive n-te Einheitswurzel

13.2. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$ und sei k ein Körper mit $\operatorname{char}(k) \nmid n$; sei weiter K_n der n-te Kreisteilungskörper über k. Dann ist $k \subset K_n$ eine Galois-Erweiterung. Sei $\zeta \in K_n$ eine primitive n-te Einheitswurzel. Dann ist $K_n = k(\zeta)$ und*

SATZ Kreisteilungskörper

$$\Phi\colon \operatorname{Gal}(K_n/k) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \gamma \longmapsto \log_\zeta \gamma(\zeta)$$

ist ein injektiver Gruppenhomomorphismus. Für $m \in \mathbb{Z}$ sei dabei

$$\log_\zeta \zeta^m = m + n\mathbb{Z}\,.$$

Insbesondere ist $[K_n : k]$ ein Teiler von $\varphi(n)$ und die Galoisgruppe $\operatorname{Gal}(K_n/k)$ ist abelsch.

Beweis. Als Zerfällungskörper des separablen Polynoms $X^n - 1$ ist K_n eine Galois-Erweiterung von k. Alle Nullstellen von $X^n - 1$ sind Potenzen von ζ; daraus folgt $K_n = k(\zeta)$. Sei $\gamma \in \operatorname{Gal}(K_n/k)$. Dann ist $\gamma(\zeta)$ wieder eine primitive n-te Einheitswurzel (denn $\operatorname{ord}(\gamma(\zeta)) = \operatorname{ord}(\zeta)$ als Elemente von $K_n^\times$), also ist $\gamma(\zeta) = \zeta^m$ mit $m \perp n$. Damit ist $\log_\zeta \gamma(\zeta) = m + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, und Φ ist als Abbildung wohldefiniert. Ist γ' ein weiteres Element von $\operatorname{Gal}(K_n/k)$, dann gilt $\gamma'(\zeta) = \zeta^{m'}$ für geeignetes m', und es folgt $(\gamma' \circ \gamma)(\zeta) = \gamma'(\zeta^m) = \gamma'(\zeta)^m = \zeta^{m'm}$, also gilt $\Phi(\gamma' \circ \gamma) = \Phi(\gamma')\Phi(\gamma)$. Damit ist Φ ein Gruppenhomomorphismus. Φ ist injektiv, denn $\ker(\Phi) = \{\mathrm{id}_{K_n}\}$: Gilt $\Phi(\gamma) = 1$, dann wird ζ von γ fest gelassen; wegen $K_n = k(\zeta)$ muss dann $\gamma = \mathrm{id}_{K_n}$ sein.

Es folgt, dass $\operatorname{Gal}(K_n/k)$ zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ isomorph und damit abelsch ist. Nach dem Satz von Lagrange haben wir dann auch

$$[K_n : k] = \#\operatorname{Gal}(K_n/k) \mid \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)\,. \qquad \square$$

Es stellt sich jetzt die Frage, ob Φ surjektiv sein kann, d.h., ob $[K_n : k] = \varphi(n)$ möglich ist. Wir werden zeigen, dass das für $k = \mathbb{Q}$ der Fall ist.

Zuerst definieren wir ein Polynom Φ_n kleineren Grades als n, sodass K_n auch Zerfällungskörper von Φ_n ist.

13.3. **Definition.** Das Polynom **DEF** Kreisteilungspolynom

$$\Phi_n = \prod_{\substack{\zeta\in\mathbb{C}\\ \text{pr. } n\text{-te EW}}} (X-\zeta) = \prod_{0\le m<n, m\perp n} (X - e^{2\pi i m/n}) \in \mathbb{C}[X]$$

heißt das n-te Kreisteilungspolynom. ♢

13.4. **Lemma.** *Das Kreisteilungspolynom hat folgende Eigenschaften:* **LEMMA** Eigensch. Kreisteilungspolynom

(1) $\prod_{d|n} \Phi_d = X^n - 1$ *(d durchläuft die positiven Teiler von n).*

(2) $\Phi_n \in \mathbb{Z}[X]$, *und* Φ_n *ist normiert.*

Beweis.

(1) Jede n-te Einheitswurzel $\zeta \in \mathbb{C}$ ist eine primitive d-te Einheitswurzel für genau einen Teiler d von n (nämlich $d = \#\langle\zeta\rangle = \operatorname{ord}(\zeta)$). Die Nullstellen von $X^n - 1$ sind also gerade die Nullstellen aller Polynome Φ_d mit $d \mid n$ zusammen. Daraus, und weil alle vorkommenden Polynome normiert sind, folgt die Produktformel.

(2) Dass Φ_n normiert ist, ist klar. Wir zeigen $\Phi_n \in \mathbb{Z}[X]$ durch Induktion. Für $n = 1$ ist $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Sei also $n > 1$. Nach Teil (1) gilt dann

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n, d<n} \Phi_d};$$

nach Induktionsvoraussetzung ist der Nenner ein normiertes Polynom mit ganzzahligen Koeffizienten. Polynomdivision zeigt, dass der Quotient auch ganzzahlige Koeffizienten hat. ❑

13.5. **Beispiele.** Die ersten paar Kreisteilungspolynome ergeben sich wie folgt: **BSP** Kreisteilungspolynome

$$\begin{aligned}
\Phi_1 &= X - 1\\
\Phi_2 &= X + 1\\
\Phi_3 &= X^2 + X + 1\\
\Phi_4 &= X^2 + 1\\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1\\
\Phi_6 &= X^2 - X + 1
\end{aligned}$$

Allgemein gilt für Primzahlen p:

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1$$

und für Zweierpotenzen 2^m mit $m \ge 1$:

$$\Phi_{2^m} = X^{2^{m-1}} + 1\,.$$

Diese Beispiele lassen vermuten, dass die Koeffizienten von Φ_n immer nur -1, 0 oder 1 sind. Das ist aber falsch: Die Koeffizienten werden sogar beliebig groß. Das kleinste n, für das ein Koeffizient vom Betrag > 1 auftritt, ist $n = 105$. ♣

Weil Φ_n Koeffizienten in $\mathbb{Z}$ hat, können wir für jeden Körper (oder sogar Ring) k das Kreisteilungspolynom $\Phi_{n,k} \in k[X]$ definieren, indem wir den kanonischen Homomorphismus $\mathbb{Z} \to k$ auf die Koeffizienten von Φ_n anwenden.

13.6. **Lemma.** *Seien k ein Körper und $n \in \mathbb{Z}_{>0}$ mit $\operatorname{char}(k) \nmid n$. Sei $\Phi_{n,k} \in k[X]$ das n-te Kreisteilungspolynom über k. Dann ist der n-te Kreisteilungskörper K_n über k der Zerfällungskörper von $\Phi_{n,k}$, und $[K_n : k] = \varphi(n)$ gilt genau dann, wenn $\Phi_{n,k}$ irreduzibel ist.* **LEMMA**

Beweis. Sei ζ eine Nullstelle von $\Phi_{n,k}$. Dann ist ζ eine primitive n-te Einheitswurzel, also gilt $K_n = k(\zeta)$, und Letzterer ist der Zerfällungskörper von $\Phi_{n,k}$. Das Minimalpolynom f von ζ über k ist ein Teiler von $\Phi_{n,k}$; es gilt

$$[K_n : k] = \deg(f) \leq \deg(\Phi_{n,k}) = \varphi(n)$$

mit Gleichheit genau dann, wenn $f = \Phi_{n,k}$ ist, also wenn $\Phi_{n,k}$ irreduzibel ist. ❑

Es bleibt zu zeigen, dass Φ_n über $\mathbb{Q}$ irreduzibel ist. Der entscheidende Beweisschritt wird im folgenden Lemma getan.

13.7. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$, sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ. Sei weiter p eine Primzahl mit $p \nmid n$. Dann ist $f(\zeta^p) = 0$.* **LEMMA**

Beweis. Wir nehmen an, die Behauptung sei falsch. Da ζ^p eine Nullstelle von Φ_n ist, können wir $\Phi_n = fg$ schreiben mit $g \in \mathbb{Q}[X]$ normiert, sodass $g(\zeta^p) = 0$ ist. Da ζ eine Nullstelle von $g(X^p)$ ist, gilt $f \mid g(X^p)$. Aus dem Lemma von Gauß folgt, dass f und g ganzzahlige Koeffizienten haben. Wir können also die Gleichung $\Phi_n = fg$ modulo p betrachten: $\Phi_{n,\mathbb{F}_p} = \bar{f}\bar{g}$ in $\mathbb{F}_p[X]$, und $\bar{f}$ teilt $\bar{g}(X^p) = \bar{g}^p$ (hier verwenden wir $a^p = a$ für $a \in \mathbb{F}_p$ und $(x+y)^p = x^p + y^p$ in Charakteristik p). Auf der anderen Seite sind $\bar{f}$ und $\bar{g}$ teilerfremd, da $X^n - 1$ auch über $\mathbb{F}_p$ nur einfache Nullstellen hat. Das ist der gewünschte Widerspruch. ❑

* 13.8. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Dann ist $\Phi_n \in \mathbb{Q}[X]$ irreduzibel. Für den n-ten Kreisteilungskörper K_n über $\mathbb{Q}$ gilt $[K_n : \mathbb{Q}] = \varphi(n)$ und $\operatorname{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.* **SATZ** Kreisteilungspolynom irreduzibel

Beweis. Sei f ein irreduzibler Faktor von Φ_n. Sei $\zeta \in \mathbb{C}$ eine Nullstelle von f; dann ist ζ eine primitive n-te Einheitswurzel mit Minimalpolynom f. Nach Lemma 13.7 ist dann für jede Primzahl $p \nmid n$ auch ζ^p eine Nullstelle von f. Durch nochmalige Anwendung des Lemmas sieht man, dass dann auch ζ^{pq} für beliebige Primzahlen $p, q \nmid n$ eine Nullstelle von f ist; das kann dann auf beliebige Produkte von n nicht teilenden Primzahlen ausgedehnt werden. Da jede primitive n-te Einheitswurzel die Form ζ^m hat mit $0 \leq m < n$ und $m \perp n$ und da jedes solche m als Produkt von Primzahlen $p \nmid n$ geschrieben werden kann, sind *alle* primitiven n-ten Einheitswurzeln Nullstellen von f. Dann muss aber $f = \Phi_n$ sein; insbesondere ist Φ_n selbst irreduzibel.

Die restlichen Aussagen folgen aus Satz 13.2 und Lemma 13.6. ❑

Als Anwendung wollen wir die Zahlen $n \in \mathbb{Z}_{>0}$ charakterisieren, für die das reguläre n-Eck mit Zirkel und Lineal konstruierbar ist. Diese Charakterisierung wird durch den folgenden Satz von Gauß gegeben:

SATZ Konstruierbarkeit des regulären n-Ecks

$*$ 13.9. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n) = 2^m$ ist für ein $m \geq 0$. Das bedeutet konkret, dass n die Form $n = 2^k p_1 p_2 \cdots p_l$ hat mit $k \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, p_2, \ldots, p_l$.*

Zur Erinnerung: Eine Fermatsche Primzahl ist eine Primzahl der Form 2^m+1. Dabei muss m selbst eine Potenz von 2 sein. Die folgenden Fermatschen Primzahlen sind bekannt:

$$F_0 = 2^{2^0} + 1 = 3, \quad F_1 = 2^{2^1} + 1 = 5, \quad F_2 = 2^{2^2} + 1 = 17,$$
$$F_3 = 2^{2^3} + 1 = 257, \quad F_4 = 2^{2^4} + 1 = 65\,537\,.$$

Wir hatten bereits in Folgerung 9.7 gesehen, dass die Konstruierbarkeit des regulären p-Ecks für eine Primzahl p impliziert, dass p eine Fermatsche Primzahl sein muss. Satz 13.9 ist im Wesentlichen die Umkehrung dieser Aussage.

Beweis. Die Konstruierbarkeit des regulären n-Ecks ist äquivalent zur Konstruierbarkeit von $\cos\frac{2\pi}{n}$. Sei $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$; ζ_n ist eine primitive n-te Einheitswurzel. Es ist

$$(X - \zeta_n)(X - \zeta_n^{-1}) = X^2 - 2(\cos\tfrac{2\pi}{n})X + 1 \in \mathbb{Q}(\cos\tfrac{2\pi}{n})[X]\,,$$

also ist $\mathbb{Q}(\zeta_n)$ eine höchstens quadratische Erweiterung von $\mathbb{Q}(\cos\frac{2\pi}{n})$. Es gilt also

$$\exists m' \in \mathbb{Z}_{\geq 0}\colon [\mathbb{Q}(\cos\tfrac{2\pi}{n}) : \mathbb{Q}] = 2^{m'} \iff \exists m \in \mathbb{Z}_{\geq 0}\colon [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^m$$

(mit $m = m'$ oder $m = m'+1$). Nach Satz 9.9 ist $\cos\frac{2\pi}{n}$ genau dann konstruierbar, wenn $\cos\frac{2\pi}{n}$ in einem Körper liegt, der aus $\mathbb{Q}$ durch sukzessive quadratische Erweiterungen erhalten werden kann. Notwendig dafür ist, dass $[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}]$ eine Potenz von 2 ist. Nach der obigen Überlegung ist also $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^m$ für geeignetes $m \in \mathbb{Z}_{\geq 0}$ eine notwendige Bedingung für die Konstruierbarkeit des regulären n-Ecks. Es bleibt zu zeigen, dass die Bedingung auch hinreichend ist. Sei also $\varphi(n) = 2^m$. Die Gruppe $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ ist abelsch von der Ordnung 2^m. Man findet dann (etwa mit Hilfe des Klassifikationssatzes für endliche abelsche Gruppen) leicht eine Folge

$$\{\mathrm{id}\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_m = \Gamma$$

von Untergruppen mit $(G_k : G_{k-1}) = 2$ für alle $k = 1, 2, \ldots, m$. Nach dem Satz 12.11 über die Galois-Korrespondenz gehört dazu eine Kette von Körpererweiterungen

$$\mathbb{Q} = L_m \subset L_{m-1} \subset \ldots \subset L_1 \subset L_0 = \mathbb{Q}(\zeta_n) \ni \cos\tfrac{2\pi}{n}$$

(mit $L_k = \mathcal{F}(G_k)$), sodass $[L_{k-1} : L_k] = 2$ ist. Das zeigt, dass $\cos\frac{2\pi}{n}$ konstruierbar ist.

Die Charakterisierung der n mit $\varphi(n) = 2^m$ ergibt sich so: Sei $n = 2^r p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ die Primfaktorzerlegung von n (mit $r \geq 0$, paarweise verschiedenen ungeraden Primzahlen p_j und $e_j \geq 1$). Dann ist

$$\begin{aligned}\varphi(n) &= \varphi(2^r)\varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_l^{e_l}) \\ &= 2^{\max\{0, r-1\}} p_1^{e_1-1}(p_1-1) p_2^{e_2-1}(p_2-1) \cdots p_l^{e_l-1}(p_l-1)\,.\end{aligned}$$

Das ist genau dann eine Zweierpotenz, wenn das auf jeden Faktor zutrifft. Das bedeutet gerade $e_j = 1$ für alle j und $p_j = 2^{m_j} + 1$, also dass die p_j Fermatsche Primzahlen sind. ❑

14. Die Diskriminante

Wir dehnen den Begriff der Galois-Gruppe auf Polynome aus:

∗ 14.1. **Definition.** Seien k ein Körper und $f \in k[X]$ ein separables Polynom. Sei weiter K ein Zerfällungskörper von f über k; dann ist $k \subset K$ eine Galois-Erweiterung. Die Galois-Gruppe $\mathrm{Gal}(K/k)$ heißt die *Galois-Gruppe von f über k* und wird auch $\mathrm{Gal}(f/k)$ geschrieben. ♢

DEF Galois-Gruppe eines Polynoms

Wir halten zunächst einmal folgende Beobachtung fest:

14.2. **Lemma.** *In der Situation von Definition 14.1 sei $N_f \subset K$ die Menge der Nullstellen von f. Dann definiert*

$$\mathrm{Gal}(f/k) \longrightarrow S(N_f)\,, \quad \sigma \longmapsto \sigma|_{N_f}$$

einen injektiven Gruppenhomomorphismus. Ist $\#N_f = n$, dann können wir $S(N_f)$ durch Nummerierung der Nullstellen mit S_n identifizieren; damit ist $\mathrm{Gal}(f/k)$ *isomorph zu einer Untergruppe der S_n, und diese Untergruppe ist bis auf Konjugation eindeutig bestimmt. Ist f irreduzibel, dann operiert diese Untergruppe transitiv auf N_f bzw. $\{1, 2, \ldots, n\}$ und ihre Ordnung ist durch n teilbar.*

LEMMA Galois-Gruppe als Untergr. von S_n

Beweis. Da K Zerfällungskörper von f ist, gilt $K = k(N_f)$. Es folgt, dass jeder Automorphismus $\sigma \in \mathrm{Aut}(K/k) = \mathrm{Gal}(f/k)$ durch $\sigma|_{N_f}$ eindeutig bestimmt ist. Außerdem muss jeder Automorphismus von $k \subset K$ jede Nullstelle von f wieder auf eine Nullstelle von f abbilden; damit ist $\sigma|_{N_f} \in S(N_f)$. Beides zusammen zeigt, dass die Abbildung wohldefiniert und injektiv ist; dass sie ein Gruppenhomomorphismus ist, ist klar. Eine Bijektion $\nu\colon N_f \to \{1, 2, \ldots, n\}$ (also eine Nummerierung der Nullstellen) induziert einen Isomorphismus $S(N_f) \to S_n$, $\sigma \mapsto \nu \circ \sigma \circ \nu^{-1}$; durch Nachschalten dieses Isomorphismus erhalten wir eine Einbettung $\mathrm{Gal}(f/k) \to S_n$. Eine Änderung der Nummerierung bewirkt das Nachschalten eines inneren Automorphismus von S_n. Es folgt, dass die Bilder von $\mathrm{Gal}(f/k)$ unter allen diesen Isomorphismen gerade eine Konjugationsklasse von Untergruppen der S_n durchlaufen. Dass $\mathrm{Gal}(K/k)$ auf den Nullstellen in K jedes über k irreduziblen Polynoms transitiv operiert, folgt aus Lemma 11.5. Für die letzte Aussage sei $\alpha \in K$ eine Nullstelle von f. Dann ist $k \subset k(\alpha) \subset K$ und $[k(\alpha) : k] = \deg(f) = n$; die Teilbarkeit folgt dann aus dem Gradsatz und aus $\#\,\mathrm{Gal}(f/k) = [K : k]$. ❑

Unser Ziel in diesem Abschnitt wird sein, ein Kriterium zu entwickeln, mit dessen Hilfe wir entscheiden können, ob die Galois-Gruppe $\mathrm{Gal}(f/k)$ (bzw. ihr Bild in der S_n) in der A_n enthalten ist. Als motivierendes Beispiel betrachten wir den Fall $\deg(f) = 2$. Sei also $f = x^2 + px + q \in k[x]$. Im Fall $\mathrm{char}(k) \neq 2$ haben wir die wohlbekannte Lösungsformel für quadratische Gleichungen:

$$x^2 + px + q = 0 \quad \Longrightarrow \quad x = \frac{-p \pm \sqrt{p^2 - 4q}}{2}\,.$$

Hat f keine mehrfache Nullstelle, dann ist $p^2 - 4q \neq 0$, und aus obiger Formel folgt

$$\begin{aligned} p^2 - 4q \text{ ist ein Quadrat in } k &\iff f \text{ zerfällt über } k \text{ in Linearfaktoren} \\ &\iff \mathrm{Gal}(f/k) = A_2 = \{\mathrm{id}\}\,. \end{aligned}$$

Im anderen Fall ist $\mathrm{Gal}(f/k) = S_2$. Der Ausdruck $p^2 - 4q$ ist als die *Diskriminante* von f bekannt.

Wir wollen das jetzt auf Polynome höheren Grades verallgemeinern. Dazu betrachten wir zunächst ein (separables) Polynom vom Grad 3:

$$f(x) = x^3 + ax^2 + bx + c\,.$$

Wir nehmen an, dass das Polynom irreduzibel ist, denn sonst könnten wir es faktorisieren, und dann hätten wir es mit Polynomen kleineren Grades zu tun. Wir nummerieren die Nullstellen von f in einem Zerfällungskörper und identifizieren so $\mathrm{Gal}(f/k)$ mit einer Untergruppe der S_3. Aus Lemma 14.2 folgt dann, dass

$$\mathrm{Gal}(f/k) = S_3 \qquad \text{oder} \qquad \mathrm{Gal}(f/k) = A_3$$

ist. Wie können wir entscheiden, welche der beiden Möglichkeiten zutrifft?

Im Fall $\mathrm{Gal}(f/k) = S_3$ muss es einen Zwischenkörper $k \subset L \subset K$ geben, der quadratisch über k ist, nämlich $L = \mathcal{F}(A_3)$. Wenn $\mathrm{char}(k) \neq 2$ ist, dann ist $L = k(\sqrt{d})$ für ein $d \in k$, das kein Quadrat ist. Da A_3 ein Normalteiler von S_3 ist, ist $k \subset L$ galoissch (das ist auch so klar, da jede quadratische Körpererweiterung in Charakteristik $\neq 2$ galoissch ist) mit Galois-Gruppe S_3/A_3. Das heißt konkret, dass für $\sigma \in S_3 = \mathrm{Gal}(f/k)$ gilt

$$\sigma \in A_3 \Rightarrow \sigma(\sqrt{d}) = \sqrt{d} \qquad \text{und} \qquad \sigma \in S_3 \setminus A_3 \Rightarrow \sigma(\sqrt{d}) = -\sqrt{d}\,.$$

(Im zweiten Fall wird $\sqrt{d}$ nicht fixiert, muss also auf die andere Nullstelle von $x^2 - d$ abgebildet werden.) Man kann das als

$$\sigma(\sqrt{d}) = \varepsilon(\sigma)\sqrt{d}$$

zusammenfassen; dabei ist $\varepsilon(\sigma)$ das Signum der Permutation σ.

Umgekehrt gilt: Ist $\delta \in K$ mit $\sigma(\delta) = \varepsilon(\sigma)\delta$ für alle $\sigma \in S_3$, dann ist $\delta^2 \in k$ und $L = k(\delta)$. Denn $\sigma(\delta^2) = \sigma(\delta)^2 = \varepsilon(\sigma)^2\delta^2 = \delta^2$ für alle $\sigma \in S_3$, also ist $\delta^2 \in \mathcal{F}(S_3) = k$. Da δ von allen $\sigma \in A_3$ fest gelassen wird, gilt entsprechend $\delta \in \mathcal{F}(A_3) = L$. Aus $\delta \in L \setminus k$ folgt $L = k(\delta)$.

Wir werden jetzt ein solches Element δ aus den Nullstellen von f zusammenbauen:

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\,.$$

Eine Permutation σ der drei Nullstellen vertauscht die drei Faktoren und ändert möglicherweise bei einigen von ihnen das Vorzeichen:

$$\frac{\sigma(\delta)}{\delta} = (-1)^{\#\{(i,j)\,|\,1\le i<j\le 3,\,\sigma(i)>\sigma(j)\}} = \varepsilon(\sigma)\,,$$

also hat δ die gewünschte Eigenschaft.

$$\mathrm{disc}(f) = d = \delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in k^\times$$

heißt die *Diskriminante* von f. Wir haben dann das folgende Ergebnis:

14.3. **Satz.** *Sei k ein Körper mit $\mathrm{char}(k) \neq 2$ und sei $f \in k[x]$ irreduzibel und separabel mit $\deg(f) = 3$. Ist $\mathrm{disc}(f) \in k^\times$ ein Quadrat in k, dann ist $\mathrm{Gal}(f/k) = A_3$, anderenfalls ist $\mathrm{Gal}(f/k) = S_3$.*

SATZ $\mathrm{Gal}(f/k) = A_3$ oder S_3

Beweis. Ist $\mathrm{disc}(f) = \delta^2$ kein Quadrat in k, dann ist $\delta \notin k$, also gibt es den quadratischen Zwischenkörper $L = k(\delta)$, und es folgt $2 = [L : k] \mid [K : k] = \#\,\mathrm{Gal}(f/k)$, also muss $\mathrm{Gal}(f/k) = S_3$ sein.

Sei jetzt $\mathrm{disc}(f)$ ein Quadrat, also $\delta \in k$. Sei $\sigma \in \mathrm{Gal}(f/k) \subset S_3$. Nach dem oben Gesagten gilt einerseits $\sigma(\delta) = \varepsilon(\sigma)\delta$, andererseits wegen $\delta \in k$ aber auch $\sigma(\delta) = \delta$.

Beides zusammen impliziert $\varepsilon(\sigma) = 1$, also $\sigma \in A_3$. Es folgt $A_3 \subset \mathrm{Gal}(f/k) \subset A_3$, also $\mathrm{Gal}(f/k) = A_3$. ❑

Aus der Tatsache, dass $\mathrm{disc}(f)$ in jedem Körper enthalten ist, der die Koeffizienten von f enthält, folgt, dass $\mathrm{disc}(f)$ durch diese ausgedrückt werden kann. Um diesen Ausdruck möglichst einfach zu halten, vereinfachen wir unser Polynom f ein wenig. Dafür nehmen wir an, dass $\mathrm{char}(k) \neq 3$ ist. Ähnlich wie man ein Polynom vom Grad 2 durch „quadratisches Ergänzen“ vereinfachen kann, können wir dann durch „kubisches Ergänzen“ den Koeffizienten von x^2 zum Verschwinden bringen. Sei $f = x^3 + ax^2 + bx + c$. Dann ist

$$f\big(x - \tfrac{1}{3}a\big) = (x^3 - ax^2 + \ldots) + ax^2 + \ldots = x^3 + px + q$$

mit Koeffizienten p und q, die gewisse Ausdrücke in a, b und c sind. Die Diskriminante ändert sich dadurch nicht, da wir alle Nullstellen um denselben Betrag $a/3$ verschieben, sodass die Differenzen gleich bleiben.

LEMMA Diskriminante für Grad 3

14.4. **Lemma.** *Für $f = x^3 + px + q$ gilt*

$$\mathrm{disc}(f) = -4p^3 - 27q^2\,.$$

Beweis. Aus $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ folgt

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p, \qquad \alpha_1\alpha_2\alpha_3 = -q\,.$$

Die behauptete Gleichheit folgt dann durch eine einfache, aber umständliche Rechnung. ❑

Die Aussage von Satz 14.3 lässt sich verallgemeinern. Dazu definieren wir die Diskriminante für ein beliebiges normiertes Polynom.

* **DEF** Diskriminante

14.5. **Definition.** Seien k ein Körper und $f \in k[x]$ ein normiertes Polynom vom Grad $n \geq 1$. Sei K ein Zerfällungskörper von f über k; es gelte

$$f = \prod_{j=1}^{n}(x - \alpha_j) \in K[x]\,.$$

Dann ist die *Diskriminante* von f definiert als

$$\mathrm{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2\,. \qquad \diamondsuit$$

LEMMA Diskriminante und mehrfache Nullstellen

14.6. **Lemma.** *Seien k ein Körper und $f \in k[x]$ ein normiertes Polynom vom Grad n. Dann gilt:*

(1) $\mathrm{disc}(f) \in k$.

(2) $\mathrm{disc}(f) \neq 0$ *genau dann, wenn f nur einfache Nullstellen hat; insbesondere ist f dann separabel.*

Beweis. Der zweite Teil folgt direkt aus der Definition der Diskriminante. Wenn $\mathrm{disc}(f) = 0$ ist, dann ist $\mathrm{disc}(f) \in k$. Sei also jetzt $\mathrm{disc}(f) \neq 0$. Dann ist f separabel, also ist $k \subset K$ eine Galois-Erweiterung, wobei K ein Zerfällungskörper von f über k ist. Die Elemente von $\mathrm{Gal}(f/k) = \mathrm{Aut}(K/k)$ permutieren die Nullstellen α_j von f und damit die Faktoren in der Definition von $\mathrm{disc}(f)$. Es folgt $\mathrm{disc}(f) \in \mathcal{F}(\mathrm{Aut}(K/k)) = k$. ❑

Man kann sogar zeigen, dass die Diskriminante ein Polynom mit ganzzahligen Koeffizienten in den Koeffizienten $a_0, a_1, \ldots, a_{n-1}$ von

$$f = x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0$$

ist. Genauer gilt

$$\operatorname{disc}(f) = (-1)^{\binom{n}{2}} \begin{vmatrix} 1 & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & 1 & a_{n-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} & \cdots & a_1 & a_0 \\ n & (n-1)a_{n-1} & (n-2)a_{n-2} & \cdots & a_1 & 0 & \cdots & 0 \\ 0 & n & (n-1)a_{n-1} & \cdots & 2a_2 & a_1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & n & (n-1)a_{n-1} & \cdots & 2a_2 & a_1 \end{vmatrix} .$$

Das ist eine $(2n-1)$-reihige Determinante, in deren ersten $n-1$ Zeilen die Koeffizienten von f stehen (in jeder Zeile gegenüber der vorigen um einen Platz nach rechts verschoben) und in deren letzten n Zeilen die Koeffizienten der Ableitung f' stehen. Zum Beispiel erhalten wir für $f = x^3 + px + q$:

$$\begin{aligned} \operatorname{disc}(f) &= -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 0 & 0 & -2p & -3q & 0 \\ 0 & 0 & 0 & -2p & -3q \\ 0 & 0 & 3 & 0 & p \end{vmatrix} \\ &= -\big((-2p)(-2p)p + (-3q)(-3q)q\big) = -4p^3 - 27q^2 . \end{aligned}$$

Für $f = x^2 + px + q$ erhalten wir die bekannte Formel

$$\operatorname{disc}(f) = -\begin{vmatrix} 1 & p & q \\ 2 & p & 0 \\ 0 & 2 & p \end{vmatrix} = p^2 - 4q .$$

Die Verallgemeinerung unseres Satzes 14.3 lautet jetzt wie folgt.

* 14.7. **Satz.** *Sei k ein Körper mit $\operatorname{char}(k) \neq 2$ und sei $f \in k[x]$ ein normiertes Polynom vom Grad $n \geq 1$ mit $\operatorname{disc}(f) \neq 0$. Dann ist f separabel und es gilt für die Galois-Gruppe $\operatorname{Gal}(f/k) \subset S_n$:* **SATZ** $\operatorname{Gal} \subset A_n$

$$\operatorname{Gal}(f/k) \subset A_n \iff \operatorname{disc}(f) \text{ ist ein Quadrat in } k.$$

Beweis. Dass aus $\operatorname{disc}(f) \neq 0$ folgt, dass f separabel ist, hatten wir bereits in Lemma 14.6 gesehen. Sei K ein Zerfällungskörper von f über k und sei $\delta \in K$ mit $\delta^2 = \operatorname{disc}(f)$, also etwa

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j) ,$$

wenn $\alpha_1, \ldots, \alpha_n \in K$ die Nullstellen von f sind. Für $\sigma \in \operatorname{Gal}(f/k) \subset S_n$ gilt dann wie vorher $\sigma(\delta) = \varepsilon(\sigma)\delta$. Ist $\operatorname{disc}(f)$ ein Quadrat in k, dann ist $\delta \in k$, also $\sigma(\delta) = \delta$, und es folgt $\varepsilon(\sigma) = 1$ (man beachte $1 \neq -1$ wegen $\operatorname{char}(k) \neq 2$), also $\sigma \in A_n$. Ist $\delta \notin k$, dann ist $L = k(\delta)$ ein Zwischenkörper vom Grad 2 in $k \subset K$ und es gilt $L = \mathcal{F}(\operatorname{Gal}(f/k) \cap A_n)$, denn

$$\sigma|_L = \mathrm{id}_L \iff \sigma(\delta) = \delta \iff \varepsilon(\sigma) = 1 .$$

Dann muss $\operatorname{Gal}(f/k) \cap A_n$ eine echte Untergruppe von $\operatorname{Gal}(f/k)$ sein, also folgt $\operatorname{Gal}(f/k) \not\subset A_n$. ❑

15. Lösungsformeln für Gleichungen vom Grad 3 und 4

In diesem Abschnitt wollen wir analog zur bekannten Lösungsformel für quadratische Gleichungen Lösungsformeln für Gleichungen vom Grad 3 und 4 entwickeln.

Für ein irreduzibles Polynom $f = x^3 + px + q \in k[x]$ vom Grad 3 (dabei nehmen wir $\mathrm{char}(k) \neq 2, 3$ an) haben wir nach den Ergebnissen des letzten Abschnitts den Körperturm

$$k \subset L = k(\sqrt{\mathrm{disc}(f)}) \subset K\,,$$

wobei K der Zerfällungskörper von f ist; die Körpererweiterung $L \subset K$ ist galoissch mit Galois-Gruppe $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Können wir die Elemente von K (also insbesondere die Nullstellen von f) durch geeignete dritte Wurzeln von Elementen von L ausdrücken? Dazu nehmen wir erst einmal an, dass k eine primitive dritte Einheitswurzel enthält, also ein Element ω mit $\omega^3 = 1$, aber $\omega \neq 1$ (d.h., ω erfüllt die Gleichung $\omega^2 + \omega + 1 = 0$). Sei $\sigma \in \mathrm{Gal}(K/L)$ ein Erzeuger. Dann ist $\sigma\colon K \to K$ ein L-linearer Endomorphismus des L-Vektorraums K, und σ hat Ordnung 3. Das Minimalpolynom von σ als L-linearer Endomorphismus ist dann ein Teiler von $x^3 - 1$, also ist σ diagonalisierbar (hier brauchen wir $\mathrm{char}(k) \neq 3$) und die Eigenwerte von σ sind in $\{1, \omega, \omega^2\}$. Der Eigenraum zum Eigenwert 1 ist L mit Dimension 1. Es muss also einen weiteren Eigenwert ω oder ω^2 geben. Tatsächlich treten beide auf: Ist z.B. $\xi \in K$ mit $\sigma(\xi) = \omega^2\xi$, dann ist $\sigma(\xi^2) = \sigma(\xi)^2 = (\omega^2\xi)^2 = \omega\xi^2$.

Sei $\alpha \in K$ ein Eigenvektor zum Eigenwert ω; es gelte also $\sigma(\alpha) = \omega\alpha$. Dann ist $a = \alpha^3 \in L$, denn $\sigma(\alpha^3) = (\omega\alpha)^3 = \omega^3\alpha^3 = \alpha^3$, und es folgt $K = L(\alpha) = L(\sqrt[3]{a})$ (denn $\alpha \in K \setminus L$).

Wenn k keine primitive dritte Einheitswurzel enthält, dann adjungieren wir eine, ersetzen k also durch $k(\omega) = k(\sqrt{-3})$. (Es ist ja $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.) Um eine explizite Formel zu bekommen, müssen wir noch herausfinden, wie wir das Element a durch $\sqrt{\mathrm{disc}(f)}$ und die Koeffizienten von f ausdrücken können. Seien dazu $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von f in K. Wir können die Nummerierung so wählen, dass $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ und $\sigma(\alpha_3) = \alpha_1$ ist. Dann gilt für $\alpha = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$:

$$\sigma(\alpha) = \alpha_2 + \omega^2\alpha_3 + \omega\alpha_1 = \omega(\omega^2\alpha_2 + \omega\alpha_3 + \alpha_1) = \omega\alpha\,,$$

also liegt α im richtigen Eigenraum. Wir machen noch ein paar vorbereitende Rechnungen. Sei dazu

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = (\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) - (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2)$$

eine Quadratwurzel aus $\mathrm{disc}(f)$. Aus einem Koeffizientenvergleich

$$x^3 + px + q = f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

folgt

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad \text{und} \quad \alpha_1\alpha_2\alpha_3 = -q$$

und damit

$$\begin{aligned}(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2)& \\ = (\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - 3\alpha_1\alpha_2\alpha_3& \\ = 3q&\end{aligned}$$

und

$$\begin{aligned}\alpha_1^3+\alpha_2^3+\alpha_3^3 &\\ &= (\alpha_1+\alpha_2+\alpha_3)^3 - 3(\alpha_1+\alpha_2+\alpha_3)(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) + 3\alpha_1\alpha_2\alpha_3\\ &= -3q\,.\end{aligned}$$

Wir haben dann

$$\begin{aligned}a = \alpha^3 &= (\alpha_1+\omega^2\alpha_2+\omega\alpha_3)^3\\ &= \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3\\ &\qquad + 3\omega(\alpha_1\alpha_2^2+\alpha_3\alpha_1^2+\alpha_2\alpha_3^2) + 3\omega^2(\alpha_1^2\alpha_2+\alpha_3^2\alpha_1+\alpha_2^2\alpha_3)\\ &= -3q-6q+\frac{3}{2}\omega(3q-\delta)+\frac{3}{2}\omega^2(3q+\delta)\\ &= -\frac{27}{2}q-\frac{3\sqrt{-3}}{2}\delta\\ &= 27\Big(-\frac{q}{2}-\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}\Big)\end{aligned}$$

(bei geeigneter Wahl der Quadratwurzel). Mit $\bar\alpha = \alpha_1+\omega\alpha_2+\omega^2\alpha_3$ und $\bar a = \bar\alpha^3$ erhalten wir analog

$$\bar a = 27\Big(-\frac{q}{2}+\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}\Big)\,.$$

Dabei gilt

$$\begin{aligned}\alpha\bar\alpha &= \alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_1\alpha_3-\alpha_2\alpha_3\\ &= (\alpha_1+\alpha_2+\alpha_3)^2-3(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)\\ &= -3p\,.\end{aligned}$$

N. Tartaglia (1499?–1557)

Wegen

$$\alpha_1 = \frac{1}{3}\big((\alpha_1+\alpha_2+\alpha_3)+\alpha+\bar\alpha\big) = \frac{1}{3}(\alpha+\bar\alpha)$$

ist

$$\alpha_1 = \sqrt[3]{-\frac{q}{2}+\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}}\,;$$

dabei sind die dritten Wurzeln so zu wählen, dass ihr Produkt $-p/3$ ist. Wir halten fest (α und $\bar\alpha$ im Satz entsprechen $\bar\alpha/3$ und $\alpha/3$ in der Überlegung oben):

SATZ Lösungsformel für kubische Gleichungen

15.1. **Satz.** *Sei k ein Körper mit $\operatorname{char}(k)\neq 2,3$ und sei $f = x^3+px+q \in k[x]$. Sei $k\subset K$ eine Körpererweiterung, die eine primitive dritte Einheitswurzel ω und die Nullstellen von f enthält.*

Sei weiter $d = (p/3)^3+(q/2)^2 = -\operatorname{disc}(f)/(4\cdot 27)$ und $\delta = \sqrt{d}\in K$ eine Quadratwurzel von d. Seien $\alpha = \sqrt[3]{-q/2+\delta}$, $\bar\alpha = \sqrt[3]{-q/2-\delta}\in K$ dritte Wurzeln mit $\alpha\bar\alpha = -p/3$. Dann sind die Nullstellen von f in K gegeben durch

$$\alpha_1 = \alpha+\bar\alpha, \qquad \alpha_2 = \omega\alpha+\omega^2\bar\alpha \qquad \textit{und} \qquad \alpha_3 = \omega^2\alpha+\omega\bar\alpha\,.$$

G. Cardano (1501–1576)

Diese Formeln gehen auf Tartaglia und del Ferro (ca. 1515) zurück. Cardano veröffentlichte sie als Erster (1545), nachdem er unveröffentlichte Notizen von del Ferro dazu gesehen hatte, obwohl Tartaglia ihm die Formeln nur unter der Bedingung verraten hatte, dass er sie geheim hält.

Beweis. Dass $\delta, \alpha, \bar\alpha \in K$ sind, folgt aus den vorhergehenden Überlegungen (und in jedem Fall könnte man K geeignet wählen). Man rechnet nun nach:

$$(\alpha\bar\alpha)^3 = \alpha^3\bar\alpha^3 = \Big(-\frac{q}{2}+\delta\Big)\Big(-\frac{q}{2}-\delta\Big) = \Big(\frac{q}{2}\Big)^2 - \Big(\Big(\frac{p}{3}\Big)^3 + \Big(\frac{q}{2}\Big)^2\Big) = \Big(-\frac{p}{3}\Big)^3,$$

also können α und $\bar\alpha$ wie angegeben gewählt werden. Es gilt dann:

$$\alpha_1+\alpha_2+\alpha_3 = (1+\omega+\omega^2)\alpha + (1+\omega^2+\omega)\bar\alpha = 0\,,$$

$$\begin{aligned}\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= (\omega+\omega^2+1)\alpha^2 + (\omega^2+\omega+1)\bar\alpha^2 \\ &\quad + (\omega^2+\omega+\omega+\omega^2+\omega^2+\omega)\alpha\bar\alpha \\ &= -3\alpha\bar\alpha = p\,,\end{aligned}$$

$$\begin{aligned}\alpha_1\alpha_2\alpha_3 &= \alpha^3+\bar\alpha^3 + (\omega^2+\omega+1)\alpha^2\bar\alpha + (1+\omega^2+\omega)\alpha\bar\alpha^2 \\ &= \alpha^3+\bar\alpha^3 = -\frac{q}{2}+\delta-\frac{q}{2}-\delta = -q\,.\end{aligned}$$

Die Behauptung folgt jetzt durch Koeffizientenvergleich in

$$f = x^3+px+q = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\,. \qquad \square$$

Für diesen Beweis haben wir die Galois-Theorie nicht gebraucht, wohl aber dafür, die Formel herzuleiten.

15.2. **Beispiel.** Seien $k=\mathbb{Q}$, $K=\mathbb{C}$ und $f = x^3-3x+1 \in \mathbb{Q}[x]$. Wir haben also $p=-3$ und $q=1$. Das ergibt **BSP** x^3-3x+1

$$d = (p/3)^3 + (q/2)^2 = -1+1/4 = -3/4\,,$$

also $\delta = \sqrt{-3}/2$. Für α haben wir $\alpha = \sqrt[3]{-1/2+\sqrt{-3}/2} = \sqrt[3]{\omega}$ (mit $\omega = e^{2\pi i/3} = (-1+\sqrt{-3})/2$ wie oben), also können wir $\alpha = \zeta_9 = e^{2\pi i/9}$ nehmen; das ergibt dann $\bar\alpha = 1/\alpha = \zeta_9^{-1}$. Die Nullstellen von f sind demnach

$$\begin{aligned}\zeta_9 + \zeta_9^{-1} &= 2\cos\frac{2\pi}{9}\,, \\ \omega\zeta_9 + \omega^2\zeta_9^{-1} = \zeta_9^4 + \zeta_9^{-4} &= 2\cos\frac{8\pi}{9} \qquad \text{und} \\ \omega^2\zeta_9 + \omega\zeta_9^{-1} = \zeta_9^{-2} + \zeta_9^2 &= 2\cos\frac{4\pi}{9}\,. \qquad \clubsuit\end{aligned}$$

In diesem Beispiel mussten wir mit echt komplexen Zahlen rechnen (δ ist rein imaginär), obwohl die Nullstellen alle reell sind. Das ist kein Zufall.

15.3. **Lemma.** *Sei $f \in \mathbb{R}[x]$ normiert mit $\deg(f)=3$. Dann hat f entweder genau eine oder genau drei reelle Nullstellen (mit Vielfachheit gerechnet). Der erste Fall tritt ein, wenn $\operatorname{disc}(f)<0$ ist, der zweite Fall, wenn $\operatorname{disc}(f)\ge 0$ ist.* **LEMMA** kubische Polynome über $\mathbb{R}$

Beweis. Seien $\alpha_1,\alpha_2,\alpha_3 \in \mathbb{C}$ die Nullstellen von f. Es ist

$$\operatorname{disc}(f) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2\,.$$

Sind die Nullstellen reell, dann ist $\operatorname{disc}(f)$ Quadrat einer reellen Zahl, also ≥ 0. Sind nicht alle Nullstellen reell, dann gibt es eine reelle Nullstelle α und ein Paar zueinander konjugierter echt komplexer Nullstellen β und $\bar\beta$. Dann ist

$$\operatorname{disc}(f) = \big((\alpha-\beta)(\alpha-\bar\beta)\big)^2(\beta-\bar\beta)^2 < 0\,,$$

denn der erste Faktor ist das Quadrat der von null verschiedenen reellen Zahl $\alpha^2 - 2\alpha \operatorname{Re}\beta + |\beta|^2$ und der zweite Faktor ist $-4(\operatorname{Im}\beta)^2 < 0$. ❑

Da wir für die Lösungsformel die Quadratwurzel aus $-\operatorname{disc}(f)/108$ brauchen, ist diese rein imaginär genau dann, wenn die Nullstellen von f alle reell sind. Diese Beobachtung ('casus irreducibilis' genannt) hat übrigens in der historischen Entwicklung letztendlich zur Anerkennung der komplexen Zahlen geführt, nicht etwa der Wunsch, einer Gleichung wie $x^2+1=0$ eine Lösung zu verschaffen. Denn man konnte ja akzeptieren, dass so eine Gleichung keine (reelle) Lösung hat, während im kubischen Fall drei reelle Lösungen existieren konnten, zu deren Berechnung man aber die komplexen Zahlen benötigte.

Für die Lösung einer Gleichung vom Grad 4 gehen wir erst einmal davon aus, dass das zugehörige Polynom Galois-Gruppe S_4 hat. In der S_4 gibt es als Normalteiler die *Kleinsche Vierergruppe* $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Es ist $S_4/V_4 \cong S_3$ (S_4 operiert auf den drei nichttrivialen Elementen von V_4 durch Konjugation, das liefert einen Homomorphismus in die S_3 mit Kern V_4). Der entsprechende Zwischenkörper ist dann galoissch über dem Grundkörper mit Galois-Gruppe S_3; man sollte ihn also durch Lösen einer geeigneten kubischen Gleichung erhalten können. Die verbleibende Erweiterung bis zum Zerfällungskörper hat dann Galois-Gruppe $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und ist durch Quadratwurzeln erzeugbar. Die Nullstellen der kubischen Gleichung sollten also gerade den Fixkörper von V_4 erzeugen. Wie bei quadratischen und kubischen Gleichungen können wir durch geeignete Verschiebung erreichen, dass das Polynom vierten Grades, dessen Nullstellen wir berechnen wollen, die Form $f = x^4 + px^2 + qx + r$ hat. Wir bezeichnen die Nullstellen von f mit $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Dann sind die Elemente

$$\beta = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4), \quad \beta' = (\alpha_1+\alpha_3)(\alpha_2+\alpha_4) \quad \text{und} \quad \beta'' = (\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$$

in $\mathcal{F}(V_4)$, denn sie sind unter den Permutationen in V_4 invariant. Aus der Relation $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$ folgt

$$(\alpha_1+\alpha_2)^2 = -\beta, \qquad (\alpha_1+\alpha_3)^2 = -\beta' \qquad \text{und} \qquad (\alpha_1+\alpha_4)^2 = -\beta'',$$

sodass mit geeigneten Quadratwurzeln gilt

$$\alpha_1 = \frac{1}{2}\big((\alpha_1+\alpha_2)+(\alpha_1+\alpha_3)+(\alpha_1+\alpha_4)\big) = \frac{1}{2}(\sqrt{-\beta}+\sqrt{-\beta'}+\sqrt{-\beta''}).$$

Man kann folgende Beziehung nachrechnen:

$$(x-\beta)(x-\beta')(x-\beta'') = x^3 - 2px^2 + (p^2-4r)x + q^2.$$

Außerdem ist $(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)(\alpha_1+\alpha_4) = -q$. Wir fassen zusammen:

SATZ Lösungsformel für Gleichungen vom Grad 4

15.4. **Satz.** *Seien k ein Körper mit $\operatorname{char}(k) \neq 2, 3$ und $f = x^4+px^2+qx+r \in k[x]$. Sei $k \subset K$ eine Körpererweiterung, die eine primitive dritte Einheitswurzel ω und die Nullstellen von f enthält.*

Sei $g = x^3 - 2px^2 + (p^2-4r)x + q^2$. Dann zerfällt g über K in Linearfaktoren. Seien $\beta, \beta', \beta'' \in K$ die Nullstellen von g (die man mit Satz 15.1 bestimmen kann). Seien weiter $\gamma = \sqrt{-\beta} \in K$, $\gamma' = \sqrt{-\beta'}, \gamma'' = \sqrt{-\beta''} \in K$ Quadratwurzeln, sodass $\gamma\gamma'\gamma'' = -q$ ist. Dann sind die Nullstellen von f gegeben durch

$$\begin{aligned}
\alpha_1 &= \tfrac{1}{2}(\gamma+\gamma'+\gamma''),\\
\alpha_2 &= \tfrac{1}{2}(\gamma-\gamma'-\gamma''),\\
\alpha_3 &= \tfrac{1}{2}(-\gamma+\gamma'-\gamma'') \qquad \textit{und}\\
\alpha_4 &= \tfrac{1}{2}(-\gamma-\gamma'+\gamma'').
\end{aligned}$$

Die Formeln gehen auf Ferrari (ca. 1545) zurück.

Beweis. Man rechnet die relevanten Beziehungen nach, analog zum Beweis von Satz 15.1. ❑

15.5. **Definition.** Das Polynom g heißt die *kubische Resolvente* von f. Es gilt $\operatorname{disc}(g) = \operatorname{disc}(f)$, denn es ist $\beta - \beta' = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$; die anderen Differenzen sind analog darstellbar. ♢

DEF kubische Resolvente

15.6. **Beispiel.** Seien $k = \mathbb{Q}$, $K = \mathbb{C}$ und $f = x^4 - 10x^2 + 1$. Die kubische Resolvente ist $g = x^3 + 20x^2 + 96x = x(x+8)(x+12)$. Ihre Nullstellen sind $\beta = 0$, $\beta' = -8$, $\beta'' = -12$. Wir können also $\gamma = 0$, $\gamma' = 2\sqrt{2}$, $\gamma'' = 2\sqrt{3}$ wählen und erhalten die Nullstellen

$$\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}, \quad \sqrt{2} - \sqrt{3} \quad \text{und} \quad -\sqrt{2} + \sqrt{3}\,.$$

In diesem Fall könnte man die Lösungen auch durch sukzessives Lösen zweier quadratischer Gleichungen finden: $x^2 = 5 \pm 2\sqrt{6}$, also sind die Lösungen $\pm\sqrt{5 \pm 2\sqrt{6}}$. Tatsächlich ist $(\sqrt{2} \pm \sqrt{3})^2 = 5 \pm 2\sqrt{6}$; der Satz liefert die einfachere Form direkt. ♣

BSP $x^4 - 10x^2 + 1$

Die kubische Resolvente erlaubt es uns auch, zwischen den verschiedenen Möglichkeiten für die Galois-Gruppe eines irreduziblen Polynoms vom Grad 4 zu unterscheiden. Grundsätzlich gilt folgende Aussage:

15.7. **Lemma.** *Sei k ein Körper und sei $f \in k[x]$ ein normiertes Polynom ohne mehrfache Nullstellen in seinem Zerfällungskörper. f ist genau dann irreduzibel, wenn die Galois-Gruppe* $\operatorname{Gal}(f/k)$ *auf den Nullstellen von f transitiv operiert.*

LEMMA Kriterium für irreduzibel

Beweis. Sei K ein Zerfällungskörper von f über k. Dann ist $\operatorname{Gal}(f/k) = \operatorname{Aut}(K/k)$. Wenn diese Gruppe transitiv auf den Nullstellen von f operiert, dann ist f nach Lemma 11.5 irreduzibel. Ist die Operation nicht transitiv, dann führt jede Bahn wiederum nach Lemma 11.5 zu einem nichttrivialen Teiler von f in $k[x]$, also ist in diesem Fall f nicht irreduzibel. ❑

Etwas genauer gilt also, dass die Bahnen der Operation von $\operatorname{Gal}(f/k)$ auf den Nullstellen von f in K genau den irreduziblen Faktoren von f entsprechen.

Die transitiv operierenden Untergruppen der S_4 sind (bis auf Konjugation)

(1) die zyklische Gruppe $C_4 = \langle (1\,2\,3\,4) \rangle$,

(2) die Kleinsche Vierergruppe V_4,

(3) die Diedergruppe $D_4 = \langle (1\,2\,3\,4), (1\,3) \rangle$,

(4) die alternierende Gruppe A_4 und

(5) die symmetrische Gruppe S_4 selbst.

Davon sind die V_4 und die A_4 in der A_4 enthalten, die übrigen Gruppen nicht (denn ein Viererzykel ist eine ungerade Permutation). Da wir über die Diskriminante feststellen können, ob die Galois-Gruppe in der A_4 enthalten ist, müssen wir noch zwischen V_4 und A_4 bzw. zwischen C_4, D_4 und S_4 unterscheiden. Dazu betrachten wir die Anzahl der Nullstellen der kubischen Resolvente in k. Wenn eine Nullstelle, zum Beispiel $\beta' = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$, in k liegt, dann muss jedes Element $\sigma \in \operatorname{Gal}(f/k) \subset S_4$ dieses Element fest lassen, was dazu äquivalent

ist, dass σ die Partition $\{\{1,3\},\{2,4\}\}$ von $\{1,2,3,4\}$ fest lässt. Das bedeutet $\mathrm{Gal}(f/K) \subset D_4$. (Beachte, dass die kubische Resolvente g keine mehrfachen Nullstellen hat, denn $\mathrm{disc}(g) = \mathrm{disc}(f) \neq 0$.) Sind alle drei Nullstellen von g in k, dann folgt entsprechend $\mathrm{Gal}(f/k) \subset V_4$.

SATZ Galois-Gruppen Grad 4

15.8. **Satz.** *Sei k ein Körper mit $\mathrm{char}(k) \neq 2$ und sei $f \in k[x]$ irreduzibel vom Grad 4. Wir setzen $d = \mathrm{disc}(f) \neq 0$. Seien weiter g die kubische Resolvente von f und n die Anzahl der Nullstellen von g in k. Dann ergibt sich die Galois-Gruppe $\mathrm{Gal}(f/k)$ aus folgender Tabelle (dabei heißt „$d = \square$“, dass d ein Quadrat in k ist):*

	$n=0$	$n=1$	$n=3$
$d = \square$	A_4	$-$	V_4
$d \neq \square$	S_4	C_4, D_4	$-$

Die Unterscheidung zwischen C_4 und D_4 ist etwas schwieriger; wir werden das hier nicht ausführen. Man kann aber im Fall „C_4 oder D_4“ geeignete Ausdrücke D in den Koeffizienten von f und der Nullstelle von g in k konstruieren, sodass (wenn $D \neq 0$ ist, anderenfalls muss man einen anderen Ausdruck verwenden) man genau dann im Fall C_4 ist, wenn D ein Quadrat in k ist. In den Beispielen unten werden wir statt dessen ad-hoc-Argumente verwenden.

Ist $b \in k$ die einzige Nullstelle von g in k und hat f die Form $f = x^4 + px^2 + qx + r$, dann sei $D = 2b^2p - 3bp^2 - 4br - 3q^2$. Ist $D \neq 0$, dann ist die Galois-Gruppe genau dann C_4, wenn D ein Quadrat in k ist. Dieser Ausdruck ergibt sich (mit $b = \beta'$) aus

$$\left((\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_4 + \alpha_4^2\alpha_1) - (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_4^2 + \alpha_4\alpha_1^2)\right)^2 .$$

Die Elemente der C_4 lassen beide Terme in der Differenz fest, während die zusätzlichen Elemente der D_4 die beiden Terme vertauschen. Die Galois-Gruppe ist also genau dann die C_4, wenn die Differenz in k ist, jedenfalls dann, wenn diese Differenz nicht verschwindet.

Bevor wir uns Beispiele anschauen, überlegen wir noch Folgendes:

Sei $f \in k[x]$ vom Grad 4 mit kubsicher Resolvente g. Ist g irreduzibel, dann operiert $G = \mathrm{Gal}(f/k)$ transitiv auf den Nullstellen von g. Damit ist das Bild von G unter $G \hookrightarrow S_4 \to S_3$ mindestens die A_3. Ist f nicht irreduzibel, dann muss f eine Nullstelle in k haben, denn im verbleibenden Fall, dass f Produkt zweier irreduzibler Faktoren vom Grad 2 ist, ist $G \subset \langle (1\ 2), (3\ 4) \rangle$ (wobei wir die Nullstellen so nummeriert haben, dass die ersten beiden zu einem der irreduziblen Faktoren gehören) und damit $\#G$ ein Teiler von 4, sodass das Bild von G in S_3 nicht durch 3 teilbare Ordnung haben kann. Also:

Ist g irreduzibel und hat f keine Nullstelle in k, dann ist auch f irreduzibel.

BSP Grad 4: Galois-Gruppen

15.9. **Beispiele.** Wie üblich sei $k = \mathbb{Q}$.

(1) $f = x^4 + x + 1$. Dann ist f irreduzibel nach dem Reduktionskriterium mit $p = 2$ (denn $x^4 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$) und $g = x^3 - 4x + 1$ mit

$$\mathrm{disc}(f) = \mathrm{disc}(g) = -4(-4)^3 - 27 \cdot 1^2 = 256 - 27 = 229 .$$

g ist irreduzibel (da ohne rationale Nullstelle; nur ± 1 kommen infrage) und $\mathrm{disc}(f)$ ist kein Quadrat, also ist $\mathrm{Gal}(f/\mathbb{Q}) = S_4$.

(2) $f = x^4 + 3x^2 - 7x + 4$. Dann ist $g = x^3 - 6x^2 - 7x + 49$. Zur Berechnung der Diskriminante betrachten wir $g(x+2) = x^3 - 19x + 19$; es ergibt sich

$$\mathrm{disc}(f) = \mathrm{disc}(g) = -4(-19)^3 - 27 \cdot 19^2 = 17689 = 133^2 .$$

Außerdem ist $g(x+2)$ irreduzibel nach Eisenstein mit $p = 19$. f hat keine rationale Nullstelle (nur ± 1, ± 2, ± 4 kommen infrage), also ist f irreduzibel und $\mathrm{Gal}(f/\mathbb{Q}) = A_4$.

(3) $f = x^4 - 2$; f ist irreduzibel nach Eisenstein mit $p = 2$. Die kubische Resolvente ist $g = x^3 + 8x = x(x^2 + 8)$; der zweite Faktor ist irreduzibel, also ist die Galois-Gruppe C_4 oder D_4. Wir wissen, dass f zwei reelle und ein Paar konjugiert komplexe Nullstellen hat. Die komplexe Konjugation liefert ein Element von $\mathrm{Gal}(f/\mathbb{Q})$, das genau zwei Nullstellen vertauscht. Damit kann $\mathrm{Gal}(f/\mathbb{Q})$ nicht C_4 sein, also ist $\mathrm{Gal}(f/\mathbb{Q}) = D_4$.

(4) $f = x^4 + 1$. Es ist $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$; dieses Polynom ist irreduzibel nach Eisenstein mit $p = 2$. Es ist $g = x^3 - 4x = x(x-2)(x+2)$ mit drei rationalen Nullstellen, also ist die Galois-Gruppe V_4.

(5) $f = x^4 + x^3 + x^2 + x + 1$. Die Nullstellen von f sind gerade die fünften Einheitswurzeln außer 1, also $\zeta, \zeta^2, \zeta^3, \zeta^4$ mit $\zeta = e^{2\pi i/5}$. Sei $K = \mathbb{Q}(\zeta) \subset \mathbb{C}$ der Zerfällungskörper von f. Wir wissen bereits, dass $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$ ist. Unabhängig davon könnten wir auch wie folgt argumentieren. Wir bestimmen die kubische Resolvente. Zunächst eliminieren wir den Term mit x^3 aus f:

$$f(x - \tfrac{1}{4}) = x^4 + \frac{5}{8}x^2 + \frac{5}{8}x + \frac{205}{256};$$

damit ist die Resolvente

$$g = x^3 - \frac{5}{4}x^2 - \frac{45}{16}x + \frac{25}{64}.$$

Mögliche rationale Nullstellen von g erfüllen $64x^3 - 80x^2 - 180x + 25 = 0$, der Zähler muss also ein Teiler von 25 und der Nenner ein Teiler von 64 sein. Man findet die Nullstelle $-5/4$ und damit

$$g = \Big(x + \frac{5}{4}\Big)\Big(x^2 - \frac{5}{2}x + \frac{5}{16}\Big).$$

Die Diskriminante des zweiten Faktors ist $(-5/2)^2 - 4 \cdot 5/16 = 5$ und damit kein Quadrat. Also hat g genau eine Nullstelle, und die Galois-Gruppe von f muss C_4 oder D_4 sein. Da $K = \mathbb{Q}(\zeta)$ ist, gilt $\#\,\mathrm{Gal}(f/\mathbb{Q}) = \#\,\mathrm{Gal}(K/\mathbb{Q}) = \deg(f) = 4$, also ist $\mathrm{Gal}(f/\mathbb{Q}) = C_4$. ♣

16. Radikalerweiterungen und auflösbare Gruppen

Wir wollen jetzt der Frage nachgehen, ob es auch für Polynome vom Grad ≥ 5 Lösungsformeln der gleichen Art gibt wie für Polynome vom Grad 2, 3 oder 4. Dazu formalisieren wir zunächst einmal, was eine „Lösungsformel der gleichen Art“ sein soll. Die Idee ist, dass wir außer den vier Grundrechenarten auch das Ziehen von beliebigen n-ten Wurzeln zulassen wollen. Das führt auf den folgenden Begriff:

* 16.1. **Definition.** Sei k ein Körper. Eine *Radikalerweiterung* von k ist eine Körpererweiterung $k \subset K$, sodass es einen Turm von Körpererweiterungen **DEF** Radikalerweiterung

$$k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$$

gibt mit $K \subset K_m$ und der Eigenschaft, dass es für jedes $j \in \{1, 2, \ldots, m\}$ ein Element $a_j \in K_{j-1}$ und eine Zahl $n_j \in \mathbb{Z}_{>0}$ mit $\mathrm{char}(k) \nmid n_j$ gibt, sodass K_j der Zerfällungskörper von $X^{n_j} - a_j$ über K_{j-1} ist. ♢

Man erhält also K_j aus K_{j-1} durch Adjunktion aller n_j-ten Wurzeln aus a_j. Das bedeutet gerade, dass sich alle Elemente von K durch einen *Radikalausdruck* über k darstellen lassen, also eine Formel der oben beschriebenen Art, in die Elemente von k eingesetzt werden.

Das ist analog zur Definition von konstruierbaren Elementen: Dort sind alle $n_j = 2$. Wir kommen darauf am Ende dieses Abschnitts zurück.

Die Ergebnisse aus Abschnitt 15 lassen sich dann so interpretieren, dass die Nullstellen eines Polynoms vom Grad höchstens 4 über k in einer Radikalerweiterung von k enthalten sind.

Unser Ziel in diesem Abschnitt wird es sein, das folgende Ergebnis zu beweisen:

* 16.2. **Satz.** *Sei $k \subset K$ eine endliche Körpererweiterung mit $\mathrm{char}(k) = 0$. K ist genau dann eine Radikalerweiterung von k, wenn es eine endliche Galois-Erweiterung $k \subset L$ gibt, deren Galois-Gruppe auflösbar ist, und sodass $K \subset L$ ist.* **SATZ** Charakterisierung von Radikalerweiterungen

Was ist eine auflösbare Gruppe?

* 16.3. **Definition.** Eine Gruppe G heißt *auflösbar*, wenn es eine Kette von Untergruppen **DEF** auflösbare Gruppe

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

in G gibt, sodass für alle $j \in \{1, 2, \ldots, n\}$ die Untergruppe G_{j-1} ein Normalteiler von G_j mit abelscher Faktorgruppe G_j/G_{j-1} ist. ♢

Es ist nicht schwer zu sehen, dass Untergruppen und Faktorgruppen von auflösbaren Gruppen wieder auflösbar sind. Eine Umkehrung gilt ebenfalls.

16.4. **Lemma.** *Seien G eine auflösbare Gruppe und $U \leq G$ eine Untergruppe. Dann ist U ebenfalls auflösbar.* **LEMMA** Untergruppe auflösbar

Beweis. Sei

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

eine Kette von Untergruppen wie in Definition 16.3. Für $j \in \{0, 1, \ldots, n\}$ sei $U_j = U \cap G_j$. Dann ist

$$\{1\} = U_0 \leq U_1 \leq \ldots \leq U_n = U$$

eine Kette von Untergruppen von U. Für gegebenes $j \geq 1$ betrachten wir den Gruppenhomomorphismus $\phi_j \colon U_j = U \cap G_j \to G_j \to G_j/G_{j-1}$. Sein Kern ist $U_j \cap G_{j-1} = U \cap G_{j-1} = U_{j-1}$, also ist $U_{j-1} \triangleleft U_j$, und wir bekommen nach dem Homomorphiesatz für Gruppen EZAS.14.6 einen *injektiven* Gruppenhomomorphismus $U_j/U_{j-1} \to G_j/G_{j-1}$. Da G_j/G_{j-1} nach Voraussetzung abelsch ist, gilt das auch für U_j/U_{j-1}, denn diese Gruppe ist zu einer Untergruppe von G_j/G_{j-1} isomorph. Damit ist U auflösbar. ❑

16.5. **Lemma.** *Seien G eine Gruppe und $N \triangleleft G$ ein Normalteiler. G ist genau dann auflösbar, wenn sowohl N als auch die Faktorgruppe G/N auflösbar sind.*

LEMMA Faktorgruppe auflösbar

Beweis. "⇒": Sei G auflösbar. Nach Lemma 16.4 ist dann auch N auflösbar. Um zu zeigen, dass G/N auflösbar ist, sei $\phi \colon G \to G/N$ der kanonische Epimorphismus, und

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

eine Kette von Untergruppen wie in Definition 16.3. Wir setzen $Q_j = \phi(G_j) \leq G/N$; dann ist

$$\{1_{G/N}\} = Q_0 \leq Q_1 \leq \ldots \leq Q_n = G/N$$

eine Kette von Untergruppen von G/N mit $Q_{j-1} \triangleleft Q_j$ für alle $j \in \{1, 2, \ldots, n\}$. (Dass Q_{j-1} ein Normalteiler von Q_j ist, folgt daraus, dass ein surjektiver Gruppenhomomorphismus Normalteiler auf Normalteiler abbildet; vgl. EZAS.14.3.) Der Kern von $G_j \xrightarrow{\phi} Q_j \to Q_j/Q_{j-1}$ enthält G_{j-1}, also erhalten wir einen surjektiven Gruppenhomomorphismus $G_j/G_{j-1} \to Q_j/Q_{j-1}$ (EZAS.14.6). Damit ist Q_j/Q_{j-1} (als Faktorgruppe einer abelschen Gruppe) abelsch, und G/N ist auflösbar.

"⇐": Seien N und G/N auflösbar, und seien

$$\{1\} = N_0 \leq N_1 \leq \ldots \leq N_m = N \quad \text{und} \quad \{1_{G/N}\} = Q_0 \leq Q_1 \leq \ldots \leq Q_n = G/N$$

Ketten von Untergruppen wie in Definition 16.3. Für $j \in \{0, 1, \ldots, m\}$ sei $G_j = N_j$ und für $k \in \{0, 1, \ldots, n\}$ sei $G_{m+k} = \phi^{-1}(Q_k)$, wobei $\phi \colon G \to G/N$ der kanonische Epimorphismus ist (beide Definitionen von $G_m = N$ stimmen überein). Dann ist

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_{m-1} \leq G_m = N \leq G_{m+1} \leq \ldots \leq G_{m+n} = G$$

eine Kette von Untergruppen von G mit $G_{j-1} \triangleleft G_j$ für alle $j \geq 1$ (für $j > m$ verwenden wir, dass Urbilder von Normalteilern unter Gruppenhomomorphismen wieder Normalteiler sind; vgl. EZAS.14.3), und es gilt $G_j/G_{j-1} = N_j/N_{j-1}$ für $j \leq m$ und $G_j/G_{j-1} \cong Q_{j-m}/Q_{j-m-1}$ für $j > m$; alle Faktorgruppen sind nach Voraussetzung abelsch, also ist G auflösbar. ❑

16.6. **Lemma.** *Ist G endlich, dann kann man in Definition 16.3 sogar verlangen, dass die Faktorgruppen G_j/G_{j-1} zyklisch (und von Primzahlordnung) sind.*

LEMMA zyklische Faktorgruppen

Beweis. Durch Induktion über $\#G$. Die Aussage ist klar für $\#G = 1$. Sei G also nichttrivial und auflösbar und sei $G_{n-1} \triangleleft G_n = G$ der letzte Schritt in der Kette von Untergruppen aus Definition 16.3; dabei sei ohne Einschränkung $G_{n-1} \neq G$. Nach Induktionsvoraussetzung (angewandt auf die nach Lemma 16.4 auflösbare Gruppe G_{n-1}) können wir annehmen, dass die Faktorgruppen G_j/G_{j-1} zyklisch von Primzahlordnung sind für $j < n$. Wenn G/G_{n-1} ebenfalls zyklisch von Primzahlordnung ist, dann sind wir fertig. Anderenfalls gibt es eine echte Untergruppe $Q \subset G/G_{n-1}$ von Primzahlordnung (nach dem 1. Satz von Sylow 3.5 oder dem Klassifikationssatz für endliche abelsche Gruppen EZAS.15.14). Da G/G_{n-1}

abelsch ist, ist Q Normalteiler. Nach Induktionsvoraussetzung, angewandt auf $(G/G_{n-1})/Q$ (beachte $\#(G/G_{n-1})/Q < \#G/G_{n-1} \leq \#G$), gibt es eine Kette

$$\{1_{(G/G_{n-1})/Q}\} \leq Q'_1 \leq \ldots \leq Q'_m = (G/G_{n-1})/Q$$

mit Faktorgruppen, die zyklisch von Primzahlordnung sind. Wie im Beweis von Lemma 16.5 können wir diese Kette zunächst zu einer Kette

$$\{1_{G/G_{n-1}}\} \leq Q \leq Q_1 \leq \ldots \leq G/G_{n-1}$$

für G/G_{n-1} hochheben und dann mit der Kette für G_{n-1} zu einer Kette für G mit den gewünschten Eigenschaften zusammensetzen. ❑

In einer Kette von Untergruppen, von denen jede ein Normalteiler der folgenden ist, können wir offensichtlich annehmen, dass die Untergruppen alle verschieden sind. Ist eine der Faktorgruppen G_j/G_{j-1} nicht einfach, dann können wir die Kette „verfeinern“, indem wir $\phi^{-1}(N)$ zwischen G_{j-1} und G_j einfügen, wobei $N \triangleleft G_j/G_{j-1}$ ein nichttrivialer Normalteiler und $\phi\colon G_j \to G_j/G_{j-1}$ der kanonische Epimorphismus ist. Eine solche Kette, die nicht weiter verfeinert werden kann, bei der also jede Faktorgruppe einfach ist, heißt eine *Kompositionsreihe* von G; die Faktorgruppen heißen die *Kompositionsfaktoren* von G. Nach dem Satz von Jordan-Hölder sind die Kompositionsfaktoren (für eine endliche Gruppe) bis auf Reihenfolge und Isomorphie eindeutig bestimmt (das kann man als ein Analogon des Satzes über die eindeutige Primfaktorzerlegung von natürlichen Zahlen betrachten). Eine endliche Gruppe ist also genau dann auflösbar, wenn ihre Kompositionsfaktoren abelsch sind.

Es gibt recht allgemeine Sätze, die sagen, dass bestimmte endliche Gruppen auflösbar sind:

16.7. **Satz.** *Sei G eine endliche Gruppe der Ordnung $\#G = p^a q^b$, wobei p und q Primzahlen sind. Dann ist G auflösbar.*

SATZ
Satz von Burnside

16.8. **Satz.** *Jede endliche Gruppe ungerader Ordnung ist auflösbar.*

SATZ
Satz von Feit und Thompson

Die Beweise sind im Rahmen dieser Vorlesung nicht zu leisten. (Der Originalbeweis von Feit und Thompson von 1963 hat 350 Seiten. 2012 wurde dieser Beweis mit maschineller Unterstützung formal verifiziert, ein Projekt, das eine Reihe von Mathematikern etliche Jahre beschäftigt hat.)

Die Existenz der Lösungsformeln für Gleichungen von Grad ≤ 4 hängt mit folgender Tatsache zusammen:

16.9. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Die symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist.*

SATZ
Auflösbarkeit von S_n

Beweis. Die Gruppen S_1 und S_2 sind abelsch und daher trivialerweise auflösbar. Die Gruppe S_3 enthält den abelschen Normalteiler A_3 mit abelscher Faktorgruppe $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, ist also ebenfalls auflösbar. In der S_4 haben wir die Kette $\{\mathrm{id}\} \leq V_4 \leq A_4 \leq S_4$ mit abelschen Faktorgruppen $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$, $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ und $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Sei jetzt $n \geq 5$. Dann ist die Untergruppe $A_n \leq S_n$ eine nicht-abelsche einfache Gruppe. Wäre S_n auflösbar, dann müsste nach Lemma 16.4 auch A_n auflösbar sein. Eine einfache Gruppe hat aber (definitionsgemäß) keine nicht-trivialen Normalteiler, also könnte die Länge der Untergruppen-Kette nur 1 sein. Die Faktorgruppe $A_n/\{\mathrm{id}\} \cong A_n$ ist aber nicht abelsch, also kann die Bedingung für Auflösbarkeit nicht erfüllt werden. ❑

Tatsächlich haben wir die im Beweis für $n = 3$ und $n = 4$ angegebenen Ketten von Untergruppen für die Konstruktion der Lösungsformeln benutzt.

N.H. Abel
1802–1829

Aus Satz 16.9 und Satz 16.2 folgt, dass die Nullstellen eines irreduziblen Polynoms vom Grad $n \geq 5$, dessen Galois-Gruppe S_n (oder A_n) ist, nicht durch einen Radikalausdruck gegeben werden können. Dieses Resultat (Satz von Abel-Ruffini) wurde sehr viel später erhalten als die expliziten Formeln für niedrigere Grade, die ja aus dem 16. Jahrhundert stammen. Wie in vielen anderen ähnlichen Fällen auch liegt das daran, dass ein Unmöglichkeitsbeweis oft sehr viel schwieriger zu führen ist als der Nachweis, dass ein Objekt mit gewissen Eigenschaften (wie die expliziten Lösungsformeln) existiert: Auf die Lösungsformeln kann man mit genügend Intuition und Hartnäckigkeit kommen (und ihre Gültigkeit kann man dann ohne allzu große Schwierigkeiten beweisen), während man für den Beweis ihrer Nicht-Existenz erst einmal die Theorie der Radikalerweiterungen (und dafür wiederum die Galois-Theorie) aufbauen muss.

Ein wesentlicher Schritt im Beweis von Satz 16.2 wird durch das folgende Lemma geleistet.

LEMMA
zyklische
Galois-Gruppe

16.10. **Lemma.** *Seien k ein Körper und $n \in \mathbb{Z}_{>0}$ mit $\operatorname{char}(k) \nmid n$; k enthalte eine primitive n-te Einheitswurzel ζ.*

(1) *Seien $a \in k$ und K der Zerfällungskörper von $X^n - a$ über k. Dann ist $k \subset K$ galoissch mit zyklischer Galois-Gruppe, deren Ordnung ein Teiler von n ist.*

(2) *Sei $k \subset K$ eine galoissche Körpererweiterung mit zyklischer Galois-Gruppe der Ordnung n. Dann gibt es $a \in k$, sodass K der Zerfällungskörper von $X^n - a$ über k ist.*

Beweis.

(1) (Siehe Aufgabe (1) auf dem letzten Übungsblatt.)
Sei $\alpha \in K$ mit $\alpha^n = a$ eine Nullstelle von $X^n - a$. Dann sind alle Nullstellen von der Form $\zeta^j \alpha$ mit $j \in \{0, 1, \ldots, n-1\}$. Wegen $\zeta \in k$ ist $K = k(\alpha)$. Ein Automorphismus $\gamma \in \operatorname{Gal}(K/k)$ ist dann durch $\gamma(\alpha)$ festgelegt. Wir definieren $\Phi\colon \operatorname{Gal}(K/k) \to \mathbb{Z}/n\mathbb{Z}$, $\gamma \mapsto j + n\mathbb{Z}$, wobei $\gamma(\alpha) = \zeta^j \alpha$ ist. Nach den eben Gesagten ist Φ wohldefiniert und injektiv; außerdem ist Φ ein Gruppenhomomorphismus: Seien $\gamma, \gamma' \in \operatorname{Gal}(K/k)$ mit $\Phi(\gamma) = j + n\mathbb{Z}$, $\Phi(\gamma') = j' + n\mathbb{Z}$. Dann ist

$$(\gamma \circ \gamma')(\alpha) = \gamma(\gamma'(\alpha)) = \gamma(\zeta^{j'}\alpha) = \zeta^{j'}\gamma(\alpha) = \zeta^{j'}\zeta^j\alpha = \zeta^{j+j'}\alpha\,,$$

also ist $\Phi(\gamma \circ \gamma') = (j + j') + n\mathbb{Z} = \Phi(\gamma) + \Phi(\gamma')$. Es folgt, dass $\operatorname{Gal}(K/k)$ zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ isomorph ist; das sind aber (bis auf Isomorphie) genau die zyklischen Gruppen mit n teilender Ordnung.

(2) (Siehe Aufgabe (2) auf dem letzten Übungsblatt.)
Sei $\gamma \in \operatorname{Gal}(K/k)$ ein Erzeuger (also $\operatorname{ord}(\gamma) = n$). $\gamma\colon K \to K$ ist k-linear; die Eigenwerte müssen n-te Einheitswurzeln sein. Als k-linearer Automorphismus endlicher Ordnung (die nicht durch $\operatorname{char}(k)$ teilbar ist) ist γ diagonalisierbar; seien $\alpha_1, \ldots, \alpha_n \in K$ k-linear unabhängige Eigenvektoren zu den Eigenwerten $\zeta^{m_1}, \ldots, \zeta^{m_n}$. Da $\operatorname{ord}(\gamma) = n$ ist und kein echter Teiler

davon, gilt $\langle \zeta^{m_1}, \dots, \zeta^{m_n} \rangle = \langle \zeta \rangle$. Es gibt also ganze Zahlen $l_1, \dots, l_n$ mit $\zeta = (\zeta^{m_1})^{l_1} \cdots (\zeta^{m_n})^{l_n}$. Sei $\alpha = \alpha_1^{l_1} \cdots \alpha_n^{l_n}$. Dann ist

$$\begin{aligned}\gamma(\alpha) &= \gamma(\alpha_1^{l_1}) \cdots \gamma(\alpha_n^{l_n}) = \gamma(\alpha_1)^{l_1} \cdots \gamma(\alpha_n)^{l_n} \\ &= (\zeta^{m_1}\alpha_1)^{l_1} \cdots (\zeta^{m_n}\alpha_n)^{l_n} = (\zeta^{m_1})^{l_1} \cdots (\zeta^{m_n})^{l_n} \cdot \alpha_1^{l_1} \cdots \alpha_n^{l_n} = \zeta\alpha\,.\end{aligned}$$

Genauso sieht man, dass $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ Eigenvektoren zu den Eigenwerten $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ sind. Damit ist $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ eine k-Basis von K; insbesondere ist $K = k(\alpha)$. Außerdem gilt für $a = \alpha^n$, dass $\gamma(a) = \gamma(\alpha^n) = \gamma(\alpha)^n = (\zeta\alpha)^n = \alpha^n = a$ ist; es folgt $a \in k$. Das zeigt, dass K der Zerfällungskörper von $X^n - a$ über k ist. ❑

Um das auf unser Problem anwenden zu können, müssen wir sicherstellen, dass k „genügend viele“ Einheitswurzeln enthält. Damit das funktioniert, brauchen wir noch etwas mehr Information aus der Galois-Theorie.

SATZ Kompositum von Galois-Erweiterungen

16.11. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und seien L_1 und L_2 Zwischenkörper, die endlich und galoissch über k sind. Dann ist auch das Kompositum L_1L_2 über k galoissch, und* $\mathrm{Gal}(L_1L_2/k) \to \mathrm{Gal}(L_1/k) \times \mathrm{Gal}(L_2/k)$, $\gamma \mapsto (\gamma|_{L_1}, \gamma|_{L_2})$, *ist ein injektiver Gruppenhomomorphismus.*

Beweis. Nach Satz 12.3 gibt es separable (irreduzible) Polynome $f_1, f_2 \in k[X]$, sodass L_1 und L_2 die Zerfällungskörper von f_1 und f_2 über k sind. Dann ist L_1L_2 der Zerfällungskörper von f_1f_2, und nach Folgerung 12.7 ist L_1L_2 über k galoissch.

Die angegebene Abbildung ist wohldefiniert, da L_1 und L_2 galoissch über k sind; siehe Satz 12.9. Dass die Abbildung ein Gruppenhomomorphismus ist, ist klar. Ist $\gamma \in \mathrm{Gal}(L_1L_2/k)$ im Kern, dann folgt $\gamma|_{L_1} = \mathrm{id}_{L_1}$ und $\gamma|_{L_2} = \mathrm{id}_{L_2}$. Weil sich die Elemente von L_1L_2 rational über k durch die Elemente von L_1 und L_2 ausdrücken lassen, folgt $\gamma = \mathrm{id}_{L_1L_2}$. Der Kern ist also trivial; damit ist die Abbildung injektiv. ❑

SATZ Translation von Galois-Erweiterungen

16.12. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und seien L_1 und L_2 Zwischenkörper, sodass L_1 endlich und galoissch über k ist. Dann ist L_1L_2 galoissch über L_2, und* $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/k)$, $\gamma \mapsto \gamma|_{L_1}$, *ist ein injektiver Gruppenhomomorphismus. Insbesondere ist* $\mathrm{Gal}(L_1L_2/L_2)$ *isomorph zu einer Untergruppe von* $\mathrm{Gal}(L_1/k)$.

Beweis. Nach Satz 12.3 gibt es ein separables (irreduzibles) Polynom $f \in k[X]$, sodass L_1 der Zerfällungskörper von f über k ist. Dann ist L_1L_2 der Zerfällungskörper von f über L_2, also ist nach Folgerung 12.7 L_1L_2 galoissch über L_2.

Dass die angegebene Abbildung wohldefiniert und ein Gruppenhomomorphismus ist, sieht man wie im Beweis von Satz 16.11. Ist $\gamma \in \mathrm{Gal}(L_1L_2/L_2)$ im Kern, dann folgt $\gamma|_{L_1} = \mathrm{id}_{L_1}$; außerdem ist $\gamma|_{L_2} = \mathrm{id}_{L_2}$ nach Definition von $\mathrm{Gal}(L_1L_2/L_2)$. Wie oben folgt $\gamma = \mathrm{id}_{L_1L_2}$; der Kern ist also trivial. ❑

Damit können wir schon einmal eine Richtung von Satz 16.2 beweisen:

LEMMA auflösbare Erweiterung ist Radikalerweiterung

16.13. **Lemma.** *Sei* $\mathrm{char}(k) = 0$ *und* $k \subset K$ *endlich und galoissch mit auflösbarer Galois-Gruppe. Dann ist* $k \subset K$ *eine Radikalerweiterung.*

Beweis. Sei $G = \mathrm{Gal}(K/k)$ und sei $\{\mathrm{id}\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$ eine Kette von Untergruppen wie in Definition 16.3. Nach Lemma 16.6 können wir annehmen, dass die Faktorgruppen G_j/G_{j-1} alle zyklisch sind. Sei N das kleinste gemeinsame Vielfache aller ihrer Ordnungen. Sei L der N-te Kreisteilungskörper (hier brauchen wir $\mathrm{char}(k) = 0$ oder wenigstens $\mathrm{char}(k) \nmid N$); dann ist nach Satz 16.12 KL galoissch über L und die Galois-Gruppe G' ist als Untergruppe von $\mathrm{Gal}(K/k)$ ebenfalls auflösbar. Sei $\{\mathrm{id}\} = G'_0 \leq G'_1 \leq \ldots \leq G'_m = G'$ eine Kette von Untergruppen mit zyklischen Faktorgruppen von N teilender Ordnung und seien $L = L_m \subset L_{m-1} \subset \ldots \subset L_1 \subset L_0 = KL$ die zugehörigen Fixkörper. Nach Satz 12.11 ist L_{j-1} galoissch über L_j mit zyklischer Galois-Gruppe G'_j/G'_{j-1} der Ordnung $n_j \mid N$. Da die N-ten Einheitswurzeln in L vorhanden sind, folgt nach Lemma 16.10, dass es $a_j \in L_j$ gibt, sodass L_{j-1} der Zerfällungskörper von $X^{n_j} - a_j$ über L_j ist. Außerdem ist L der Zerfällungskörper von $X^N - 1$ über k. Wegen $K \subset KL$ ist K eine Radikalerweiterung. ❑

Für die andere Richtung müssen wir noch ein wenig mehr arbeiten.

LEMMA Radikalerweiterung in Galois-Erweiterung

16.14. **Lemma.** *Ist* $k \subset K$ *eine Radikalerweiterung, dann gibt es eine Radikalerweiterung* $k \subset L$ *mit* $K \subset L$*, die galoissch ist.*

Beweis. Sei $k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$ ein Körperturm wie in Definition 16.1 mit $K \subset K_m$. Wir führen den Beweis durch Induktion über m. Im Fall $m = 0$ ist nichts zu zeigen (denn $K = k$). Sei also $m > 0$. Wir können die Induktionsvoraussetzung auf K_{m-1} anwenden: Es gibt eine galoissche Körpererweiterung $k \subset L'$ mit $K_{m-1} \subset L'$, die eine Radikalerweiterung ist. Sei K_m der Zerfällungskörper von $X^n - a$ über K_{m-1} (mit $a \in K_{m-1}$). Dann ist $a \in L'$; sei $\{a_1 = a, a_2, a_3, \ldots, a_l\}$ die Bahn von a unter $\mathrm{Gal}(L'/k)$. Dann ist $f = (X^n - a_1)(X^n - a_2)\cdots(X^n - a_l) \in k[X]$, denn die Koeffizienten von f sind unter $\mathrm{Gal}(L'/k)$ invariant, da die Faktoren nur permutiert werden. Sei L'' der Zerfällungskörper von f über k; dann ist $k \subset L''$ galoissch. Sei schließlich $L = L'L''$ das Kompositum von L' und L''. Nach Satz 16.11 ist $k \subset L$ galoissch. Außerdem ist L auch der Zerfällungskörper von f über L', enthält also K_m als Zerfällungskörper von $X^n - a_1$ über $K_{m-1} \subset L'$. Es bleibt zu zeigen, dass $k \subset L$ eine Radikalerweiterung ist. Das ergibt sich daraus, dass wir einen Körperturm

$$L' = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_l = L$$

haben, wo L_j der Zerfällungskörper von $X^n - a_j$ über L_{j-1} ist, zusammen mit der Aussage, dass $k \subset L'$ eine Radikalerweiterung ist. ❑

Das folgende Lemma ergibt den letzten fehlenden Schritt im Beweis von Satz 16.2:

LEMMA Radikalerweiterung auflösbar

16.15. **Lemma.** *Ist* $k \subset K$ *eine galoissche Radikalerweiterung, dann ist ihre Galois-Gruppe* $\mathrm{Gal}(K/k)$ *auflösbar.*

Beweis. Sei $k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$ ein Körperturm wie in Definition 16.1 mit $K \subset K_m$. Nach Lemma 16.14 können wir annehmen, dass $k \subset K_m$ ebenfalls galoissch ist. Es genügt dann zu zeigen, dass $\mathrm{Gal}(K_m/k)$ auflösbar ist, denn $\mathrm{Gal}(K/k)$ ist eine Faktorgruppe von $\mathrm{Gal}(K_m/k)$, also nach Lemma 16.5 ebenfalls auflösbar.

Der Beweis geht durch Induktion über m. Der Fall $m = 0$ ist klar (die triviale Gruppe ist auflösbar). Sei also $m > 0$. Dann ist K_1 der Zerfällungskörper eines Polynoms $X^n - a \in k[X]$ (mit $\mathrm{char}(k) \nmid n$) und damit eine Galois-Erweiterung von k. Nach Induktionsvoraussetzung, angewandt auf die galoissche Radikalerweiterung $K_1 \subset K_m$, ist die Untergruppe $\mathrm{Gal}(K_m/K_1)$ von $\mathrm{Gal}(K_m/k)$ auflösbar. Nach Lemma 16.5 genügt es also zu zeigen, dass auch die Faktorgruppe $\mathrm{Gal}(K_1/k)$ auflösbar ist. Dazu beachten wir, dass K_1 den n-ten Kreisteilungskörper k' über k enthält (denn eine primitive n-te Einheitswurzel ergibt sich als Quotient geeigneter Nullstellen von $X^n - a$). Wir haben also den Turm $k \subset k' \subset K_1$. Nach Satz 13.2 ist $k \subset k'$ galoissch mit abelscher Galois-Gruppe, und nach Lemma 16.10 ist $k' \subset K_1$ galoissch mit abelscher (sogar zyklischer) Galois-Gruppe; insgesamt folgt, dass $\mathrm{Gal}(K_1/k)$ auflösbar ist (mit der Kette $\{\mathrm{id}\} \leq \mathrm{Gal}(K_1/k') \leq \mathrm{Gal}(K_1/k)$; beachte, dass $\mathrm{Gal}(K_1/k)/\mathrm{Gal}(K_1/k') \cong \mathrm{Gal}(k'/k)$ ist). ❑

Der Beweis von Satz 16.2 geht dann so:

Beweis. „⇒“: Sei $k \subset K$ eine Radikalerweiterung. Nach Lemma 16.14 gibt es eine galoissche Radikalerweiterung $k \subset L$ mit $K \subset L$. Nach Lemma 16.15 ist die Galois-Gruppe von $k \subset L$ auflösbar.

„⇐“: Sei $\mathrm{char}(k) = 0$ und $k \subset L$ endlich und galoissch mit auflösbarer Galois-Gruppe, sodass $K \subset L$ ist. Nach Lemma 16.13 ist $k \subset L$ eine Radikalerweiterung. Dann ist aber $k \subset K$ ebenfalls eine Radikalerweiterung (man kann denselben Körperturm verwenden wie für $k \subset L$). ❑

Daraus ergibt sich unmittelbar:

16.16. **Folgerung.** *Seien k ein Körper mit $\mathrm{char}(k) = 0$ und $f \in k[X]$. Die Nullstellen von f lassen sich genau dann durch Radikalausdrücke über k darstellen, wenn die Galois-Gruppe $\mathrm{Gal}(f/k)$ auflösbar ist.*

FOLG Auflösung durch Radikale

16.17. **Folgerung.** *Für jedes $n \geq 5$ gibt es Polynome $f \in \mathbb{Q}[X]$ vom Grad n, deren Nullstellen nicht durch Radikalausdrücke darstellbar sind.*

FOLG nicht auflösbare Polynome

Beweis. Wir konstruieren ein Polynom f mit $\mathrm{Gal}(f/\mathbb{Q}) = S_5$. Da S_5 nicht auflösbar ist, sind die Nullstellen von f nicht durch Radikalausdrücke darstellbar. Für beliebiges $n \geq 5$ betrachten wir ein Polynom der Form fg mit $g \in \mathbb{Q}[X]$ normiert vom Grad $n - 5$. Die Konstruktion von f wird durch das folgende Lemma erledigt. ❑

16.18. **Lemma.** *Sei p eine ungerade Primzahl.*

LEMMA $\mathrm{Gal}(f/\mathbb{Q}) = S_p$

(1) *Ist G eine Untergruppe von S_p, sodass G ein Element der Ordnung p und eine Transposition enthält, dann ist $G = S_p$.*

(2) *Ist $f \in \mathbb{Q}[X]$ normiert vom Grad p und irreduzibel, sodass f genau $p - 2$ reelle und ein Paar konjugiert komplexer Nullstellen hat, dann hat f Galois-Gruppe $\mathrm{Gal}(f/\mathbb{Q}) = S_p$.*

(3) *Polynome wie in Teil (2) existieren.*

Beweis.

(1) Das ist die Aussage von Satz 1.10 (3).

(2) Sei $G = \mathrm{Gal}(f/\mathbb{Q})$. Da f irreduzibel ist, ist p ein Teiler von $\#G$ (Lemma 14.2), also enthält G ein Element der Ordnung p (1. Satz von Sylow 3.5). Sei $\mathbb{Q} \subset K \subset \mathbb{C}$ der Zerfällungskörper von f. Die komplexe Konjugation induziert durch Einschränkung auf K ein Element von G, das die beiden konjugiert komplexen Nullstellen von f vertauscht und die übrigen Nullstellen fest lässt; dieses Element entspricht also einer Transposition. Nach Teil (1) folgt $G = S_p$.

(3) Wir betrachten zunächst das folgende Polynom vom Grad p:

$$\begin{aligned} h &= X(X^2-2)(X^2-4)\cdots(X^2-(p-3))(X^2+2p^2) \\ &= X(X^2+2p^2)\prod_{j=1}^{(p-3)/2}(X^2-2j) \\ &= X^p + \Big(2p^2 - \frac{(p-1)(p-3)}{4}\Big)X^{p-2} + \ldots \in \mathbb{Q}[X]\,. \end{aligned}$$

Es hat offensichtlich genau $p-2$ reelle Nullstellen. Seine $(p-2)$-te Ableitung ist

$$h^{(p-2)} = \frac{p!}{2}X^2 + (p-2)!\Big(2p^2 - \frac{(p-1)(p-3)}{4}\Big)$$

und damit ohne reelle Nullstelle (da der konstante Term positiv ist). Außerdem gilt für ungerade Zahlen $1 \le 2m+1 \le p-2$, dass

$$h(\pm\sqrt{2m+1}) = \pm\sqrt{2m+1}(2m+1+2p^2)\prod_{j=1}^{(p-3)/2}(2(m-j)+1)$$

Betrag $\ge 2p^2$ hat. Da h nur einfache reelle Nullstellen hat, und zwar an den Stellen $-\sqrt{p-3},\ldots,-\sqrt{4},-\sqrt{2},0,\sqrt{2},\ldots,\sqrt{p-3}$, müssen die Vorzeichen an den $p-1$ Stellen

$$-\sqrt{p-2},\ldots,-\sqrt{3},-1,1,\sqrt{3},\ldots,\sqrt{p-2}$$

alternieren. Wir setzen jetzt $f = h+2$. Das Polynom h ist ungerade und $h \equiv X^p \bmod 2$. Es folgt $f \equiv X^p \bmod 2$ und $f(0) = 2$; damit ist f irreduzibel nach dem Eisenstein-Kriterium. Da $2 < 2p^2$ ist, hat f an den $p-1$ oben angegebenen Stellen dasselbe Vorzeichen wie h; nach dem Zwischenwertsatz hat f also mindestens $p-2$ reelle Nullstellen. Auf der anderen Seite kann f nicht mehr als $p-2$ reelle Nullstellen haben, denn sonst hätte die $(p-2)$-te Ableitung von f zwei reelle Nullstellen (Induktion mit dem Satz von Rolle), was wegen $f^{(p-2)} = h^{(p-2)}$ nicht stimmt. ❑

Für $p = 5$ kann man z.B. auch $f = X^5 - 6X + 1$ nehmen (denn f ist irreduzibel mod 5 und hat genau drei reelle Nullstellen: ≥ 3 mit Zwischenwertsatz, ≤ 3, da $f' = 5X^4 - 6$ nur zwei reelle Nullstellen hat).

Man kann für jedes n (nicht nur für Primzahlen) Polynome über $\mathbb{Q}$ konstruieren, deren Galois-Gruppe S_n (oder auch A_n) ist. Die weitergehende Frage, ob *jede* endliche Gruppe (bis auf Isomorphie) als Galois-Gruppe eines Polynoms über $\mathbb{Q}$ auftritt, das sogenannte *Umkehrproblem der Galois-Theorie*, ist jedoch offen.

Auf der anderen Seite ist leicht einzusehen, dass jede endliche Gruppe als Galois-Gruppe irgendeiner Galois-Erweiterung auftritt: Sei G eine endliche Gruppe mit $\#G = n$, dann ist G isomorph zu einer Untergruppe der S_n (betrachte die Operation von G auf sich selbst durch Translation). Ist $p > n$ eine Primzahl, dann ist S_n isomorph zu einer Untergruppe von S_p (die aus den Permutationen besteht, die gewisse $p-n$ Elemente fest lassen). Sei $\mathbb{Q} \subset K$ eine Galois-Erweiterung mit $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$ und sei $k = \mathcal{F}(G)$ der Fixkörper von G (als Untergruppe von S_p

betrachtet). Dann ist nach dem Satz 12.11 über die Galois-Korrespondenz $k \subset K$ galoissch mit $\mathrm{Gal}(K/k) \cong G$.

Wenn man sich bei der Definition von Radikalerweiterungen auf die Adjunktion von *Quadratwurzeln* (statt beliebiger n-ter Wurzeln) beschränkt, dann erhält man genau die (mit Zirkel und Lineal) *konstruierbaren* Elemente; siehe Abschnitt 9. Mit im Wesentlichen dem gleichen Beweis (sogar einfacher, weil die zweiten Einheitswurzeln ± 1 in jedem Körper der Charakteristik 0 schon vorhanden sind) erhält man dafür die folgende Aussage:

SATZ Charakterisierung von Konstruierbarkeit

16.19. **Satz.** *Sei $k \subset \mathbb{C}$ ein Teilkörper und sei $\alpha \in \mathbb{C}$. Dann sind äquivalent:*

(1) *α ist ausgehend von den Elementen von k mit Zirkel und Lineal konstruierbar.*

(2) *Es gibt eine Galois-Erweiterung $k \subset K$ mit $K \subset \mathbb{C}$ und $\alpha \in K$, sodass $\#\,\mathrm{Gal}(K/k) = 2^n$ ist für ein $n \in \mathbb{Z}_{\geq 0}$.*

(3) *α ist algebraisch über k und für das Minimalpolynom $f \in k[X]$ von α über k gilt $\#\,\mathrm{Gal}(f/k) = 2^n$ für ein $n \in \mathbb{Z}_{\geq 0}$.*

Der Beweis liefert zunächst, dass die Galois-Gruppe auflösbar sein muss (mit sukzessiven Faktorgruppen $\cong \mathbb{Z}/2\mathbb{Z}$, was bedeutet, dass die Gruppenordnung eine Potenz von 2 sein muss). Der Schritt, der im Beweis noch fehlt, ist folgende Aussage (für $p = 2$):

SATZ p-Gruppen sind auflösbar

16.20. **Satz.** *Sei p eine Primzahl und G eine endliche p-Gruppe, d.h., $\#G = p^n$ für ein $n \in \mathbb{Z}_{\geq 0}$. Dann ist G auflösbar. Genauer gilt: Es gibt eine Kette*

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

von Untergruppen mit $G_{j-1} \triangleleft G_j$ und $G_j/G_{j-1} \cong \mathbb{Z}/p\mathbb{Z}$ für alle $1 \leq j \leq n$.

Beweis. Wir erinnern uns daran, dass das *Zentrum* einer Gruppe G definiert war als

$$Z(G) = \{g \in G \mid \forall g' \in G\colon gg' = g'g\}\,.$$

Daraus folgt sofort, dass jede Untergruppe von $Z(G)$ ein Normalteiler von G ist. Nach Folgerung 2.17 ist das Zentrum einer p-Gruppe stets nichttrivial. Insbesondere hat eine p-Gruppe stets einen (dann zyklischen) Normalteiler der Ordnung p (1. Satz von Sylow 3.5 oder Struktursatz über endliche abelsche Gruppen, angewandt auf das Zentrum).

Der Beweis erfolgt nun durch Induktion über n. Im Fall $n = 0$ ist G trivial, und es ist nichts zu zeigen. Sei also $n > 0$. Nach obiger Überlegung hat G einen Normalteiler G_1 mit $\#G_1 = p$. Sei $G' = G/G_1$, dann ist $\#G' = p^{n-1}$; nach Induktionsvoraussetzung gibt es also eine Kette

$$\{1_{G'}\} = G'_0 \leq G'_1 \leq \ldots \leq G'_{n-1} = G'$$

von Untergruppen von G' mit $G'_{j-1} \triangleleft G'_j$ und $G'_j/G'_{j-1} \cong \mathbb{Z}/p\mathbb{Z}$ für $1 \leq j \leq n-1$. Sei $\phi\colon G \to G'$ der kanonische Epimorphismus. Wir setzen $G_j = \phi^{-1}(G'_{j-1})$ für $1 \leq j \leq n$ (für $j = 1$ erhalten wir dieselbe Gruppe G_1 wie oben) und $G_0 = \{1_G\}$, dann gilt $G_j/G_{j-1} \cong G'_{j-1}/G'_{j-2} \cong \mathbb{Z}/p\mathbb{Z}$ für $2 \leq j \leq n$ und $G_1/G_0 \cong G_1 \cong \mathbb{Z}/p\mathbb{Z}$. ❑

Sei $\alpha \in \mathbb{C}$ algebraisch mit Minimalpolynom f über $\mathbb{Q}$ vom Grad n. Die Bedingung „n ist Zweierpotenz“ ist *notwendig* für die Konstruierbarkeit von α (denn da f irreduzibel ist, gilt $n \mid \#\,\mathrm{Gal}(f/\mathbb{Q})$) — das haben wir für verschiedene Unmöglichkeitsbeweise benutzt — aber *nicht hinreichend*. Wir haben gesehen, dass es irreduzible Polynome f vom Grad 4 über $\mathbb{Q}$ gibt mit $\mathrm{Gal}(f/\mathbb{Q}) \cong S_4$ oder A_4, aber $\#S_4 = 24$ und $\#A_4 = 12$ sind keine Zweierpotenzen.

Literatur

[Fi] Gerd Fischer: *Lehrbuch der Algebra,* Vieweg, 2008. Signatur 80/SK 200 F529 L5. Online-Zugriff unter
http://dx.doi.org/10.1007/978-3-8348-9455-7
- Ein Standard-Lehrbuch. Das Buch folgt dem üblichen Aufbau Gruppen-Ringe-Körper.

[KM] Christian Karpfinger und Kurt Meyberg: *Algebra. Gruppen - Ringe - Körper,* Spektrum Akademischer Verlag, 2010. Online-Zugriff unter
http://dx.doi.org/10.1007/978-3-8274-2601-7.
- Das Buch folgt dem üblichen Aufbau Gruppen-Ringe-Körper.