Einführung in die Algebra

Sommersemester 2013

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

Bildschirmversion vom 7. September 2013, 13:33 Uhr.

Diese Vorlesung setzt die Vorlesung „Einführung in die Zahlentheorie und algebraische Strukturen“ aus dem Wintersemester 2012/2013 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 Lemmata 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 werde ich 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 schreibe ich $A \subsetneq B$.

1. Gruppen und Untergruppen

Wir erinnern uns daran, was eine Gruppe ist.

* 1.1. **Definition.** Eine *Gruppe* ist ein Quadrupel $(G, *, e, i)$, bestehend aus einer Menge G, einer Abbildung $*\colon G \times G \to G$, einem Element $e \in G$ und einer Abbildung $i\colon G \to G$ mit den folgenden Eigenschaften: **DEF** Gruppe abelsche Gruppe endliche Gruppe Ordnung

(1) (Assoziativität) $\forall a, b, c \in G\colon (a * b) * c = a * (b * c)$.

(2) (Neutrales Element) $\forall a \in G\colon a * e = a = e * a$.

(3) (Inverses Element) $\forall a \in G\colon a * i(a) = e = i(a) * a$.

Die Gruppe heißt *kommutativ* oder *abelsch*, wenn zusätzlich gilt

(4) (Kommutativität) $\forall a, b \in G\colon a * b = b * a$.

Ist die Menge G endlich, dann heißt die Gruppe *endlich*, und ihre Kardinalität $\#G$ heißt die *Ordnung* der Gruppe. ♢

Die Bezeichnung „abelsch“ ehrt den norwegischen Mathematiker Niels Henrik Abel, nach dem auch der *Abelpreis* benannt ist, ein dem Nobelpreis vergleichbarer Preis für Mathematik, der seit 2003 jährlich verliehen wird.

Da, wie wir uns früher schon überlegt haben, sowohl das neutrale Element (wenn es existiert) als auch das zu a inverse Element (wenn es existiert) eindeutig bestimmt sind, definiert man eine Gruppe sehr häufig in der folgenden Form:

1.2. **Definition.** Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung $*\colon G \times G \to G$, sodass es $e \in G$ und eine Abbildung $i\colon G \to G$ gibt, die die Eigenschaften (1) bis (3) in Definition 1.1 erfüllen. ♢ **DEF** Gruppe

Man spricht deshalb auch einfach von „der Gruppe $(G, *)$“ oder auch von „der Gruppe G“, wenn die Verknüpfung aus dem Kontext klar ist. Für das Inverse $i(a)$ schreibt man meist a^{-1}.

Gruppen schreibt man gerne „multiplikativ“, dann ist die Verknüpfung $a \cdot b$ oder kurz ab und das neutrale Element heißt 1 (oder 1_G).

Abelsche (kommutative) Gruppen schreibt man auch häufig „additiv“, dann ist die Verknüpfung $a+b$, das neutrale Element heißt 0 und das Inverse von a wird als das Negative von a geschrieben: $-a$. Dann schreibt man auch kurz $a - b$ für $a + (-b)$. Abelsche Gruppen haben wir gegen Ende der „Einführung in die Zahlentheorie und algebraische Strukturen“ bereits genauer studiert und den Klassifikationssatz für endlich erzeugte abelsche Gruppen bewiesen.

1.3. **Beispiel.** Das einfachste Beispiel einer Gruppe ist $G = \{e\}$ (mit $e * e = e$ und $i(e) = e$). Eine Gruppe, die nur aus dem neutralen Element besteht, heißt auch *triviale Gruppe*. ♣ **BSP** triviale Gruppe

BSP
Permutationsgruppe
symmetrische Gruppe

1.4. **Beispiel.** Ein wichtiges und grundlegendes Beispiel einer Gruppe ist die Gruppe $S(X)$ der Permutationen einer Menge X. Die unterliegende Menge besteht hier aus allen bijektiven Abbildungen $X \to X$, die Verknüpfung ist die Verknüpfung von Abbildungen, das neutrale Element ist die identische Abbildung id_X und das Inverse $i(f)$ ist die Umkehrabbildung f^{-1}. Die in Definition 1.1 geforderten Eigenschaften sind elementare Eigenschaften von Mengen und Abbildungen.

Für $\#X \leq 1$ ist die Gruppe $S(X) = \{\mathrm{id}_X\}$ trivial. Für $\#X \geq 3$ ist $S(X)$ nicht abelsch.

Für $S\big(\{1, 2, \ldots, n\}\big)$ schreibt man auch S_n (in der Literatur auch häufig in Fraktur: $\mathfrak{S}_n$) und nennt S_n die *symmetrische Gruppe* auf n Elementen. Ihre Ordnung ist $\#S_n = n!$. ♣

Diese Gruppe S_n ist uns bereits in der Linearen Algebra im Zusammenhang mit der Determinante und der „Leibniz-Formel“

$$\det\big((a_{ij})_{1\leq i,j\leq n}\big) = \sum_{\sigma\in S_n} \varepsilon(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

begegnet. Die Abbildung $\varepsilon\colon S_n \to \{\pm 1\}$ ist übrigens ein Beispiel für einen *Gruppenhomomorphismus*; diesen Begriff werden wir bald einführen.

Warum sind Gruppen in der Mathematik so wichtig?

In der Mathematik betrachtet man meistens Mengen mit einer Zusatzstruktur und Abbildungen zwischen solchen Mengen, die mit den Zusatzstrukturen verträglich sind. In der Algebra heißen solche Abbildungen dann *Homomorphismen*. Bijektive Homomorphismen (oder genauer: Homomorphismen, für die es einen inversen Homomorphismus gibt) sind *Isomorphismen*, und Isomorphismen, deren Quelle und Ziel übereinstimmen, heißen *Automorphismen* der betreffenden Struktur. Wir haben diese Begriffe bereits für Vektorräume, Ringe und abelsche Gruppen eingeführt und werden es bald auch für (beliebige) Gruppen tun.

Wir werden sehen, dass die Automorphismen einer Struktur X eine Gruppe bilden, die *Automorphismengruppe* $\mathrm{Aut}(X)$ von X. Dass Gruppen so in sehr natürlicher Weise in der Mathematik auftreten, zeigt ihre Wichtigkeit. Meistens lässt sich durch das Studium seiner Automorphismen oder Symmetrien viel über eine Struktur oder ein geometrisches Objekt herausfinden. Daher hat die Gruppentheorie viele Anwendungen in allen Teilgebieten der Mathematik. Ein Beispiel aus der Algebra ist die *Galois-Theorie*, die Körpererweiterungen mit Hilfe ihrer Automorphismengruppen studiert. Darauf werden wir eventuell noch am Ende des Semesters zu sprechen kommen.

Wir erinnern uns aber zunächst an den Begriff der Untergruppe.

* DEF
Untergruppe

1.5. **Definition.** Sei $(G, *, e, i)$ eine Gruppe und $H \subset G$ eine Teilmenge. Dann ist H eine *Untergruppe* von G, wenn H die folgenden Bedingungen erfüllt:

(1) $e \in H$.

(2) $\forall a, b \in H\colon a * b \in H$.

(3) $\forall a \in H\colon i(a) \in H$.

H muss also das neutrale Element enthalten und unter der Verknüpfung und Inversenbildung abgeschlossen sein. Man schreibt häufig $H \leq G$ für „H ist Untergruppe von G“. ♢

Natürlich ist die Definition gerade so gemacht, dass $(H, *|_{H\times H}, e, i|_H)$ (also mit den von G auf H eingeschränkten Abbildungen) wieder eine Gruppe ist. Das folgt daraus, dass alle Axiome in Definition 1.1 die Form „für alle ...“ haben — wenn sie für alle Elemente von G gelten, dann auch für alle Elemente von H, solange die vorkommenden Ausdrücke Sinn haben. Das ist aber durch die Abgeschlossenheit von H sichergestellt.

Wie üblich haben Untergruppen die folgende Durchschnittseigenschaft.

LEMMA Durchschnitt von Untergruppen

1.6. **Lemma.** *Sei G eine Gruppe und $(H_i)_{i\in I}$ eine Familie von Untergruppen von G mit nichtleerer Indexmenge I. Dann ist auch $\bigcap_{i\in I} H_i$ wieder eine Untergruppe von G.*

Beweis. Analog wie für Untervektorräume, Unterringe, Ideale, ...

Der Vollständigkeit halber sei der Beweis hier ausgeführt. Wir müssen die drei Bedingungen aus Definition 1.5 nachweisen. Sei $H = \bigcap_{i\in I} H_i$; die Gruppe sei $(G, *, e, i)$.

(1) Da $e \in H_i$ ist für alle $i \in I$, ist auch $e \in H$.
(2) Seien $a, b \in H$. Dann gilt $a, b \in H_i$ für alle $i \in I$. Da die H_i Untergruppen sind, folgt $a * b \in H_i$ für alle $i \in I$ und damit auch $a * b \in H$.
(3) Sei $a \in H$. Dann ist $a \in H_i$ für alle $i \in I$. Da die H_i Untergruppen sind, folgt $i(a) \in H_i$ für alle $i \in I$ und damit auch $i(a) \in H$. ❑

Als ersten Schritt zum Beweis, dass die Automorphismen einer Struktur eine Gruppe bilden, zeigen wir, dass die Permutationen von X, die eine Zusatzstruktur erhalten, eine Untergruppe von $S(X)$ bilden. Diese Zusatzstruktur ist dabei durch eine Abbildung gegeben, wie sie im folgenden Lemma betrachtet wird.

LEMMA Strukturverträgliche Permutationen bilden Untergruppe

1.7. **Lemma.** *Seien X eine Menge und f eine Abbildung von einem der folgenden Typen:*

(1) $f\colon X^n \to X$ *für ein* $n \in \mathbb{Z}_{>0}$.
(2) $f\colon X^n \to Y$ *für ein* $n \in \mathbb{Z}_{>0}$ *mit einer Menge* Y.
(3) $f\colon Y \to X$ *mit einer Menge* Y.
(4) $f\colon Y \times X^n \to X$ *für ein* $n \in \mathbb{Z}_{>0}$ *mit einer Menge* Y.

Sei $H_f \subset S(X)$ die Teilmenge der Permutationen σ, die folgende Bedingung erfüllen (je nach Typ von f):

(1) $\forall x_1, x_2, \dots, x_n \in X\colon f\big(\sigma(x_1), \sigma(x_2), \dots, \sigma(x_n)\big) = \sigma\big(f(x_1, x_2, \dots, x_n)\big)$.
(2) $\forall x_1, x_2, \dots, x_n \in X\colon f(\sigma(x_1), \sigma(x_2), \dots, \sigma(x_n)) = f(x_1, x_2, \dots, x_n)$.
(3) $\forall y \in Y\colon \sigma\big(f(y)\big) = f(y)$.
(4) $\forall y \in Y, x_1, x_2, \dots, x_n \in X\colon$
$f\big(y, \sigma(x_1), \sigma(x_2), \dots, \sigma(x_n)\big) = \sigma\big(f(y, x_1, x_2, \dots, x_n)\big)$.

Dann ist H_f eine Untergruppe von $S(X)$.

Man kann sich die Bedingungen in der Form von Diagrammen veranschaulichen, die kommutativ sein sollen, wie zum Beispiel:

$$\begin{array}{ccc} X\times X & \xrightarrow{f} & X \\ {\scriptstyle \sigma\times\sigma}\downarrow & & \downarrow{\scriptstyle \sigma} \\ X\times X & \xrightarrow{f} & X \end{array} \qquad \begin{array}{ccc} X\times X & & \\ {\scriptstyle \sigma\times\sigma}\downarrow & \searrow^{f} & \\ X\times X & \xrightarrow{f} & Y \end{array} \qquad \begin{array}{ccc} & \nearrow_{f} & X \\ Y & & \downarrow{\scriptstyle \sigma} \\ & \searrow_{f} & X \end{array} \qquad \begin{array}{ccc} Y\times X & \xrightarrow{f} & X \\ {\scriptstyle \mathrm{id}_Y\times\sigma}\downarrow & & \downarrow{\scriptstyle \sigma} \\ Y\times X & \xrightarrow{f} & X \end{array}$$

Beweis. Wir müssen jeweils die Bedingungen aus Definition 1.5 nachprüfen. Wir tun das beispielhaft für Typ (1); die übrigen Fälle sind eine Übungsaufgabe.

(1) $\mathrm{id}_X \in H_f$ ist klar.

(2) Seien $\sigma, \tau \in H_f$ und $x_1, x_2, \dots, x_n \in X$. Dann gilt

$$\begin{aligned} f\big((\sigma\circ\tau)(x_1), (\sigma\circ\tau)(x_2), \dots, (\sigma\circ\tau)(x_n)\big) &= f\big(\sigma(\tau(x_1)), \sigma(\tau(x_2)), \dots, \sigma(\tau(x_n))\big) \\ &\overset{(*)}{=} \sigma\big(f(\tau(x_1), \tau(x_2), \dots, \tau(x_n))\big) \\ &= \sigma\big(\tau(f(x_1, x_2, \dots, x_n))\big) \\ &= (\sigma\circ\tau)\big(f(x_1, x_2, \dots, x_n)\big)\,, \end{aligned}$$

also ist $\sigma \circ \tau \in H_f$. An der Stelle $(*)$ haben wir die Eigenschaft von σ für $\tau(x_j) \in X$ verwendet.

(3) Seien $\sigma \in H_f$ und $x_1, x_2, \dots, x_n \in X$. Wir können die Eigenschaft von σ auf $\sigma^{-1}(x_j)$ anwenden:

$$\begin{aligned} f(x_1, x_2, \dots, x_n) &= f\big(\sigma(\sigma^{-1}(x_1)), \sigma(\sigma^{-1}(x_2)), \dots, \sigma(\sigma^{-1}(x_n))\big) \\ &= \sigma\big(f(\sigma^{-1}(x_1), \sigma^{-1}(x_2), \dots, \sigma^{-1}(x_n))\big)\,; \end{aligned}$$

Anwenden von σ^{-1} auf beide Seiten zeigt, dass $\sigma^{-1} \in H_f$ ist. ❑

Da algebraische Strukturen jeweils durch eine oder meistens mehrere Abbildungen der im Lemma betrachteten Typen gegeben sind, folgt zum Beispiel:

1.8. **Folgerung.** *Die Automorphismen eines Ringes, eines Körpers, einer abelschen Gruppe bzw. eines K-Vektorraums bilden jeweils eine Gruppe.*

FOLG Automorphismengruppen

Beweis. Wir skizzieren den Beweis für Ringe; der Beweis für die anderen Strukturen geht analog und ist eine Übungsaufgabe.

Ein Ring $(R, +, 0, -, \cdot, 1)$ ist gegeben durch die Menge R und Abbildungen

$$+\colon R \times R \to R, \quad -\colon R \to R, \quad \cdot\colon R \times R \to R$$

und die Elemente 0 und 1, die man sich als durch eine Abbildung $e\colon \{0,1\} \to R$ gegeben denken kann. Insgesamt haben wir vier Abbildungen, nämlich $+$, $-$, $\cdot$ vom Typ (1) (mit $n = 2, 1, 2$) und e vom Typ (3) (mit $Y = \{0,1\}$), die die Ringstruktur festlegen. Ein Automorphismus von R ist eine bijektive Abbildung $R \to R$, die mit diesen vier Abbildungen im Sinne von Lemma 1.7 verträglich ist. Seien H_+, H_-, $H_\cdot$, H_e die durch Lemma 1.7 gegebenen Untergruppen von $S(R)$, die aus Permutationen bestehen, die mit der jeweils im Index angegebenen Abbildung verträglich sind. Dann ist

$$\mathrm{Aut}(R) = H_+ \cap H_- \cap H_\cdot \cap H_e$$

nach Lemma 1.6 wieder eine Untergruppe von $S(R)$ und damit selbst eine Gruppe.

(Da die Ringstruktur bereits durch die beiden Verknüpfungen Addition und Multiplikation festgelegt ist, würde es genügen, nur $H_+ \cap H_\cdot$ zu betrachten.) ❑

Für die Automorphismengruppe eines K-Vektorraums V schreibt man üblicherweise $\mathrm{GL}(V)$; im Fall $V = K^n$ auch $\mathrm{GL}(n, K)$ (oder $\mathrm{GL}_n(K)$). Das ist gerade die Gruppe der invertierbaren $n \times n$-Matrizen über K.

BSP Gruppen

1.9. **Beispiele.** Weitere Beispiele von „Symmetriegruppen“ oder Automorphismengruppen sind:

(1) Die Symmetriegruppe eines geometrischen Objekts, also die Menge der (eventuell auch nur der orientierungserhaltenden) Bewegungen, die das Objekt in sich überführen. Die Symmetriegruppe des Einheitskreises in der Ebene ist zum Beispiel die orthogonale Gruppe $\mathrm{O}(2)$, während sich für reguläre Polygone endliche Gruppen ergeben, die sogenannten *Diedergruppen*, die wir später noch genauer betrachten werden.

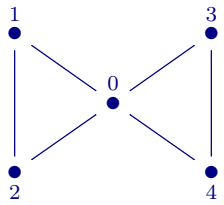
(2) Die Isometriegruppe eines metrischen Raums X, also die Menge der bijektiven Abbildungen $f\colon X \to X$, die die Metrik (die eine Abbildung $d\colon X \times X \to \mathbb{R}$ vom Typ (2) ist) erhalten:

$$\forall x, y \in X\colon d\big(f(x), f(y)\big) = d(x, y)\,.$$

(3) Die Diffeomorphismengruppe einer differenzierbaren Mannigfaltigkeit X, also die Menge der differenzierbaren Abbildungen $f\colon X \to X$ mit differenzierbarer Inverser.

(4) Ein (einfacher, schlingenloser, ungerichteter) *Graph* $\Gamma = (V, E)$ ist gegeben durch eine Menge V von „Ecken“ (engl. *vertex/vertices*) und eine Menge E von zweielementigen Teilmengen von V, den „Kanten“ (engl. *edges*); die Idee dabei ist, dass jede Kante zwei Ecken verbindet. Ein Automorphismus von Γ ist eine Permutation von V, die Kanten auf Kanten abbildet. Die Automorphismen von Γ bilden eine Gruppe. Zum Beispiel ist $\#\operatorname{Aut}(\Gamma) = 8$ für den folgenden Graphen

$$\Gamma = \big(\{0,1,2,3,4\}, \{\{0,1\},\{0,2\},\{0,3\},\{0,4\},\{1,2\},\{3,4\}\}\big)\ :$$



♣

Die Durchschnittseigenschaft aus Lemma 1.6 ermöglicht folgende Definitionen, die wir in analoger Weise schon aus anderen Zusammenhängen kennen.

DEF Erzeugnis

Erzeugendensystem

endlich erzeugt

zyklische Gruppe

Ordnung eines Elements

1.10. **Definition.** Sei G eine Gruppe und sei $T \subset G$ eine Teilmenge. Dann gibt es die kleinste Untergruppe von G, die T enthält; wir bezeichnen sie mit

$$\langle T\rangle = \langle T\rangle_G = \bigcap\{H \leq G \mid T \subset H\}$$

und nennen sie die *von T erzeugte Untergruppe* von G. Ist $T = \{t_1, t_2, \dots, t_n\}$ endlich, dann schreiben wir statt $\langle T\rangle$ auch $\langle t_1, t_2, \dots, t_n\rangle$.

Ist $\langle T\rangle = G$, dann heißt T ein *Erzeugendensystem* von G. Ist dabei T endlich, dann heißt G *endlich erzeugt*. Gilt $T = \{g\}$, also $G = \langle g\rangle$, dann heißt G *zyklisch*.

Für $g \in G$ heißt $\operatorname{ord}(g) = \#\langle g\rangle \in \mathbb{Z}_{>0} \cup \{\infty\}$ die *Ordnung* von g. ♢

Beachten Sie, dass es in der Gruppentheorie *zwei* Begriffe von „Ordnung“ gibt: Die Ordnung einer (endlichen) Gruppe und die Ordnung eines Elements. Auch wenn es zwischen den beiden einen Zusammenhang gibt (darauf kommen wir bald noch zu sprechen), muss man die beiden Begriffe sorgfältig auseinanderhalten.

1.11. **Beispiel.** Was ist $\langle\ \rangle_G = \langle\emptyset\rangle_G$? In diesem Fall ist die Bedingung $\emptyset \subset H$ stets erfüllt; man bekommt also die kleinste Untergruppe von G, das ist $\{e\}$. ♣ **BSP** $\langle\ \rangle$

In einer multiplikativ geschriebenen Gruppe G definieren wir g^n für $g \in G$ und $n \in \mathbb{Z}$ wie üblich durch

$$g^0 = 1_G\,, \qquad g^{n+1} = g \cdot g^n \quad \text{für } n \geq 0\,, \qquad g^{-n} = (g^{-1})^n \quad \text{für } n > 0.$$

Man beweist dann leicht die „Potenzrechengesetze“

$$g^{m+n} = g^m \cdot g^n \qquad \text{und} \qquad (g^m)^n = g^{mn}$$

durch Induktion und Fallunterscheidung nach den Vorzeichen von m und n.

In additiv geschriebenen (abelschen) Gruppen entspricht der Potenz das Vielfache $n \cdot g$ mit den Regeln $(m+n)\cdot g = m\cdot g + n\cdot g$ und $(mn)\cdot g = m\cdot(n\cdot g)$. Das hatten wir bereits in der „Einführung in die Zahlentheorie und algebraische Strukturen“ eingeführt.

1.12. **Lemma.** *Seien G eine multiplikativ geschriebene Gruppe und $g \in G$. Dann ist*

$$\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}\,.$$

Insbesondere sind zyklische Gruppen abelsch.

Ist $\mathbb{Z} \to G$, $n \mapsto g^n$, injektiv, dann ist $\operatorname{ord}(g) = \infty$. Anderenfalls ist

$$\operatorname{ord}(g) = \min\{n \in \mathbb{Z}_{>0} \mid g^n = 1_G\} < \infty\,.$$

LEMMA zyklische Gruppen

Charakterisierung von $\operatorname{ord}(g)$

Beweis. Die Menge $U = \{g^n \mid n \in \mathbb{Z}\}$ enthält offensichtlich $g = g^1$, und jede g enthaltende Untergruppe von G muss U enthalten. Aus den Potenzrechengesetzen folgt, dass U bereits eine Untergruppe von G ist. Damit muss U die kleinste Untergruppe sein, die g enthält, also ist $\langle g\rangle = U$. Wegen $g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$ ist U abelsch.

Wir betrachten jetzt $f\colon \mathbb{Z} \to G$, $n \mapsto g^n$ mit $\langle g\rangle = \operatorname{im}(f)$. Ist f injektiv, dann ist $\operatorname{ord}(g) = \#\langle g\rangle = \infty$. Anderenfalls gibt es $m < n$ in $\mathbb{Z}$ mit $f(m) = g^m = g^n = f(n)$; es folgt $g^{n-m} = 1_G$, also ist die Menge $\{n \in \mathbb{Z}_{>0} \mid g^n = 1_G\}$ nicht leer. Sei N ihr Minimum. Dann gilt für $n = qN + r$ mit $0 \leq r < N$, dass

$$g^n = g^{qN+r} = (g^N)^q \cdot g^r = 1_G^q \cdot g^r = g^r$$

ist; es folgt $\#\operatorname{im}(f) \leq N$. Auf der anderen Seite müssen alle g^r mit $0 \leq r < N$ verschieden sein, sonst würde man wie oben aus $0 \leq r < r' < N$ mit $g^r = g^{r'}$ den Widerspruch $g^{r'-r} = 1_G$ bekommen. Also gilt auch $\#\operatorname{im}(f) \geq N$ und damit insgesamt $\operatorname{ord}(g) = N$. ❑

Allgemeiner kann man sich überlegen, dass $\langle T\rangle$ genau aus allen endlichen Produkten beliebiger Länge von Elementen von T und deren Inversen besteht. Im Allgemeinen lässt sich das nicht mehr wie bei abelschen Gruppen zu Linearkombinationen vereinfachen, da etwa xyz, xzy, yxz usw. alle verschieden sein können. Dazu beachte man die folgenden Rechenregeln, die in allen Gruppen gelten:

$$(xy)^{-1} = y^{-1}x^{-1} \qquad \text{und} \qquad (x^{-1})^{-1} = x\,.$$

Daraus folgt, dass die Menge der Produkte wie oben nicht nur unter der Verknüpfung (das sollte klar sein), sondern auch unter der Inversenbildung abgeschlossen ist. Das neutrale Element ist als leeres Produkt ebenfalls enthalten.

Wir bringen noch ein paar Beispiele für Ordnungen von Gruppen.

1.13. **Beispiele.** **BSP** Ordnung **DEF** Diedergruppe

(1) Die Ordnung der *Diedergruppe* D_n, also der Gruppe der Bewegungen der Ebene, die ein reguläres n-Eck invariant lassen, ist $2n$, denn ihre Elemente sind n Drehungen (um Vielfache von $2\pi/n$ um den Mittelpunkt des n-Ecks) und n Spiegelungen (an Geraden durch den Mittelpunkt des n-Ecks; falls n ungerade ist, gehen diese Geraden jeweils durch einen Eckpunkt und den gegenüberliegenden Kantenmittelpunkt, falls n gerade ist, gehen $n/2$ dieser Geraden durch zwei gegenüberliegende Ecken und die anderen $n/2$ Geraden durch zwei gegenüberliegende Kantenmittelpunkte). Diese Gruppe enthält (z.B.) Elemente der Ordnung n und der Ordnung 2.

(2) Ist G eine endliche Gruppe und ist $g \in G$ ein Element mit $\operatorname{ord}(g) = \#G$, dann ist $G = \langle g \rangle$ zyklisch.

(3) Ist F ein endlicher Körper mit $\#F = q$, dann gilt (Übung)

$$\#\operatorname{GL}(2, F) = (q^2 - 1)(q^2 - q)\,. \qquad \clubsuit$$

1.14. **Definition.** Sei G eine Gruppe und seien $A, B \subset G$ zwei Teilmengen. Wir schreiben **DEF** Produkt von Teilmengen

$$AB = \{ab \mid a \in A, b \in B\}$$

für das elementweise Produkt der Mengen A und B. Im Fall $A = \{a\}$ schreiben wir auch aB, im Fall $B = \{b\}$ entsprechend Ab. $\diamondsuit$

1.15. **Beispiel.** Sind U_1 und U_2 Untergruppen von G, dann muss U_1U_2 nicht unbedingt ebenfalls eine Untergruppe sein. Zum Beispiel können wir in $G = S_3$ die Untergruppen $U_1 = \langle \tau_1 \rangle$ und $U_2 = \langle \tau_2 \rangle$ betrachten, wobei τ_1 die Elemente 1 und 2 und τ_2 die Elemente 2 und 3 der Menge $\{1, 2, 3\}$ vertauscht. Dann ist **BSP** U_1U_2 keine Untergruppe

$$U_1U_2 = \{\mathrm{id}, \tau_1, \tau_2, \tau_1 \circ \tau_2\}\,;$$

diese Menge ist weder unter der Verknüpfung noch unter der Inversenbildung abgeschlossen, da $\tau_2 \circ \tau_1 = (\tau_1 \circ \tau_2)^{-1}$ nicht in ihr enthalten ist. ($\tau_1 \circ \tau_2$ hat den Effekt $1 \mapsto 2 \mapsto 3 \mapsto 1$, während $\tau_2 \circ \tau_1$ den Effekt $1 \mapsto 3 \mapsto 2 \mapsto 1$ hat.)

Wir werden bald eine Bedingung kennenlernen, die garantiert, dass U_1U_2 tatsächlich eine Untergruppe ist. $\clubsuit$

Eine Untergruppe einer Gruppe G führt zu einer Aufteilung von G in Teilmengen.

$*$ 1.16. **Definition.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Für $g \in G$ heißt gU die *Linksnebenklasse von g bezüglich U* und Ug die *Rechtsnebenklasse von g bezüglich U*. Wir schreiben $G/U = \{gU \mid g \in G\}$ für die Menge der Linksnebenklassen bezüglich U in G und $U\backslash G = \{Ug \mid g \in G\}$ für die Menge der Rechtsnebenklassen bezüglich U in G. **DEF** Nebenklasse $\diamondsuit$

1.17. **Lemma.** *Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Für Elemente $g, h \in G$ sind äquivalent:*

LEMMA Nebenklassen bilden Partition

(1) $h^{-1}g \in U$,

(2) $g \in hU$,

(3) $gU \subset hU$,

(4) $gU = hU$,

(5) $gU \cap hU \neq \emptyset$.

Insbesondere definiert $g \sim h \iff gU = hU$ eine Äquivalenzrelation auf G; G/U ist die Menge der zugehörigen Äquivalenzklassen.

Natürlich gelten die entsprechenden Aussagen auch für *Rechts*nebenklassen Ug.

Beweis. Wir zerlegen den Beweis in mehrere Schritte.

„(1) $\Rightarrow$ (2)“: $h^{-1}g \in U \Rightarrow \exists u \in U : h^{-1}g = u \Rightarrow \exists u \in U : g = hu \Rightarrow g \in hU$.

„(2) $\Rightarrow$ (3)“: $g \in hU$ bedeutet $g = hu$ für ein $u \in U$; es folgt für $u' \in U$ beliebig, dass $gu' = (hu)u' = h(uu') \in hU$ ist. Das bedeutet $gU \subset hU$.

„(3) $\Rightarrow$ (5)“ ist trivial, da $gU \neq \emptyset$.

„(5) $\Rightarrow$ (1)“: Aus (5) folgt $gu_1 = hu_2$ mit geeigneten $u_1, u_2 \in U$, also $h^{-1}g = u_2 u_1^{-1} \in U$ und damit (1).

„(1) $\Rightarrow$ (4)“: Aus (1) folgt auch $g^{-1}h = (h^{-1}g)^{-1} \in U$ und damit nach dem schon Gezeigten $gU \subset hU$ und $hU \subset gU$, also $gU = hU$.

„(4) $\Rightarrow$ (3)“ ist trivial. ❑

1.18. **Lemma.** *Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann wird durch $x \mapsto x^{-1}$ eine Bijektion*

LEMMA G/U und $U\backslash G$

$$G/U \longrightarrow U\backslash G\,, \qquad gU \longmapsto Ug^{-1}$$

induziert. Insbesondere gilt $\#(G/U) = \#(U\backslash G)$.

Beweis. Übung. ❑

1.19. **Definition.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann heißt $\#(G/U) = \#(U\backslash G)$ der *Index* $(G : U)$ der Untergruppe U in G. ♢

DEF Index

Der Index kann endlich sein, auch wenn G und U unendlich sind. Zum Beispiel hat $\mathbb{Z}$ die Untergruppe $n\mathbb{Z}$ (für jedes $n \in \mathbb{Z}_{>0}$) vom Index n.

1.20. **Lemma.** *Seien G eine Gruppe, $U \leq G$ und $g, h \in G$. Dann definiert $x \mapsto (hg^{-1})x$ eine Bijektion $gU \to hU$. Insbesondere gilt, dass alle (Links-)Nebenklassen bzgl. U dieselbe Anzahl von Elementen haben.*

LEMMA $\#gU = \#hU$

Beweis. Die Abbildung schickt $gu \in gU$ auf $hg^{-1} \cdot gu = hu \in hU$, ist also wohldefiniert. Es gibt eine analoge Abbildung $x \mapsto gh^{-1} \cdot x$ von hU nach gU; die Abbildungen sind offensichtlich invers zueinander. ❑

* 1.21. **Folgerung.** *Seien G eine endliche Gruppe und U eine Untergruppe von G. Dann gilt $\#G = (G : U) \cdot \#U$. Insbesondere ist $\#U$ ein Teiler von $\#G$.*

FOLG Satz von Lagrange

Beweis. Es gilt $\#G = \sum_{gU \in G/U} \#gU$. Da nach Lemma 1.20 alle Nebenklassen gU dieselbe Kardinalität $\#gU = \#U$ haben, folgt die Behauptung. ❑

1.22. **Folgerung.** *Seien G eine endliche Gruppe und $g \in G$. Dann ist $\operatorname{ord}(g)$ ein Teiler der Gruppenordnung $\#G$. Insbesondere gilt $g^{\#G} = 1$.*

FOLG $\operatorname{ord}(g) \mid \#G$

Beweis. Wir wenden Folgerung 1.21 auf $U = \langle g \rangle$ an. Es gilt dann $\#G = m \operatorname{ord}(g)$ mit $m \in \mathbb{Z}$. Es folgt $g^{\#G} = (g^{\operatorname{ord}(g)})^m = 1^m = 1$. ❑

1.23. **Folgerung.** *Sei p eine Primzahl. Für alle ganzen Zahlen a mit $p \nmid a$ gilt*

$$a^{p-1} \equiv 1 \bmod p\,.$$

FOLG Kleiner Satz von Fermat

Beweis. Wir wenden Folgerung 1.22 auf die multiplikative Gruppe $\mathbb{F}_p^\times$ an. ❑

Das lässt sich verallgemeinern: Anwendung auf die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ der Ordnung $\phi(n)$ (Eulersche ϕ-Funktion) liefert:

1.24. **Folgerung.** *Seien $n \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ mit $a \perp n$. Dann gilt*

$$a^{\phi(n)} \equiv 1 \bmod n\,.$$

FOLG Satz von Euler

Dieser Satz ist recht nützlich, wenn man Potenzen modulo n berechnen will. Wie findet man zum Beispiel die Restklasse von $7^{11^{13}}$ mod 15? Der Satz von Euler sagt uns, dass $7^{\phi(15)} = 7^8 \equiv 1 \bmod 15$ ist; es kommt also nur auf den Exponenten 11^{13} mod 8 an. Der Satz sagt dann wieder, dass $11^4 \equiv 1 \bmod 8$ ist (tatsächlich gilt ja sogar $a^2 \equiv 1 \bmod 8$ für alle ungeraden ganzen Zahlen a; der Satz ist also nicht „scharf“ — im Gegensatz zum kleinen Satz von Fermat, wie wir noch sehen werden), also ist $11^{13} \equiv 11^1 \equiv 3 \bmod 8$ und damit

$$7^{11^{13}} \equiv 7^3 = 343 \equiv -2 \bmod 15\,.$$

Man kann sich jetzt die Frage stellen, welche Teiler der Gruppenordnung als Ordnung eines Elements auftreten. Das sind im Allgemeinen sicher nicht alle, denn zum Beispiel folgt aus $\operatorname{ord}(g) = \#G$, dass die Gruppe G zyklisch ist. (In diesem Fall treten tatsächlich alle Teiler von $\#G$ als Elementordnung auf — Übung!) Man kann aber folgende allgemeine Aussage machen.

1.25. **Satz.** *Sei G eine endliche Gruppe und sei p ein Primteiler von $\#G$. Dann gibt es in G (mindestens) ein Element der Ordnung p.* **SATZ** Satz von Cauchy

Beweis. Der Beweis verwendet einen Trick: Wir betrachten die Menge

$$M = \{(g_1, g_2, \dots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = 1_G\}\,.$$

Da das letzte Element g_p in so einem Tupel eindeutig durch die ersten $p-1$ Elemente bestimmt ist ($g_p = (g_1 \cdots g_{p-1})^{-1}$), gilt $\#M = (\#G)^{p-1}$; wegen $p \mid \#G$ (und $p - 1 \geq 1$) ist das eine durch p teilbare Zahl.

Auf der anderen Seite können wir M aufteilen in eine Menge

$$M_1 = \{(g, g, \dots, g) \mid (g, g, \dots, g) \in M\}$$

und eine Menge $M_2 = M \setminus M_1$. Die Elemente von M_2 können wir zu je p zusammenfassen:

$$(g_1, g_2, \dots, g_p), \quad (g_2, g_3, \dots, g_p, g_1), \quad \dots, \quad (g_p, g_1, g_2, \dots, g_{p-1})$$

(Man beachte, dass $(g_2, g_3, \dots, g_p, g_1)$ wieder in M ist, denn

$$g_1 g_2 \cdots g_p = 1_G \implies g_2 \cdots g_p = g_1^{-1} \implies g_2 \cdots g_p g_1 = 1_G\,.)$$

Diese Elemente sind alle verschieden, denn die Periode der Folge

$$g_1, g_2, \dots, g_p, g_1, g_2, \dots, g_p, g_1, \dots$$

kann nur p oder 1 sein, und M_2 enthält genau die Elemente von M nicht, bei denen die Periode 1 ist. Es folgt, dass $\#M_2$ durch p teilbar ist. Dann muss aber auch $\#M_1 = \#M - \#M_2$ durch p teilbar sein. M_1 enthält mindestens das Element $(1_G, 1_G, \dots, 1_G)$; es folgt, dass M_1 noch mindestens $p - 1 > 0$ weitere Elemente enthalten muss. Für so ein Element $(g, g, \dots, g)$ gilt dann aber $g \neq 1_G$ und $g^p = 1_G$, also $\mathrm{ord}(g) = p$. ❑

Später werden wir sehen, dass dieser Beweis eine Anwendung der sogenannten Bahnengleichung für die Operation (durch zyklische Vertauschung der Komponenten) der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ auf M ist.

Zum besseren Verständnis des Arguments im Beweis oben betrachten wir periodische Folgen etwas genauer.

1.26. **Definition.** Sei X eine Menge und $\boldsymbol{x} = (x_n)_{n\geq 0}$ eine Folge von Elementen von X. Eine ganze Zahl $m \geq 0$ heißt *eine Periode* von $\boldsymbol{x}$, wenn für alle $n \in \mathbb{Z}_{\geq 0}$ gilt, dass $x_{n+m} = x_n$ ist. ♢ **DEF** Periode

1.27. **Lemma.** *Sei $\boldsymbol{x}$ wie oben. Dann besteht die Menge der Perioden von $\boldsymbol{x}$ genau aus allen nichtnegativen Vielfachen einer Zahl $m_0 \in \mathbb{Z}_{\geq 0}$.* **LEMMA** Perioden

Beweis. $m = 0$ ist immer eine Periode von $\boldsymbol{x}$. Wenn es keine weiteren Perioden gibt, dann gilt die Aussage mit $m_0 = 0$. Anderenfalls sei m_0 die kleinste positive Periode von $\boldsymbol{x}$. Es ist klar, dass jedes positive Vielfache einer Periode von $\boldsymbol{x}$ wieder eine Periode von $\boldsymbol{x}$ ist; insbesondere sind alle Vielfachen von m_0 Perioden von $\boldsymbol{x}$. Sei nun m eine beliebige Periode von $\boldsymbol{x}$. Wir müssen zeigen, dass m ein Vielfaches von m_0 ist. Dazu schreiben wir $m = qm_0 + r$ mit $q \geq 0$ und $0 \leq r < m_0$. Dann gilt für alle $n \geq 0$:

$$x_{n+r} = x_{n+qm_0+r} = x_{n+m} = x_n\,,$$

weil sowohl qm_0 als auch m Perioden sind. Also ist auch r eine Periode von $\boldsymbol{x}$. Da m_0 die kleinste positive Periode ist, muss dann $r = 0$ sein; das bedeutet $m = qm_0$ wie gewünscht. ❑

1.28. **Definition.** Seien $\boldsymbol{x}$ und m_0 wie oben. Ist $m_0 > 0$, dann heißt die Folge $\boldsymbol{x}$ *periodisch* und m_0 heißt die *minimale Periode* (oder auch einfach *die Periode*) von $\boldsymbol{x}$. ♢ DEF periodisch minimale Periode

1.29. **Folgerung.** *Seien G eine Gruppe und $g \in G$ ein Element endlicher Ordnung. Für $n \in \mathbb{Z}$ gilt dann* FOLG $g^n = 1$

$$g^n = 1_G \iff \operatorname{ord}(g) \mid n\,.$$

Beweis. Wir können $n \geq 0$ annehmen (sonst ersetze man n durch $-n$). Wir betrachten die Folge $(g^n)_{n\geq 0}$ in G. Die Zahlen $m \geq 0$ mit $g^m = 1_G$ sind dann genau die Perioden dieser Folge: Ist m eine Periode, dann muss $g^m = g^0 = 1_G$ sein, und ist $g^m = 1_G$, dann gilt $g^{n+m} = g^n \cdot g^m = g^n \cdot 1_G = g^n$ für alle $n \geq 0$. Nach Lemma 1.12 ist dann $\operatorname{ord}(g)$ gerade die minimale Periode dieser Folge. Die Behauptung folgt nun aus Lemma 1.27. ❑

Damit die bisher eingeführten Begriffe etwas konkreter fassbar werden, betrachten wir als (relativ) einfaches Beispiel die Gruppe S_3.

1.30. **Beispiel.** Wir notieren für dieses Beispiel eine Permutation $\sigma \in S_n$ in der Form $[\sigma(1)\sigma(2)\ldots\sigma(n)]$ (wir werden uns später noch ausführlicher mit Permutationen beschäftigen und dann auch andere Schreibweisen kennenlernen). Dann ist zum Beispiel in S_3 $\mathrm{id} = [123]$ und BSP S_3

$$S_3 = \{[123], [213], [321], [132], [231], [312]\}\,.$$

Die Ordnungen dieser Elemente sind (in der angegebenen Reihenfolge) $1, 2, 2, 2, 3, 3$. Wir sehen also, dass es Elemente der Ordnungen 2 und 3 gibt, wie vom Satz von Cauchy 1.25 vorhergesagt. Da S_3 nicht abelsch, also insbesondere nicht zyklisch ist, kann es kein Element der Ordnung 6 geben.

Welche Untergruppen hat die S_3? Abgesehen von den *trivialen Untergruppen* $\{\mathrm{id}\}$ und S_3 muss eine Untergruppe nach dem Satz von Lagrange 1.21 die Ordnung 2 oder 3 haben. Eine Untergruppe der Ordnung 2 besteht aus der Identität und einem Element der Ordnung 2, und eine Untergruppe der Ordnung 3 besteht aus der Identität und zwei (zueinander inversen) Elementen der Ordnung 3. Es gibt also drei Untergruppen

$$\{[123], [213]\}, \quad \{[123], [321]\}, \quad \{[123], [132]\}$$

der Ordnung 2 und eine Untergruppe

$$\{[123], [231], [312]\}$$

der Ordnung 3. (Für einen Primteiler p der Ordnung einer endlichen Gruppe G gilt stets, dass die Anzahl u_p der Untergruppen der Ordnung p die Kongruenz $u_p \equiv 1 \bmod p$ erfüllt; das kann man aus dem Satz von Cauchy folgern. Wir werden diese Aussage später in stärkerer Form beweisen.)

Nach der Indexformel im Satz von Lagrange gilt dann, dass die Untergruppen der Ordnung 2 den Index 3 und die Untergruppen der Ordnung 3 den Index 2 haben. Ist $U_2 = \{[123], [213]\}$, dann sind die verschiedenen Linksnebenklassen von U_2

$$U_2 = \{[123], [213]\}, \quad [231]U_2 = \{[231], [321]\}, \quad [312]U_2 = \{[312], [132]\}$$

und die Rechtsnebenklassen sind

$$U_2 = \{[123], [213]\}, \quad U_2[231] = \{[231], [132]\}, \quad U_2[312] = \{[312], [321]\};$$

man sieht, dass sie von den Linksnebenklassen (abgesehen natürlich von U_2 selbst) verschieden sind. Für die Untergruppe U_3 der Ordnung 3 gibt es jeweils nur eine nichttriviale (also $\neq U_3$) Links- und Rechtsnebenklasse, die gleich $S_3 \setminus U_3$ sein muss. Untergruppen mit der Eigenschaft, dass ihre Links- und Rechtsnebenklassen übereinstimmen, werden wir noch genauer betrachten. ♣

2. Gruppenhomomorphismen

Als nächstes betrachten wir die strukturerhaltenden Abbildungen von Gruppen.

* 2.1. **Definition.** Seien G, G' zwei Gruppen. Eine Abbildung $\phi\colon G \to G'$ heißt ein *Gruppenhomomorphismus* (oder auch nur *Homomorphismus*), wenn für alle $g_1, g_2 \in G$ gilt, dass $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ ist.

DEF Gruppenhomomorphismus

Wie üblich nennt man ϕ einen *Monomorphismus*, *Epimorphismus*, *Isomorphismus*, *Endomorphismus* bzw. *Automorphismus*, falls ϕ injektiv, ϕ surjektiv, ϕ bijektiv, $G = G'$ bzw. ϕ bijektiv und $G = G'$ ist. Die Gruppen G und G' heißen *isomorph* und wir schreiben $G \cong G'$, wenn es einen Isomorphismus $G \to G'$ gibt. Der *Kern* von ϕ ist definiert als

isomorph

Kern

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_{G'}\}\,.$$

Wir schreiben $\mathrm{Aut}(G)$ für die Menge der Automorphismen von G. ♢

$\mathrm{Aut}(G)$

Aus $\phi(1_G) = \phi(1_G^2) = \phi(1_G)^2$ folgt $\phi(1_G) = 1_{G'}$, und aus

$$1_{G'} = \phi(1_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

folgt $\phi(g^{-1}) = \phi(g)^{-1}$; ein Homomorphismus erhält also wirklich die komplette Gruppenstruktur. Man sieht auch leicht, dass für einen Isomorphismus ϕ die Umkehrabbildung ϕ^{-1} ebenfalls ein Isomorphismus ist und dass die Komposition zweier Gruppenhomomorphismen wieder ein Gruppenhomomorphismus ist.

2.2. **Lemma.** *Sei $\phi\colon G \to G'$ ein Gruppenhomomorphismus. Dann gilt:*

LEMMA Eigensch. von Gruppenhomomorphismen

(1) *Ist $U \leq G$, dann ist $\phi(U) \leq G'$. Insbesondere ist das Bild von ϕ eine Untergruppe von G'.*

(2) *Ist $U' \leq G'$, dann ist $\phi^{-1}(U') \leq G$. Insbesondere ist der Kern von ϕ eine Untergruppe von G.*

(3) *ϕ ist genau dann injektiv, wenn $\ker(\phi)$ trivial ist.*

Beweis.

(1) $1_{G'} = \phi(1_G) \in \phi(U)$; mit $u_1' = \phi(u_1)$ und $u_2' = \phi(u_2)$ sind auch $u_1'u_2' = \phi(u_1u_2)$ und $(u_1')^{-1} = \phi(u_1^{-1})$ in $\phi(U)$.

(2) $\phi(1_G) = 1_{G'}$, also ist $1_G \in \phi^{-1}(U')$. Sind $u_1, u_2 \in \phi^{-1}(U')$, das bedeutet $\phi(u_1), \phi(u_2) \in U'$, dann folgt $\phi(u_1u_2) = \phi(u_1)\phi(u_2) \in U'$ und $\phi(u_1^{-1}) = \phi(u_1)^{-1} \in U'$ und damit $u_1u_2, u_1^{-1} \in \phi^{-1}(U')$.

(3) „⇒“ ist trivial. Für die Gegenrichtung sei $\ker(\phi) = \{1_G\}$. Dann gilt für $g_1, g_2 \in G$:

$$\begin{aligned}\phi(g_1) = \phi(g_2) &\Rightarrow \phi(g_1g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = 1_{G'}\\ &\Rightarrow g_1g_2^{-1} \in \ker(\phi) = \{1_G\}\\ &\Rightarrow g_1g_2^{-1} = 1_G \Rightarrow g_1 = g_2\,.\end{aligned}$$

❑

Wir werden im nächsten Abschnitt sehen, dass Kerne von Homomorphismen sogar spezielle Untergruppen sind.

2.3. **Beispiele.** Wir bringen eine Reihe von Beispielen von Gruppenhomomorphismen und machen dabei gleich noch einige Definitionen.

BSP Gruppenhomomorphismen

(1) Für beliebige Gruppen G und G' gibt es immer den *trivialen Homomorphismus* $G \to G'$, $g \mapsto 1_{G'}$.

(2) Die Determinante ist multiplikativ. Das bedeutet, dass für jeden Körper K und jede Zahl $n \in \mathbb{Z}_{\geq 0}$ die Abbildung $\det\colon \mathrm{GL}(n,K) \to K^\times$ ein Gruppenhomomorphismus ist. Der Kern wird $\mathrm{SL}(n,K)$ (oder $\mathrm{SL}_n(K)$) geschrieben und heißt *spezielle lineare Gruppe*. Für $n \geq 1$ ist det ein Epimorphismus.

DEF $\mathrm{SL}(n,K)$

(3) Orthogonale Matrizen haben Determinante ± 1, also haben wir in diesem Fall einen Homomorphismus $\det\colon \mathrm{O}(n) \to \{\pm 1\}$. Sein Kern ist $\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}(n,\mathbb{R})$, die *spezielle orthogonale Gruppe*. Zum Beispiel besteht $\mathrm{SO}(2)$ gerade aus den Drehungen der Ebene um den Ursprung, während $\mathrm{O}(2)$ noch zusätzlich die Spiegelungen an Ursprungsgeraden enthält.

DEF $\mathrm{SO}(n)$

(4) Für eine Permutation $\sigma \in S_n$ sei $P(\sigma) \in \mathrm{GL}(n,\mathbb{R})$ die zugehörige Permutationsmatrix (d.h., der Eintrag in Zeile $\sigma(i)$ und Spalte i ist 1, für $i = 1,\dots,n$; alle anderen Einträge sind 0), sodass gilt $P(\sigma)\mathbf{e}_i = \mathbf{e}_{\sigma(i)}$, wobei $(\mathbf{e}_1,\dots,\mathbf{e}_n)$ die Standardbasis von $\mathbb{R}^n$ ist. Dann ist $P\colon S_n \to \mathrm{GL}_n(\mathbb{R})$ ein Gruppenhomomorphismus. Das Bild von P liegt in der orthogonalen Gruppe $\mathrm{O}(n)$, denn $P(\sigma)^\top = P(\sigma^{-1})$, also gilt $P(\sigma)P(\sigma)^\top = I_n$.

(5) Die Komposition $\mathrm{sign} = \det \circ P\colon S_n \to \{\pm 1\}$ ergibt das *Signum* einer Permutation. Für $n \geq 2$ ist diese Abbildung surjektiv, denn eine *Transposition* (also eine Permutation, die zwei Elemente vertauscht und alle anderen fest lässt) hat Signum -1. Der Kern dieses Homomorphismus heißt die *alternierende Gruppe* A_n (häufig auch $\mathfrak{A}_n$ geschrieben). Die alternierende Gruppe besteht also aus allen *geraden* Permutationen (denen mit Signum $+1$).

DEF alternierende Gruppe

(6) Das Legendre-Symbol definiert für eine ungerade Primzahl p einen surjektiven Homomorphismus $\mathbb{F}_p^\times \to \{\pm 1\}$, $[a] \mapsto \left(\frac{a}{p}\right)$.

(7) Seien G eine Gruppe und $g \in G$. Dann ist $c_g\colon G \to G$, $x \mapsto gxg^{-1}$ ein Automorphismus von G. Solche Automorphismen heißen *innere Automorphismen* von G; die Abbildung c_g heißt die *Konjugation* mit g. Wir zeigen, dass c_g ein Homomorphismus ist:

DEF innerer Automorphismus

$$c_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = gxg^{-1} \cdot gyg^{-1} = c_g(x)c_g(y)\,.$$

Offensichtlich ist $c_{g^{-1}}$ die zu c_g inverse Abbildung, also ist c_g sogar ein Isomorphismus. c_g ist die Identität id_G genau dann, wenn $gxg^{-1} = x$, also $gx = xg$ gilt für alle $x \in G$. Das bedeutet gerade, dass g ein Element des *Zentrums*

DEF Zentrum

$$Z(G) = \{g \in G \mid gx = xg \text{ für alle } x \in G\}$$

von G ist. Zum Beispiel hat eine abelsche Gruppe keine inneren Automorphismen außer der Identität, denn dann ist $Z(G) = G$.

(8) Ist G eine Gruppe und $g \in G$, dann ist $\mathbb{Z} \to G$, $n \mapsto g^n$ ein Homomorphismus. Sein Kern ist trivial, falls g unendliche Ordnung hat, sonst ist der Kern $\mathrm{ord}(g)\mathbb{Z}$, siehe Lemma 1.12 und Folgerung 1.29. ♣

Ganz genauso wie in Folgerung 1.8 sieht man:

2.4. **Lemma.** *Sei G eine Gruppe. Dann ist $\mathrm{Aut}(G)$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe.*

LEMMA $\mathrm{Aut}(G)$ ist Gruppe

Beweis. Das folgt sogar direkt aus Lemma 1.7, weil die einzige Bedingung für einen Homomorphismus die Verträglichkeit mit der Verknüpfung in der Gruppe ist (das ist eine Abbildung vom Typ (1) mit $n = 2$). ❑

2.5. **Beispiel.** Die Abbildung

$$c\colon G \longrightarrow \mathrm{Aut}(G), \quad g \longmapsto c_g$$

ist ein Gruppenhomomorphismus. Es gilt nämlich für alle $g, h, x \in G$

$$(c_g \circ c_h)(x) = c_g\big(c_h(x)\big) = c_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = c_{gh}(x)\,,$$

also ist $c_g \circ c_h = c_{gh}$. Es gilt $\ker(c) = Z(G)$, siehe oben; damit ist auch klar, dass $Z(G)$ eine Untergruppe von G ist. ♣

BSP innere Automorphismen

2.6. **Definition.** Sei G eine Gruppe. Die Gruppe $\mathrm{Aut}(G)$ heißt die *Automorphismengruppe* von G. Die Untergruppe $\mathrm{Inn}(G) = \{c_g \mid g \in G\}$ (mit $c_g\colon x \mapsto gxg^{-1}$ wie oben) heißt die *innere Automorphismengruppe* von G. ♢

DEF Automorphismengruppe

Beachte, dass $\mathrm{Inn}(G)$ als Bild des Homomorphismus c aus Beispiel 2.5 tatsächlich eine Untergruppe von $\mathrm{Aut}(G)$ ist.

2.7. **Beispiele.**

BSP Automorphismengruppen

(1) Es gilt $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Denn jede Permutation von $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, die das neutrale Element fest lässt, aber die übrigen drei Elemente beliebig vertauscht, ist ein Automorphismus.

(2) Für $n \geq 3$ ist das Zentrum von S_n trivial: Sei $\tau \in S_n$ eine beliebige Transposition, τ vertausche etwa r und s. Wir setzen $T = \{r, s\}$. Für $\sigma \in S_n$ gilt dann

$$\sigma \circ \tau = \tau \circ \sigma \iff \sigma(T) = T\,.$$

Die Richtung „$\Leftarrow$“ ist leicht zu sehen und für unser Argument nicht relevant. Für die Gegenrichtung nehmen wir $\sigma(T) \neq T$ an, also ohne Einschränkung $\sigma(r) \notin T$. Dann ist

$$(\sigma \circ \tau)(r) = \sigma\big(\tau(r)\big) = \sigma(s) \quad \text{und} \quad (\tau \circ \sigma)(r) = \tau\big(\sigma(r)\big) = \sigma(r) \neq \sigma(s)\,,$$

also sind $\sigma \circ \tau$ und $\tau \circ \sigma$ verschieden.

Ist $\sigma \in Z(S_n)$ und $n \geq 3$, dann vertauscht σ mit allen Transpositionen τ. Ist $i \in \{1, 2, \ldots, n\}$, dann gibt es zwei weitere Elemente j und k (hier brauchen wir $n \geq 3$!). Aus obiger Äquivalenz folgt, dass $\sigma(\{i, j\}) = \{i, j\}$ und $\sigma(\{i, k\}) = \{i, k\}$ ist, was nur geht, wenn $\sigma(i) = i$ ist. Da hier i beliebig war, folgt $\sigma = \mathrm{id}$. Damit ist $Z(S_n) = \{\mathrm{id}\}$ trivial wie behauptet.

Es folgt, dass für $n \geq 3$ die oben betrachtete Abbildung $c\colon S_n \to \mathrm{Aut}(S_n)$ injektiv ist; damit ist $\mathrm{Inn}(S_n) \cong S_n$. Für $n \leq 2$ sind $\mathrm{Aut}(S_n)$ und $\mathrm{Inn}(S_n)$ beide trivial. ♣

Man kann auch zeigen, dass $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$ ist für alle $n \geq 3$ mit $n \neq 6$. Die symmetrische Gruppe S_6 hat dagegen äußere (also nicht-innere) Automorphismen.

3. Normalteiler und Faktorgruppen

Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Wie in anderen Situationen auch, würden wir gerne auf der Menge G/U (oder $U\backslash G$) eine Gruppenstruktur definieren, sodass die kanonische Abbildung $G \to G/U$, $g \mapsto gU$, ein Homomorphismus wird. Dazu müssten wir definieren $gU \cdot g'U = (gg')U$. Hier ergibt sich aber ein Problem: Diese Verknüpfung ist nicht immer wohldefiniert. Wenn wir $g = 1_G$ nehmen, dann ist jedes $u \in U$ ein anderer Repräsentant von $gU = U$, also sollte $ug' \in g'U$ sein für alle $u \in U$. Das bedeutet $Ug' \subset g'U$. Das muss für alle $g' \in G$ gelten, also insbesondere auch für $(g')^{-1}$; zusammen folgt $Ug' = g'U$: Links- und Rechtsnebenklassen müssen übereinstimmen. Dies ist jedoch nicht immer der Fall (siehe Beispiel 1.30 für $G = S_3$). Daher führt man einen neuen Begriff ein.

* 3.1. **Definition.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann heißt U ein *Normalteiler* von G oder *normal* in G, wenn für alle $g \in G$ gilt $gU = Ug$. Man schreibt dann $U \triangleleft G$. ♢

DEF Normalteiler

Äquivalent dazu ist $gUg^{-1} = U$ oder auch nur $gUg^{-1} \subset U$ für alle $g \in G$ (aus $gUg^{-1} \subset U$ und $g^{-1}Ug \subset U$ folgt $gUg^{-1} = U$). Normalteiler sind also Untergruppen, die von allen Konjugationsabbildungen c_g als Menge fest gelassen werden.

3.2. **Beispiele.**

BSP Normalteiler

(1) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

(2) Ist G eine Gruppe und $U \leq G$ mit $(G : U) = 2$, dann ist U ein Normalteiler. Denn für gU bzw. Ug gibt es nur die beiden Möglichkeiten U und $G \setminus U$; aus $gU \cap Ug \neq \emptyset$ folgt also $gU = Ug$. Zum Beispiel ist für $n \geq 2$ die alternierende Gruppe A_n ein Normalteiler von S_n, denn $(S_n : A_n) = 2$ nach dem Homomorphiesatz 3.6 unten.

(3) Sei $g \in G$ mit $\operatorname{ord}(g) = 2$. Dann ist $\langle g \rangle = \{1_G, g\}$ genau dann ein Normalteiler von G, wenn $g \in Z(G)$ ist. Zum Beispiel sind die Untergruppen der Ordnung 2 von S_3 keine Normalteiler.

DEF trivialer Normalteiler

(4) In jeder Gruppe sind die Untergruppen $\{1_G\}$ und G Normalteiler, die *trivialen Normalteiler* von G.

(5) In jeder Gruppe G gilt $Z(G) \triangleleft G$, denn für $g \in G$ und $z \in Z(G)$ gilt $gzg^{-1} = z \in Z(G)$ (hier gilt die Bedingung für einen Normalteiler sogar elementweise). ♣

3.3. **Lemma.** *Sei $\phi\colon G \to G'$ ein Gruppenhomomorphismus.*

LEMMA Homomorphismen und Normalteiler

(1) *Ist $N' \triangleleft G'$, dann ist auch $\phi^{-1}(N') \triangleleft G$. Insbesondere ist $\ker(\phi)$ ein Normalteiler von G.*

(2) *Ist ϕ **surjektiv** und $N \triangleleft G$, dann gilt auch $\phi(N) \triangleleft G'$.*

Beweis.

(1) Wir wissen bereits (Lemma 2.2), dass $\phi^{-1}(N')$ eine Untergruppe von G ist. Außerdem gilt für $g \in G$ und $n \in \phi^{-1}(N')$:

$$\phi\big(gng^{-1}\big) = \phi(g)\phi(n)\phi(g)^{-1} \in \phi(g)N'\phi(g)^{-1} = N'$$

und damit

$$g\phi^{-1}(N')g^{-1} \subset \phi^{-1}(N')\,.$$

(2) Wir wissen bereits, dass $\phi(N)$ eine Untergruppe von G' ist (Lemma 2.2). Da ϕ surjektiv ist, lässt sich jedes $g' \in G'$ schreiben als $\phi(g)$ mit $g \in G$. Damit gilt dann

$$g'\phi(N)(g')^{-1} = \phi(g)\phi(N)\phi(g^{-1}) = \phi(gNg^{-1}) = \phi(N)\,. \qquad \text{❑}$$

Wie schon angedeutet, haben Normalteiler $N \triangleleft G$ die Eigenschaft, dass man auf der Menge G/N in natürlicher Weise eine Gruppenstruktur definieren kann.

* 3.4. **Satz.** *Seien G eine Gruppe und N ein Normalteiler von G. Dann definiert $gN \cdot hN = (gN)(hN) = (gh)N$ eine Gruppenstruktur auf G/N, sodass die kanonische Abbildung $\phi\colon G \to G/N$, $g \mapsto gN$, ein Homomorphismus ist. Es gilt $\ker(\phi) = N$.* **SATZ** Faktorgruppe

Beweis. Wegen der Assoziativität der Verknüpfung, und weil N Normalteiler ist, gilt $(gN)(hN) = g(Nh)N = g(hN)N = (gh)(NN) = (gh)N$; damit ist auch klar, dass diese Verknüpfung wohldefiniert ist und dass $\phi(gh) = \phi(g)\phi(h)$ gilt. Letzteres, zusammen mit der Surjektivität von ϕ, erzwingt die Gültigkeit der Gruppenaxiome für G/N. Dass $\ker(\phi) = N$ ist, folgt aus

$$\phi(g) = 1_{G/N} = N \iff gN = N \iff g \in N\,. \qquad \text{❑}$$

3.5. **Definition.** Die Gruppe G/N heißt die *Faktorgruppe* (oder *Quotientengruppe*) von G nach (oder modulo) N; ϕ heißt *kanonischer Epimorphismus*. ♢ **DEF** Faktorgruppe

Wir sehen also, dass die Normalteiler von G genau die Kerne von Gruppenhomomorphismen mit Definitionsbereich G sind. Das ist vergleichbar mit der Situation bei Ringen, wo die Kerne genau die Ideale sind (und nicht etwa die Unterringe).

Wir haben den üblichen Homomorphiesatz.

* 3.6. **Satz.** *Sei $\phi\colon G \to G'$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus*

$$\tilde{\phi}\colon G/\ker(\phi) \longrightarrow \operatorname{im}(\phi)\,, \qquad g\ker(\phi) \longmapsto \phi(g)\,.$$

Insbesondere gilt $(G : \ker(\phi)) = \#\operatorname{im}(\phi)$. Für jeden Normalteiler $N \triangleleft G$ mit $N \subset \ker(\phi)$ erhalten wir einen induzierten Homomorphismus $G/N \to G'$ mit Bild $\operatorname{im}(\phi)$. **SATZ** Homomorphiesatz für Gruppen

Beweis. Wir zeigen zuerst die letzte Aussage: $\phi_N\colon G/N \to G'$, $gN \mapsto \phi(g)$ ist wohldefiniert, denn für $g' = gn$ mit $n \in N$ gilt $\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g)$, da $\phi|_N = 1_{G'}$. Außerdem ist ϕ_N ein Homomorphismus, denn

$$\phi_N\big((gN)(hN)\big) = \phi_N\big((gh)N\big) = \phi(gh) = \phi(g)\phi(h) = \phi_N(gN)\phi_N(hN)\,.$$

Es ist auch klar, dass $\operatorname{im}(\phi_N) = \operatorname{im}(\phi)$ ist. Für $N = K := \ker(\phi)$ erhalten wir $\tilde{\phi}$; es bleibt zu zeigen, dass $\tilde{\phi}$ injektiv ist. Es gilt

$$\tilde{\phi}(gK) = 1_{G'} \iff \phi(g) = 1_{G'} \iff g \in K \iff gK = K\,,$$

also besteht der Kern von $\tilde{\phi}$ nur aus dem Element K. Es folgt auch (da $\tilde{\phi}$ bijektiv ist)

$$\big(G : \ker(\phi)\big) = \#\big(G/\ker(\phi)\big) = \#\operatorname{im}(\phi)\,. \qquad \text{❑}$$

BSP $\#\ker(\phi)$

3.7. **Beispiel.** Eine typische Anwendung des Satzes ist die Berechnung der Ordnung von $\ker(\phi)$, denn es gilt (wenn G endlich ist)

$$\#\ker(\phi) = \frac{\#G}{(G:\ker(\phi))} = \frac{\#G}{\#\operatorname{im}(\phi)}\,.$$

Zum Beispiel ist $\#A_n = \frac{n!}{2}$ für $n \geq 2$, denn A_n ist der Kern des surjektiven Homomorphismus $\operatorname{sign}\colon S_n \to \{\pm 1\}$. Analog findet man

$$\#\operatorname{SL}(2,\mathbb{F}_p) = \frac{\#\operatorname{GL}(2,\mathbb{F}_p)}{\#\mathbb{F}_p^\times} = \frac{(p^2-1)(p^2-p)}{p-1} = (p^2-1)p = (p-1)p(p+1)\,,$$

denn $\operatorname{SL}(2,\mathbb{F}_p) = \ker(\det\colon \operatorname{GL}(2,\mathbb{F}_p) \to \mathbb{F}_p^\times)$, und det ist in diesem Fall surjektiv. ♣

BSP innere Automorphismen

3.8. **Beispiel.** Satz 3.6 liefert einen Isomorphismus

$$G/Z(G) \xrightarrow{\cong} \operatorname{Inn}(G)\,.$$

Die Gruppe $\operatorname{Inn}(G)$ der inneren Automorphismen einer Gruppe G ist ein Normalteiler der Automorphismengruppe $\operatorname{Aut}(G)$. Dafür ist zu zeigen, dass für jedes $g \in G$ und jeden Automorphismus $\phi \in \operatorname{Aut}(G)$ die Abbildung $\phi \circ c_g \circ \phi^{-1}$ wieder ein innerer Automorphismus ist, also die Form $c_{g'}$ hat für ein $g' \in G$. Es ist für $x \in G$

$$\begin{aligned}(\phi \circ c_g \circ \phi^{-1})(x) &= \phi\big(c_g(\phi^{-1}(x))\big) = \phi\big(g\phi^{-1}(x)g^{-1}\big)\\ &= \phi(g)\phi\big(\phi^{-1}(x)\big)\phi(g^{-1}) = \phi(g)x\phi(g)^{-1}\\ &= c_{\phi(g)}(x)\,,\end{aligned}$$

also gilt $\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}$.

DEF äußere Automorphismengruppe

Die Faktorgruppe $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ heißt die *äußere Automorphismengruppe* von G und wird $\operatorname{Out}(G)$ geschrieben („outer automorphisms“). ♣

Aus dem Homomorphiesatz 3.6 kann man weitere „Isomorphiesätze“ folgern. Einer davon ist gelegentlich nützlich.

FOLG Isomorphie-Satz

3.9. **Folgerung.** *Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $N \lhd G$ ein Normalteiler. Dann ist $NU = UN$ eine Untergruppe von G, $N \cap U$ ist ein Normalteiler von U und*

$$\phi\colon U/(N\cap U) \longrightarrow NU/N, \quad u(N\cap U) \longmapsto uN$$

ist ein Isomorphismus. Insbesondere gilt $(NU:N) = (U:N\cap U)$.

Beweis. Wir zeigen zuerst, dass $NU = UN$ ist. Für $u \in U$, $n \in N$ gilt $Nu = uN$; die Vereinigung über alle $u \in U$ liefert $NU = UN$. Wir zeigen, dass das eine Untergruppe von G ist: $1_G \in UN$ ist klar. Sind $g_1, g_2 \in NU = UN$, dann gibt es $u_1, u_2 \in U$ und $n_1, n_2 \in N$ mit $g_1 = n_1u_1$ und $g_2 = u_2n_2$; es ist dann $g_1g_2 = n_1(u_1u_2)n_2 \in NUN = NNU = NU$ und $g_1^{-1} = u_1^{-1}n_1^{-1} \in UN = NU$.

Sei $\phi_0\colon U \to NU \to NU/N$, $u \mapsto uN$, die Komposition der Inklusionsabbildung mit dem kanonischen Epimorphismus. Wir zeigen, dass ϕ_0 surjektiv ist: Sei gN ein Element von NU/N mit $g \in NU = UN$, dann ist $g = un$ mit $u \in U$ und $n \in N$; es folgt $gN = unN = uN = \phi_0(u)$. Der Kern von ϕ_0 ist

$$\ker(\phi_0) = \{u \in U \mid uN = N\} = \{u \in U \mid u \in N\} = N \cap U\,;$$

also ist $N \cap U$ ein Normalteiler von U und der von ϕ_0 induzierte Homomorphismus ϕ ist nach Satz 3.6 ein Isomorphismus. ❑

Ist U auch ein Normalteiler von G, dann gilt für $g \in G$, dass $gNU = NgU = NUg$ ist, also ist NU in diesem Fall ebenfalls ein Normalteiler von G.

3.10. **Definition.** Eine Gruppe G heißt *einfach*, wenn G nicht trivial ist und außer den trivialen Normalteilern $\{1_G\}$ und G keine Normalteiler hat.

DEF einfache Gruppe

Anders gesagt: Jedes *epimorphe Bild* von G (also jede Faktorgruppe G/N) ist entweder trivial oder (mittels des Epimorphismus) isomorph zu G. Es gibt also kein „vereinfachtes Abbild“ der Gruppe, daher der Name. ♢

In der Literatur wird nicht immer gefordert, dass G nicht trivial ist (z.B. [Fi]). Im Hinblick auf die unten beschriebene „Zerlegung“ einer Gruppe in einfache Gruppen ist diese Forderung aber sinnvoll, analog dazu, dass man von einer Primzahl verlangt, $\neq 1$ zu sein.

In gewisser Weise spielen einfache Gruppen für die Gruppentheorie eine ähnliche Rolle wie Primzahlen für die multiplikative Theorie der ganzen Zahlen. Wenn G etwa eine nichttriviale endliche Gruppe ist, dann ist G entweder einfach, oder G hat einen nichttrivialen Normalteiler N. In diesem Fall kann man G aus N und G/N „zusammensetzen“ (allerdings gibt es bei gegebenen Gruppen N und G/N im allgemeinen mehrere Möglichkeiten, wie man daraus eine Gruppe zusammenbauen kann, insofern ist die Situation deutlich komplizierter als bei den ganzen Zahlen); N und G/N lassen sich weiter zerlegen, bis man bei einfachen Gruppen ankommt. Man kann zeigen, dass die einfachen Gruppen, die man bekommt, bis auf Isomorphie eindeutig bestimmt sind, unabhängig davon, wie man diesen Prozess durchführt — das ist das Analogon zum Satz über die eindeutige Primfaktorzerlegung.

Für endliche *abelsche* Gruppen ist die Klassifikation der einfachen Gruppen recht übersichtlich.

3.11. **Satz.** *Eine endliche abelsche Gruppe ist genau dann einfach, wenn ihre Ordnung eine Primzahl ist.*

SATZ abelsche einfache Gruppen

Beweis. Sei A eine einfache endliche abelsche Gruppe. Dann ist A nicht trivial, also hat $\#A$ einen Primteiler p. Nach dem Satz von Cauchy 1.25 hat A ein Element a der Ordnung p und damit eine Untergruppe $\langle a \rangle$ der Ordnung p. In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler; da A einfach ist, muss $\langle a \rangle = A$ sein, und es gilt $\#A = p$.

Ist umgekehrt p eine Primzahl und A eine abelsche Gruppe mit $\#A = p$, dann gilt für jeden Normalteiler (= Untergruppe) N von A, dass $\#N$ ein Teiler von p ist (Satz von Lagrange 1.21), also ist $\#N = 1$ und damit $N = \{1_A\}$ oder $\#N = p$ und damit $N = A$. ❑

Damit haben wir bereits eine unendliche Familie von endlichen einfachen Gruppen kennen gelernt. Die Klassifikation der endlichen einfachen Gruppen wurde (im Wesentlichen — eine Lücke im Beweis wurde erst 2002 geschlossen) in den 1980er Jahren vollendet; der Beweis verteilt sich auf viele Tausend Seiten und eine große Zahl mathematischer Arbeiten. Das Resultat ist, dass es 18 unendliche Familien endlicher einfacher Gruppen gibt und dazu noch 26 sogenannte „sporadische einfache Gruppen“. Die größte dieser Gruppen ist das manchmal so genannte

„Monster“; diese Gruppe hat eine Ordnung von

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$
$$= 8080\,17424\,79451\,28758\,86459\,90496\,17107\,57005\,75436\,80000\,00000\,.$$

Eine weitere Familie von einfachen Gruppen sind die alternierenden Gruppen; das werden wir im nächsten Abschnitt besprechen.

Die A_5 (mit $\#A_5 = 60$) ist die kleinste nicht-abelsche einfache Gruppe.

Die anderen unendlichen Familien sind „Gruppen vom Lie-Typ“. Eine davon erhält man wie folgt:

Zu jeder Primzahlpotenz $q = p^e$ gibt es einen (bis auf Isomorphie eindeutigen) Körper $\mathbb{F}_q$ mit q Elementen (das werden wir später in dieser Vorlesung beweisen). Wir können dann die Gruppe $\mathrm{SL}(n, \mathbb{F}_q)$ betrachten. Ihr Zentrum besteht aus den skalaren Matrizen λI_n mit $\lambda^n = 1$ und ist ein Normalteiler. Der Quotient $\mathrm{PSL}(n, \mathbb{F}_q) := \mathrm{SL}(n, \mathbb{F}_q)/Z(\mathrm{SL}(n, \mathbb{F}_q))$ ist einfach, außer für sehr kleine Werte von n und q. Zum Beispiel ist die $\mathrm{PSL}(2, \mathbb{F}_7)$ der Ordnung 168 die zweitkleinste nicht-abelsche einfache Gruppe.

4. Permutationen

Als relativ konkretes (und auch wichtiges) Beispiel für endliche Gruppen wollen wir uns in diesem Abschnitt die symmetrische Gruppe S_n und ihre Elemente etwas genauer anschauen.

Wir beginnen mit einer etwas allgemeineren Definition.

DEF Zykel, Transposition

4.1. **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

4.2. **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?

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

4.3. **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 „$\circ$“.

* 4.4. **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 $B(x) = \{x, \sigma(x), \sigma^2(x), \ldots\}$. 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.

4.5. **Beispiel.** Sei etwa $\sigma = [531674289] \in S_9$ (in der Schreibweise von Beispiel 1.30). 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

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

4.6. **Definition.** Sei $\sigma \in S_n$. Die in der Zerlegung von Satz 4.4 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

4.7. **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

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

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

Beweis. Sei $T = \{t_1, t_2, \dots, t_m\}$. Für $x \in \{1, 2, \dots, n\} \setminus \sigma(T)$ 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

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

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

FOLG Konjugationsklassen in S_n

4.9. **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 4.8

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

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 $i \in \{1, 2, \dots, n\}$ 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 $\{1, 2, \dots, n\}$ genau einmal vor). Nach Lemma 4.8 gilt dann $\sigma\zeta_j\sigma^{-1} = \zeta_j'$ für $1 \le j \le k$ und damit auch $\sigma\tau_1\sigma^{-1} = \tau_2$. ❑

Die Gruppe S_n lässt sich von nur zwei Elementen erzeugen, wie wir gleich sehen werden.

SATZ Erzeugung von S_n

4.10. **Satz.** *Sei $n \ge 1$.*

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

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

(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 $\sigma \ne \mathrm{id}$ sei j die kleinste Zahl aus $\{1, 2, \dots, n\}$ mit $\sigma(j) \ne j$. 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 $\sigma = (1\,2\,\ldots\,n)$ und $\tau = (1\,2)$. Dann ist nach Lemma 4.8

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

also sind $(1\,2), (2\,3), \ldots, (n-1\,n) \in \langle\tau, \sigma\rangle$, 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 $\sigma^k = (i\,j\,\ldots)$; es gibt dann $\rho \in S_p$ mit

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

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).

4.11. **Beispiel.** Nach Teil (1) von Satz 4.10 ist jede Permutation ein Produkt von Transpositionen. Zum Beispiel ist

BSP Zykel als Produkt von Trans-positionen

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

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. ♣

Auch die alternierende Gruppe kann von den kürzesten Zykeln erzeugt werden, die sie enthält.

4.12. **Lemma.**

LEMMA 3-Zykel und A_n

(1) *Die Gruppe A_n wird von allen 3-Zykeln der S_n erzeugt.*

(2) *Ist $n \geq 5$, dann sind alle 3-Zykel in der A_n konjugiert: Zu je zwei 3-Zykeln $\zeta_1, \zeta_2 \in A_n$ gibt es ein $\sigma \in A_n$ mit $\zeta_2 = \sigma\zeta_1\sigma^{-1}$.*

Ähnlich wie in Teil (1) von Satz 4.10 gilt hier

$$A_n = \langle(1\,2\,3), (2\,3\,4), \ldots, (n-2\,n-1\,n)\rangle\,.$$

Beweis.

(1) Jeder 3-Zykel ist in der A_n, also kann die von allen 3-Zykeln erzeugte Untergruppe von S_n nicht größer sein als die A_n. Sei jetzt $\sigma \in A_n$ beliebig, dann kann σ als Produkt einer geraden Anzahl von Transpositionen geschrieben werden. Wir zeigen, dass ein Produkt von zwei Transpositionen als Produkt von 3-Zykeln geschrieben werden kann; daraus folgt, dass auch σ ein Produkt von 3-Zykeln ist, was schließlich zeigt, dass die 3-Zykel die A_n erzeugen. Es gilt für i, j, k, l paarweise verschieden:

$$(i\,j)(i\,j) = \mathrm{id}$$
$$(i\,j)(i\,k) = (i\,k\,j)$$
$$(i\,j)(k\,l) = (i\,l\,k)(i\,j\,k)$$

(2) Nach Folgerung 4.9 gibt es jedenfalls ein $\sigma' \in S_n$ mit der gewünschten Eigenschaft. Ist $\operatorname{sign}(\sigma') = 1$, dann können wir $\sigma = \sigma' \in A_n$ setzen. Anderenfalls ist $\operatorname{sign}(\sigma') = -1$. Da $n \geq 5$ ist, gibt es (mindestens) zwei Elemente in $\{1, 2, \ldots, n\}$, die von ζ_2 nicht bewegt werden; sei τ eine Transposition, die zwei solche Elemente vertauscht. Dann ist mit $\sigma = \tau\sigma' \in A_n$

$$\sigma\zeta_1\sigma^{-1} = \tau\sigma'\zeta_1\sigma'^{-1}\tau^{-1} = \tau\zeta_2\tau^{-1} = \zeta_2\tau\tau^{-1} = \zeta_2$$

wie gewünscht. ❑

Damit können wir nun auch beweisen, dass die alternierenden Gruppen (fast alle) einfach sind.

4.13. **Satz.** *Für jedes $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

SATZ A_n ist einfach

Beweis. Sei $N \triangleleft A_n$ ein Normalteiler mit $N \neq \{\mathrm{id}\}$, dann hat N ein Element $\sigma \neq \mathrm{id}$. Wir wollen zeigen, dass N auch einen 3-Zykel enthalten muss.

Sei $\sigma = \zeta_1\zeta_2\cdots\zeta_k$ die Zykelzerlegung von σ in Zykel der Länge ≥ 2; die Längen der Zykel seien absteigend geordnet. Sei m die Länge von ζ_1:

$$\zeta_1 = (t_1\,t_2\,t_3\,\ldots\,t_m)\,.$$

Mit $\tau = (t_1\,t_2\,t_3) \in A_n$ gilt dann im Fall $m \geq 4$

$$\tau\zeta_1\tau^{-1} = (t_2\,t_3\,t_1\,t_4\,\ldots\,t_m) \quad \text{und damit} \quad (\tau\zeta_1\tau^{-1})^{-1}\zeta_1 = (t_1\,t_m\,t_3)$$

und $\tau\zeta_j\tau^{-1} = \zeta_j$ für alle $j \geq 2$. Es folgt

$$(\tau\sigma\tau^{-1})^{-1}\sigma = (\tau\zeta_1\tau^{-1})^{-1}\zeta_1 = (t_1\,t_m\,t_3) \in N\,,$$

denn mit σ ist auch $\tau\sigma\tau^{-1}$ in N.

Im Fall $m = 3$ haben alle ζ_j Länge 3 oder 2; dann ist σ^2 ein Produkt aus 3-Zykeln. Entweder ist σ^2 bereits ein 3-Zykel (dann sind wir fertig), oder

$$\sigma^2 = (t_1\,t_2\,t_3)(t_4\,t_5\,t_6)\cdots\,.$$

Mit $\tau = (t_1\,t_2\,t_4)$ erhält man ähnlich wie oben

$$(\tau\sigma^2\tau^{-1})^{-1}\sigma^2 = (t_1\,t_3\,t_6\,t_2\,t_4)\,;$$

damit haben wir diese Situation auf den schon behandelten Fall $m = 5$ zurückgeführt.

Im Fall $m = 2$ haben wir ein Produkt einer geraden Anzahl von disjunkten Transpositionen:

$$\sigma = (t_1\,t_2)(t_3\,t_4)\cdots\,.$$

Sind es nur zwei Transpositionen, dann sei t_5 ein weiteres Element von $\{1, 2, \dots n\}$ (das existiert wegen $n \geq 5$); mit $\tau = (t_1\, t_2\, t_5)$ haben wir

$$(\tau\sigma\tau^{-1})^{-1}\sigma = (t_1\, t_5\, t_2) \in N\,.$$

Anderenfalls sind es mindestens vier Transpositionen:

$$\sigma = (t_1\, t_2)(t_3\, t_4)(t_5\, t_6)(t_7\, t_8)\cdots\,.$$

In diesem Fall ist (mit τ wie eben)

$$(\tau\sigma\tau^{-1})^{-1}\sigma = (t_1\, t_5)(t_2\, t_6)\,,$$

womit wir diesen Fall auf den vorherigen zurückgeführt haben.

Wir haben also gezeigt, dass N einen 3-Zykel ζ enthalten muss. Da $N \lhd A_n$ ein Normalteiler ist, enthält N auch alle Konjugierten $\sigma\zeta\sigma^{-1}$ (mit $\sigma \in A_n$) von ζ. Nach Teil (2) von Lemma 4.12 sind das *alle* 3-Zykel, und da nach Teil (1) desselben Lemmas die 3-Zykel die A_n erzeugen, folgt $N = A_n$. Es gibt also keinen Normalteiler $N \lhd A_n$ mit $N \neq \{\mathrm{id}\}$ und $N \neq A_n$; damit ist die A_n einfach.

Siehe auch [KM, § 9.3.2]. ❑

Auch die A_3 ist einfach, da sie abelsch ist und Ordnung 3 hat. Dagegen hat die A_4 einen nichttrivialen Normalteiler der Ordnung 4 (Übung). Für $n \leq 2$ ist die A_n trivial und damit nach unserer Definition nicht einfach.

5. 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 anfangs als Beispiel erwähnten Automorphismen- und Symmetriegruppen eines Objekts X 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 einer Gruppe auf einer Menge (oder einer Struktur).

* 5.1. **Definition.** Sei 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:

5.2. **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. ❑

Wir führen einige grundlegende Begriffe im Zusammenhang mit Operationen ein.

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

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

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

Bahn

transitiv

Fixpunkt

Stabilisator

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

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). ♢

5.4. **Beispiel.** Sei 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. ♣ **BSP**

Operation durch Translation

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:

5.5. **Beispiel.** Sei G eine Gruppe und $U \leq G$ eine Untergruppe. Dann operiert G transitiv auf G/U via $g \cdot g'U = (gg')U$. Wir erhalten 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. **BSP**

Operation auf G/U

Der Kern des Homomorphismus $G \to S(G/U)$ besteht aus allen $g \in G$, so 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 $U = \{1_G\}$), 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 ausnutzen, um das Folgende zu zeigen. Dies ist eine Verallgemeinerung der Aussage, dass eine Untergruppe vom Index 2 immer ein Normalteiler ist.

SATZ Normalteiler von kleinem Index

5.6. **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 $G \to S_p$. Sein Kern ist ein echter Normalteiler von G (denn die Operation ist transitiv und $U \neq G$; der Homomorphismus hat also nichttriviales Bild), dessen Index ein Teiler von $\#G$ und auch von $\#S_p = p!$ sein muss (nach dem Homomorphiesatz 3.6). Da p der *kleinste* Primteiler von $\#G$ ist, gilt $\operatorname{ggT}(\#G, p!) = p$, also ist der Index genau p. Der Kern ist außerdem in U enthalten, da U der Stabilisator der trivialen Nebenklasse $U \in G/U$ ist (der Kern ist der Durchschnitt aller Stabilisatoren). Es bleibt wegen $(G : U) = p$ nur die Möglichkeit, dass der Kern gleich U ist, also ist U als Kern eines Homomorphismus ein Normalteiler. ❑

BSP Operation durch Konjugation

DEF Konjugationsklasse

DEF Zentralisator

DEF Normalisator

5.7. **Beispiel.** Sei G eine Gruppe, dann operiert G auf sich selbst durch Gruppenautomorphismen via $g \mapsto c_g$, also $g \cdot x = gxg^{-1}$ (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 $Z(G)$, wie wir schon früher 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). ♣

Wir beweisen jetzt eine einfache, aber grundlegende Tatsache.

LEMMA Bahn und Stabilisator

5.8. **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

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

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. 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 1.21 (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.

5.9. **Lemma.** *Die Gruppe G operiere auf der Menge X, es sei $x \in X$ 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

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

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

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

Dabei sind alle Terme in der Summe Teiler der Ordnung von G.

FOLG Bahnengleichung

Man kann das so interpretieren, dass in der Summe x über ein *Repräsentantensystem* der Bahnen in $X \setminus X^G$ läuft. Nach Lemma 5.9 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 5.8. ❑

Diese harmlos erscheinende Relation hat interessante Anwendungen.

5.11. **Definition.** Sei p eine Primzahl. Eine endliche Gruppe G heißt eine *p-Gruppe*, wenn G nicht trivial ist und die Gruppenordnung eine Potenz von p ist. ♢

DEF p-Gruppe

5.12. **Folgerung.** *Sei G eine p-Gruppe, die auf der endlichen Menge X operiert.*

(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 $\#X^G \geq p$.*

FOLG Operation einer p-Gruppe

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 5.10 ergibt sich also die Kongruenz $\#X \equiv \#X^G \bmod p$. Daraus folgen sofort die beiden Behauptungen. ❑

BSP Satz von Cauchy

5.13. **Beispiel.** Wir betrachten noch einmal den Beweis des Satzes 1.25 von Cauchy. Dort war p eine Primzahl und G eine endliche Gruppe mit $p \mid \#G$. Die zyklische Gruppe $\mathbb{Z}/p\mathbb{Z}$ operiert auf G^p durch „Rotation“: Der Erzeuger bewirkt die Permutation

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

Diese Operation kann auf die Teilmenge M der p-Tupel mit $g_1 g_2 \cdots g_p = 1_G$ eingeschränkt werden. Diese Menge M hat durch p teilbare Kardinalität und es gibt jedenfalls den Fixpunkt $(1_G, 1_G, \ldots, 1_G) \in M$, also gibt es noch weitere Fixpunkte. ♣

BSP kleiner Satz von Fermat

5.14. **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). Dazu lassen wir die zyklische Gruppe $\mathbb{Z}/p\mathbb{Z}$ wie eben 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 Klassengleichung

5.15. **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

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

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

5.16. **Folgerung.** *Sei G eine p-Gruppe. Dann ist das Zentrum $Z(G)$ nicht trivial. Insbesondere ist eine p-Gruppe nur 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, siehe Satz 3.11. ❑

LEMMA $G/Z(G)$ nicht zyklisch

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

5.18. **Folgerung.** *Sei p eine Primzahl. Jede Gruppe der Ordnung p^2 ist abelsch.*

FOLG Gruppen der Ordnung p^2

Beweis. Sei G eine Gruppe mit $\#G = p^2$. Nach Folgerung 5.16 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 5.17 ist G dann ebenfalls abelsch (bzw. dieser Fall tritt nicht auf). ❑

6. 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.

Wir beginnen mit einem einfachen Spezialfall.

LEMMA Erzeuger einer zyklischen Gruppe

6.1. **Lemma.** *Sei $G = \langle g\rangle$ eine endliche zyklische Gruppe der Ordnung n. Dann hat G genau $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ 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

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

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

LEMMA Untergruppen einer zyklischen Gruppe

6.2. **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. 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 6.1 hat H genau $\phi(d)$ Erzeuger, damit hat G mindestens $\phi(d)$ 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* $\phi(d)$ 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 $2\phi(d)$ 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:

LEMMA Umkehrung

6.3. **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.*

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 $\phi(d)$ Erzeuger hat; dies sind dann genau die Elemente der Ordnung d in G. Es folgt

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

für alle Teiler d von n. Aus

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

folgt dann $a_d = \phi(d)$ für alle $d \mid n$. Insbesondere ist $a_n = \phi(n) \geq 1$, 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:

LEMMA

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

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

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

(3) *M ist eine Rechtsnebenklasse bzgl. einer Untergruppe von G genau dann, wenn G_M Ordnung p^e hat. In diesem Fall sind alle Mengen gM in der Bahn von M Rechtsnebenklassen 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 sind gerade die Rechtsnebenklassen von 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 bzgl. G_M nach Teil (1), denn die Anzahl der Rechtsnebenklassen bzgl. G_M in M ist gegeben durch $\frac{p^e}{\#G_M}$.
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 $\#G_M = p^e$.
Hat der Stabilisator G_M von M Ordnung p^e, dann gilt das auch für den Stabilisator $G_{gM} = gG_Mg^{-1}$ jeder anderen Menge gM in der Bahn von M.

(4) Die Bahn enthalte die Rechtsnebenklasse Ug bzgl. der Untergruppe U; dann enthält die Bahn die Untergruppe $U' = g^{-1}Ug \leq G$. Die Bahn besteht dann genau aus den Linksnebenklassen von 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 5.10 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 6.4 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 6.2 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 verallgemeinert.

* 6.5. **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

* 6.6. **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-Sylowgruppe

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.

* 6.7. **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 5.12 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 Normalteiler genau dann, 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.

* 6.8. **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 6.5. 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 6.7 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.

6.9. **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 (Definition 8.11 im Skript „Einführung in die Zahlentheorie und algebraische Strukturen“):

DEF direktes Produkt von Gruppen

6.10. **Definition.** Sei $(G_i)_{i\in I}$ eine Familie von Gruppen mit kartesischem Produkt $G = \prod_{i\in I} G_i$. Analog zur Situation bei Ringen wird G 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 $I = \{1, 2, \dots, n\}$ endlich, dann schreiben wir auch $G_1 \times G_2 \times \cdots \times G_n$ für das direkte Produkt. ♢

LEMMA Produkt von Sylowgruppen

6.11. **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.*

Beweis. Nach Satz 6.7 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 6.9 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 beide Seiten 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.

SATZ Gruppen der Ordnung pq

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

Beweis. Seien s_p und s_q die Anzahlen der p- und q-Sylowgruppen von G. Nach Satz 6.8 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 6.11 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.

7. Semidirekte Produkte und die Klassifikation von Gruppen kleiner Ordnung

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 $G = NU$

7.1. **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

7.2. **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

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

und

$$(n,u)\cdot(1_N,1_U) = (n\cdot(u*1_N),u1_U) = (n,u)\,.$$

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. ❑

7.3. **Definition.** In der Situation von Lemma 7.2 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 7.1 auch so formulieren:

7.4. **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 $G\cong N\rtimes U$

7.5. **Beispiel.** Die Diedergruppe D_n der Ordnung $2n$ ist isomorph zum semidirekten Produkt $\mathbb{Z}/n\mathbb{Z}\rtimes\{\pm1\}$, 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

7.6. **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 5.2 (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 $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

7.7. **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 6.1. 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

7.8. **Beispiel.** Es gibt eine nicht-abelsche Gruppe der Ordnung 2013.

Es ist $2013 = 3 \cdot 11 \cdot 61$. Die Automorphismengruppe von $\mathbb{Z}/61\mathbb{Z}$ hat Ordnung $\phi(61) = 60$ und enthält eine Untergruppe der Ordnung 3. Es gibt also eine nicht-triviale Operation φ von $\mathbb{Z}/3\mathbb{Z}$ auf $\mathbb{Z}/61\mathbb{Z}$; damit ist $\mathbb{Z}/61\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ nicht abelsch. Wir erhalten eine nicht-abelsche Gruppe der Ordnung 2013 als direktes Produkt

$$G = \big(\mathbb{Z}/61\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}\big) \times \mathbb{Z}/11\mathbb{Z}\,. \qquad ♣$$

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 $K^\times$

7.9. **Satz.** *Seien K ein Körper und $G \leq K^\times$ endlich. Dann ist G zyklisch. Insbesondere ist für jede Primzahl p die Gruppe $\mathbb{F}_p^\times$ 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 6.3 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

7.10. **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 6.12 behandelt. Wir können also $q \equiv 1 \bmod p$ voraussetzen. Wie im Beweis von Satz 6.12 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 6.12 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 7.9 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:

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

❑

FOLG $\#G = 2p$

7.11. **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 7.10 (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

7.12. **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 5.18), 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 7.11, 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 7.10, 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 5.16) und dass $Z(G) \neq G$ gilt. Wäre $\#Z(G) = 4$, dann würde wie im Beweis von Folgerung 7.11 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 6.9 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
Quaternionen-gruppe

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

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 5.18 (für den Fall $p = q$) und Satz 7.10. 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).

8. Körpererweiterungen

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

* 8.1. **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

8.2. **Beispiele.** $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}(i) \subset \mathbb{C}$ sind Körpererweiterungen. $\mathbb{Q}(i)$ 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:

8.3. **Definition.** Sei $k \subset K$ 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 $\mathbb{Q}(i)$ oder $\mathbb{Q}(\sqrt{2})$ gesehen. Ein anderes Beispiel ist $\mathbb{C} = \mathbb{R}(i)$, $\mathbb{C}$ ist also eine einfache Erweiterung von $\mathbb{R}$.

8.4. **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.

∗ 8.5. **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

8.6. **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. ❑

8.7. **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 9.1 im Skript zur „Einführung in die Zahlentheorie und algebraische Strukturen“) gibt es eine Fortsetzung von ϕ_K zu einem Homomorphismus $\tilde{\phi}_K : \mathbb{Q} \to P \subset K$. 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, oder $\mathbb{R}$ ist ein unendlichdimensionaler $\mathbb{Q}$-Vektorraum (denn jeder endlichdimensionale $\mathbb{Q}$-Vektorraum ist abzählbar). Das ermöglicht die folgende Definition.

8.8. **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*. ♢

8.9. **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 8.7), 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**

* 8.10. **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 $B = \{x_i y_j \mid 1 \le i \le m, 1 \le j \le n\}$ 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 $[K : k] = \dim_k K = \#B = nm = [K : L] \cdot [L : k]$. ❑

8.11. **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**

Beweis. Die erste Aussage folgt unmittelbar aus Satz 8.10. Die zweite ergibt sich aus $L = k \iff [L : k] = 1 \iff [K : L] = [K : k]$. ❑

8.12. **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 $b_1 = 1, b_2, \ldots, b_n$ eine k-Basis von L_2. 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. ❑

9. Algebraische Elemente und Erweiterungen

Wir kommen nun zu einer wichtigen Begriffsbildung in der Körpertheorie.

* 9.1. **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.

9.2. **Beispiele.**

BSP
algebraische und transzendente Zahlen und Körpererweiterungen

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

Im Folgenden wird mehrfach auf das Skript „Einführung in die Zahlentheorie und algebraische Strukturen“ 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.10.2 (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“

9.3. **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 (vgl. EZAS.10.10), 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.6.14 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.6.20).

„(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 9.3 auftretende Polynom f hat einen Namen:

∗ 9.4. **Definition.** Sei $k \subset K$ eine Körpererweiterung und sei $a \in K$ algebraisch über k. Dann heißt das Polynom f in Satz 9.3 das *Minimalpolynom* von a über k und der Grad $[k(a) : k] = \deg(f)$ heißt der *Grad* von a über k. ♢ **DEF** Minimalpolynom

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 9.3 hat einige wichtige Konsequenzen.

9.5. **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 9.3. ❑

9.6. **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**

9.7. **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

9.8. **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 9.3. Aus Lemma 8.12 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 9.3 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).

9.9. **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 $i = \zeta_4$ ebenfalls algebraisch ist, ist auch $\sin\frac{2\pi}{n} = \frac{1}{2i}(\zeta_n - \zeta_n^{-1})$ algebraisch. **BSP**

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 tun das in der „Vertiefung der Algebra“), dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ ist (Eulersche ϕ-Funktion); es folgt $[K_n : \mathbb{Q}] = \frac{1}{2}\phi(n)$. Für $n = 7$ und $n = 9$ ist $\phi(n) = 6$, 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.) ♣

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

FOLG endliche KE sind algebraisch

Beweis. Ist $a \in K$, dann ist $k(a) \subset K$ endlich über k, also ist a nach Satz 9.3 algebraisch über k. ❑

9.11. **Beispiel.** Die Umkehrung von Folgerung 9.10 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.11.13). 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. ♣

BSP Umkehrung gilt nicht

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

SATZ Transitivität der Algebraizität

Beweis. Wir nehmen zunächst an, dass $k \subset K$ algebraisch ist. Dann ist jedes Element $a \in K$ algebraisch über k, also ist nach Satz 9.3 $[k(a) : k] < \infty$. Es folgt $[L(a) : L] \leq [k(a) : k] < \infty$, also ist $L \subset K$ algebraisch. Wählt man $a \in L$, folgt auch, dass $k \subset L$ algebraisch ist.

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 9.3 und wiederholter Anwendung von Lemma 8.12, 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. ❑

9.13. **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.*

FOLG algebraischer Abschluss

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 9.12 ist a dann auch algebraisch über k, also liegt a in $\bar{k}$. ❑

9.14. **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. ♢

DEF algebraischer Abschluss

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

Wir sehen jedenfalls, dass der in Beispiel 9.11 eingeführte Körper $\mathbb{A}$ der algebraischen Zahlen ein algebraischer Abschluss von $\mathbb{Q}$ ist.

10. 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 9.3 weist dazu den Weg.

SATZ Existenz von Körpererweiterungen

10.1. **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 9.3. 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.

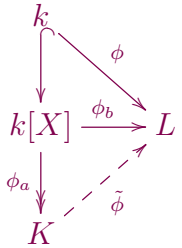
Für den Vergleich von Körpererweiterungen, in denen ein gegebenes irreduzibles Polynom eine Nullstelle hat, ist folgende Aussage nützlich.

SATZ Fortsetzung von Homomorphismen

10.2. **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 10.1 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 $\tilde{\phi}$. ❑

10.3. **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 10.2 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. ♣

BSP isomorphe Körpererweiterungen

Durch Iteration der Konstruktion von Satz 10.1 können wir erreichen, dass ein gegebenes Polynom in Linearfaktoren zerfällt.

10.4. **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. ♢

DEF Zerfällungskörper

10.5. **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 $\psi|_k = \mathrm{id}_k$.

SATZ Existenz und Eindeutigkeit des Zerfällungskörpers

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 10.1 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 10.2 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 10.2 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 in der „Vertiefung der Algebra“ genauer studieren.

10.6. **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. ♣

11. 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.

11.1. **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 8.7).*

(3) $\#F = p^e$ *mit $e \geq 1$ (Beispiel 8.9).*

(4) *In F gilt $(x+y)^p = x^p + y^p$ (und $(xy)^p = x^p y^p$).*

(5) *Die multiplikative Gruppe $F^\times$ von F ist zyklisch (Satz 7.9).*

Die vorletzte Aussage legt folgende Definition nahe:

11.2. **Definition.** Sei F ein Körper der Charakteristik $p > 0$. Dann ist die Abbildung $\phi_F : F \to F$, $x \mapsto x^p$, 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 $(x+y)^p = x^p + y^p$ („Freshman's Dream"). Als Homomorphismus zwischen Körpern ist ϕ_F injektiv. Ist F endlich, dann muss $\phi_F : F \to F$ sogar bijektiv sein.

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

11.3. **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

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). Da alle Elemente von K_f die Gleichung $x^{p^f} - x = 0$ erfüllen, muss $\#K_f \leq p^f$ sein. 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 $\#K_f \geq p^f$.

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 11.3 inspirieren.

11.4. **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).*

SATZ Existenz von Erweiterungen endlicher Körper

Beweis. Ist $F \subset F'$ eine beliebige Körpererweiterung mit $[F' : F] = n$, dann ist $\phi_{F'}^{en} = \mathrm{id}_{F'}$ nach Lemma 11.3, 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 10.5.

Sei F' ein Zerfällungskörper von f über F; so ein F' existiert nach Satz 10.5. 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 $[F' : F] = n$. ❑

11.5. **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.*

FOLG Existenz endlicher Körper

Beweis. Wir wenden Satz 11.4 auf $F = \mathbb{F}_p$ an. ❑

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

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

LEMMA Erweiterungen endlicher Körper sind einfach

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

Aus Satz 11.4 und Lemma 11.6 können wir nun Schlüsse über die Existenz von irreduziblen Polynomen vorgegebenen Grades über einem endlichen Körper ziehen.

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

SATZ Existenz irreduzibler Polynome

Beweis. Sei $q = \#F = p^e$. Nach Satz 11.4 gibt es eine Körpererweiterung F' von F vom Grad n. Nach Lemma 11.6 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

11.8. **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 10.1 gibt es eine Körpererweiterung F'' von F vom Grad n, in der f eine Nullstelle hat. Nach Satz 11.4 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 11.3 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 die Abbildung $\phi^e_{F'} : x \mapsto x^q$ 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 11.3 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 9.5. 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. ❑

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

11.9. **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 11.8 ist K ein Zerfällungskörper

von f über F, also zerfällt f auch über F' in 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

11.10. **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 $n \geq 1$*

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

Beweis. Die linke Seite ergibt den Grad des Produkts auf der rechten Seite der Formel in Lemma 11.9, die rechte Seite ist der Grad des Polynoms $X^{q^n} - X$ auf der linken Seite. ❑

BSP Anzahlen irreduzibler Polynome

11.11. **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.11.10. ♣

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

DEF Möbius-funktion

11.12. **Definition.** Die *Möbiusfunktion* $\mu : \mathbb{Z}_{>0} \to \{-1, 0, 1\}$ ist definiert durch

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

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.

LEMMA Möbius-Inversion

11.13. **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*

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

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:

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

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

FOLG Formel für $a_n(q)$

11.14. **Folgerung.** *Es gilt*

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

Beweis. Anwendung von Lemma 11.13 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.)

12. 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 bereits konstruierten Geraden und Kreisen (wenn es endlich viele sind).

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'.

* 12.1. **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

12.2. **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.*

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.

LEMMA notwendige Bedingung für Konstruierbarkeit

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:

$$(y_1 - y_2)x - (x_1 - x_2)y + x_1y_2 - x_2y_1 = 0$$
$$(x - x_3)^2 + (y - y_3)^2 - (x_4 - x_5)^2 - (y_4 - y_5)^2 = 0$$

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

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

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.

12.3. **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 12.2 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...

12.4. **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.

12.5. **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 12.2 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:

12.6. **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 12.5 nicht der Fall ist. ❑

FOLG Konstruierbarkeit des regulären p-Ecks

12.7. **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.11.14). Es gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos\frac{2\pi}{p})] = 2$ (siehe Beispiel 9.9). 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. ❑

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 65537-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 65537-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 aber nicht durch 2^m teilbar. 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.

Die Unmöglichkeit eines anderen klassischen Problems zeigt die nächste Folgerung.

FOLG Quadratur des Kreises

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

Beweis. Wäre $\sqrt{\pi}$ konstruierbar, dann wäre $\sqrt{\pi}$ und damit auch π nach Lemma 12.2 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 12.2. 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

12.9. **Satz.** *Sei $S \subset \mathbb{R}$ (mit $0, 1 \in S$). Dann ist $\alpha \in \mathbb{R}$ 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 $\alpha \in K_n$ und $[K_m : K_{m-1}] = 2$ 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 $16 \cos \frac{2\pi}{17}$.

13. Separable Körpererweiterungen

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

13.1. **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.

13.2. **Lemma.** *Seien K ein Körper und $f \in K[X]$ irreduzibel. Dann ist f 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 $L[X]$. Dann gilt

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

denn α ist eine einfache Nullstelle von f. Das zeigt $f' \neq 0$. ❑

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

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

FOLG Char. 0

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 13.2 separabel. ❑

13.4. **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 Char. p

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

Beweis. Nach Lemma 13.2 genügt es zu zeigen, dass $f' = 0$ ist genau dann, wenn $f = g(X^p)$ ist für ein $g \in K[X]$. Gilt $f = g(X^p)$, dann ist $f' = pX^{p-1}g'(X^p) = 0$. Für die Gegenrichtung sei $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. Dann ist

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

Ist $f' = 0$, dann folgt $ma_m = 0$ für alle $0 \leq m \leq n$. 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 separable Körpererweiterung

13.6. **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 Erweiterungen

13.7. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung und $a \in K$ algebraisch über k.*

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

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

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

Beweis. Der Fall von Charakteristik 0 folgt aus Folgerung 13.3.

Sei also $\operatorname{char}(k) = p > 0$. 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 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 13.5. 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 $\operatorname{char}(k) = p > 0$ etwas zu zeigen. Sei $b \in k(a)$ und sei $f \in k(b)[X]$ das

Minimalpolynom von a über $k(b)$. Wir schreiben $\phi : K \to K$ für den Frobenius-Endomorphismus $\lambda \mapsto \lambda^p$ und $f^\phi \in k(b^p)[X]$ für das Polynom, das man erhält, wenn man ϕ auf die Koeffizienten von f anwendet. Dann gilt

$$f^\phi(a^p) = f^\phi(\phi(a)) = \phi(f(a)) = \phi(0) = 0\,,$$

also hat f^ϕ die Nullstelle a^p. Damit gilt

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

also folgt unter Verwendung von $k(a) = k(a^p)$:

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

Das heißt aber $k(b) = k(b^p)$, also ist b separabel über k. ❑

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

13.8. **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

13.9. **Satz.** *Sei K ein Körper.*

SATZ
Satz von Steinitz

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

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

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

Beweis. Der Fall von Charakteristik 0 folgt wieder aus Folgerung 13.3.

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 13.7. 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

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

also 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 ein Körperhomomorphismus und als solcher injektiv. Weil K endlich ist, ist ϕ dann auch surjektiv, also ist K nach Teil (2) vollkommen. ❑

13.10. **Beispiel.** Ein unvollkommener Körper ist also nicht so leicht zu finden. Wie Beispiel 13.4 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. Wir behandeln den wesentlichen Schritt als Lemma vorneweg.

13.11. **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 11.6 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 $h = \operatorname{ggT}(g, f(c - \lambda X))$ 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 $b \in k(c)$. ❑

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

BSP primitives Element

* 13.13. **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 $k(c) = k(a, b_1, \ldots, b_n)$.*

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

SATZ Satz vom primitiven Element

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 13.11 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

13.14. **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 13.7. Nach Voraussetzung gilt $k(a^p) = k(a)$ und $k(a)(b^p) = k(a)(b)$. Es folgt $k(a^p, b^p) = k(a, b^p) = k(a, b)$. Ähnlich wie beim Beweis von Teil (3) von Lemma 13.7 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 13.13 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.

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.