Einführung in die Algebra

Würzburg, Wintersemester 2017/18

Prof. Grundhöfer*

19. Februar 2018

"a teacher ... should expound the truth to his pupils
to the limits of their patience and capacity."
G. H. Hardy 1925

Inhaltsverzeichnis

*LaTeX von Markus Sauer und Andreas Beck

Teil I.
GRUPPEN

1. Gruppen und Untergruppen

Standard-Mengen: $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Für jede endliche Menge M sei $|M|$ die Anzahl ihrer Elemente; diese Anzahl nennen wir auch die Länge von M.

Eine zweistellige (auch: binäre) Verknüpfung auf einer Menge M ist eine Abbildung $f : M \times M \to M$. Statt f schreibt man oft $+$ oder $\cdot$ und dann statt $f(a, b)$ auch $a + b$ bzw. $a \cdot b$ oder ab.

1.1 Definition. Eine Gruppe ist ein Paar $(G, \cdot)$, wobei G eine Menge und $\cdot$ eine zweistellige Verknüpfung auf G mit folgenden Eigenschaften ist:

(1) Das Assoziativgesetz: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ gilt für alle $a, b, c \in G$.

Es gibt ein Element $e \in G$ mit

(2) $\forall a \in G : a \cdot e = a = e \cdot a$ und

(3) $\forall a \in G\ \exists b \in G : a \cdot b = e = b \cdot a$.

Eine Gruppe $(G, \cdot)$ heißt abelsch oder kommutativ, falls $a \cdot b = b \cdot a$ für alle $a, b \in G$ gilt. Statt $(G, \cdot)$ schreibt man oft nur G.

Bemerkungen. Das Element e ist durch (2) eindeutig bestimmt (denn für ein weiteres solches Element e' gilt $e' = e' \cdot e = e$), es wird Neutralelement oder Einselement genannt und oft mit 1 bezeichnet (bei additiver Schreibweise: Nullelement 0).

Das Element b in (3) ist durch a eindeutig bestimmt (denn aus $a \cdot b' = e = b' \cdot a$ folgt $b' = b' \cdot e = b' \cdot (a \cdot b) = (b' \cdot a) \cdot b = e \cdot b = b$) und wird das zu a inverse Element genannt; man schreibt $b = a^{-1}$ (bzw. $b = -a$ bei additiver Schreibweise).

1.2 Beispiele. a) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe, ebenso $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(V, +)$ für jeden Vektorraum V. Das Paar $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe, aber $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen ($\mathbb{Q}$ und $\mathbb{R}$ sind Körper).

b) Sei $n \in \mathbb{N}$ und $C_n := \{0, 1, ..., n-1\}$. Wir definieren $\oplus$ durch

$$a \oplus b = \begin{cases} a + b & \text{falls } a + b < n \\ a + b - n & \text{falls } a + b \geq n \end{cases}$$

für $a, b \in C_n$. Dann ist $(C_n, \oplus)$ eine abelsche Gruppe (das kann man direkt zeigen, oder mit 3.8 begründen). Das zu $a \in C_n \setminus \{0\}$ inverse Element ist $n - a$.

c) Sei M eine Menge und $\operatorname{Sym} M = \{f \mid f : M \to M \text{ ist bijektiv}\}$. Wir bezeichnen mit $\circ$ die Komposition von Abbildungen, also $(f \circ g)(m) := f(g(m))$ für alle $m \in M$. Dann ist $(\operatorname{Sym} M, \circ)$ eine Gruppe, die symmetrische Gruppe von M.

$S_n := \operatorname{Sym}\{1, 2, ..., n\}$ heißt auch symmetrische Gruppe vom Grad n, für $n \in \mathbb{N}$. Es gilt $|S_n| = n!$.

d) Sei V ein Vektorraum und $\mathrm{GL}(V) = \{f \mid f : V \to V \text{ ist bijektiv und linear}\}$. Dann ist $\mathrm{GL}(V)$ mit der Komposition $\circ$ von Abbildungen eine Gruppe, die (generelle) lineare Gruppe von V. Ist $V = K^n$, betrachtet als Vektorraum über dem Körper K, so ist $\mathrm{GL}(V) = \mathrm{GL}(K^n) =: \mathrm{GL}_n K$ die Gruppe aller invertierbaren (regulären) $n \times n$-Matrizen mit Einträgen aus K.

e) Sind G und H Gruppen, so ist auch $G \times H$ mit der Verknüpfung $(g, h) \cdot (g', h') = (gg', hh')$ für $g, g' \in G, h, h' \in H$ eine Gruppe, das direkte Produkt von G und H. Die Gruppe $C_2 \times C_2$ heißt auch Kleinsche Vierergruppe.

1.3 Einfache Folgerungen. Sei G eine Gruppe und $a, b \in G$.
Man darf kürzen: aus $ax = ay$ (oder $xa = ya$) folgt $x = y$.
Die Gleichungen $ax = b$ bzw. $ya = b$ sind in G eindeutig lösbar (durch $x = a^{-1}b$ und $y = ba^{-1}$; i.A. ist $x \neq y$).
Es gilt $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$.
Man definiert Potenzen durch $a^0 = 1$, $a^n = a^{n-1} \cdot a$ und $a^{-n} = (a^{-1})^n$ für $n \in \mathbb{N}$ (bei additiver Schreibweise: Vielfache na statt a^n). Dann gilt $a^n \cdot a^m = a^{n+m}$ und $(a^n)^m = a^{nm}$ für alle $n, m \in \mathbb{Z}$ (Beweise durch Induktion).

1.4 Definition. Eine nichtleere Teilmenge U einer Gruppe G heißt Untergruppe von G, falls für $a, b \in U$ stets $a \cdot b \in U$ und $a^{-1} \in U$ gilt.

Jede Untergruppe U enthält das Neutralelement und ist mit der auf $U \times U$ eingeschränkten Verknüpfung wieder eine Gruppe. Man schreibt dann $U \leq G$.

1.5 Beispiele.

1. Jede Gruppe G hat die Untergruppen $\{1\}$ und G.
2. $2\mathbb{Z} := \{2z \mid z \in \mathbb{Z}\} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$, jeweils mit der Addition.
3. Jeder Untervektorraum eines Vektorraums V ist eine Untergruppe von $(V, +)$, aber nicht umgekehrt: $\mathbb{Z}^n$ (oder $\mathbb{Q}^n$) ist eine Untergruppe von $(\mathbb{R}^n, +)$, aber kein (reeller) Untervektorraum.
4. $\mathrm{GL}(V) \leq \operatorname{Sym} V$ für jeden Vektorraum V.
5. $\mathrm{SL}_n K := \{A \in \mathrm{GL}_n K \mid \det A = 1\} \leq \mathrm{GL}_n K$, für jeden Körper K, weil det multiplikativ ist.
6. $\left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \middle| \, \alpha \in \mathbb{R} \right\} \leq \mathrm{GL}_2 \mathbb{R}$, Drehungen in der Ebene um den Nullpunkt.

1.6 Satz (Lagrange)**.** *Sei G eine endliche Gruppe und $U \leq G$. Dann ist $|U|$ ein Teiler von $|G|$.*

Beweis. Wir betrachten die sog. (Rechts-) Nebenklassen $Ug := \{ug \mid u \in U\}$ mit $g \in G$. Wegen $1 \in G$ ist $g \in Ug$ und daher $G = \bigcup_{g \in G} Ug$.

Für alle $x \in U$ gilt $Ux \subseteq U$ und $Ux^{-1} \subseteq U$, also $U = U \cdot 1 = Ux^{-1}x \subseteq Ux$, und daher $Ux = U$.

Zwei Nebenklassen Ug und Ug' mit $g, g' \in G$ sind entweder disjunkt oder gleich: wenn ein gemeinsames Element $ug = u'g'$ existiert, mit $u, u' \in U$, so folgt $Ug = Uug = Uu'g' = Ug'$. Die verschiedenen Nebenklassen $Ug_1, Ug_2, \ldots, Ug_n$ (mit geeigneten $g_i \in G$) bilden also eine Partition von G, d. h. es gilt

$$G = \textstyle\bigcup_{i=1}^{n} Ug_i \quad \text{und} \quad Ug_i \cap Ug_j = \emptyset \text{ für } i \neq j.$$

Daher ist $|G| = \sum_{i=1}^{n} |Ug_i|$.

Für jedes i ist die Abbildung $U \to Ug_i : x \mapsto xg_i$ bijektiv (mit der Umkehrabbildung $Ug_i \to U : y \mapsto yg_i^{-1}$). Daher gilt $|U| = |Ug_i|$ für $1 \leq i \leq n$, also $|G| = \sum_{i=1}^{n} |Ug_i| = n \cdot |U|$. □

Man nennt die Anzahl $n = \frac{|G|}{|U|}$ der Nebenklassen von U in G auch den Index $|G : U|$ von U in G. Es gilt $|G| = |G : U| \cdot |U|$.

1.7 Definition. Sei G eine Gruppe. Ist M eine beliebige Menge von Untergruppen von G, so ist auch der Durchschnitt $\bigcap M := \{g \mid g \in U \text{ für jedes } U \in M\}$ eine Untergruppe von G. Für eine beliebige Teilmenge X von G definiert man das (gruppentheoretische) Erzeugnis von X durch

$$\langle X \rangle := \bigcap_{X \subseteq U \leq G} U.$$

Dies ist die kleinste aller Untergruppen von G, welche X enthalten.

Es gilt $\langle G \rangle = G$ und $\langle \emptyset \rangle = \{1\} = \langle 1 \rangle$.

Andere Beschreibung:

1.8 Lemma. *Für jede Teilmenge X einer Gruppe G gilt*

$$\langle X \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n} \mid n \in \mathbb{N}_0, x_i \in X \text{ und } \varepsilon_i \in \{1, -1\} \text{ für } 1 \leq i \leq n\}$$

mit der Konvention, dass leere Produkte ($n = 0$) gleich 1 sind.

Beweis. Sei Y die rechte Seite der behaupteten Gleichung. Dann gilt $X \subseteq Y$ und $Y \leq G$, also ist $\langle X \rangle \subseteq Y$ nach Definition von $\langle X \rangle$.

Für die andere Inklusion betrachte Elemente $x_i \in X$ und $\varepsilon_i \in \{1, -1\}$. Für jede Untergruppe U von G mit $X \subseteq U$ gilt $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n} \in U$ nach Definition 1.4. Daher ist $Y \subseteq \bigcap_{X \subseteq U \leq G} U = \langle X \rangle$. □

Spezialfall: Für jedes Element g einer Gruppe G ist $\langle g \rangle = \langle \{g\} \rangle = \{g^z \mid z \in \mathbb{Z}\}$ eine Untergruppe von G (bei additiver Schreibweise $\langle g \rangle = \{zg \mid z \in \mathbb{Z}\} = \mathbb{Z}g$).

1.9 Definition. Eine Gruppe G heißt zyklisch, falls $G = \langle g \rangle$ für ein $g \in G$ gilt; man nennt dann g einen Erzeuger von G.

Beispiele: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \langle 2, 3 \rangle = \langle 6, 10, 15 \rangle$, $\quad C_n = \langle 1 \rangle = \langle n - 1 \rangle$.

1.10 Definition. Sei G eine Gruppe und $g \in G$. Man nennt $|\langle g\rangle|$ die Ordnung von g. Elemente der Ordnung 2 heißen auch Involutionen.

Ist G endlich, so nennt man $|G|$ auch die Ordnung von G; nach 1.6 ist dann die Ordnung eines Gruppenelements ein Teiler der Gruppenordnung.

1.11 Satz. *Jede Gruppe von Primzahlordnung ist zyklisch.*

Beweis. Sei G eine Gruppe, $|G|$ eine Primzahl und $1 \neq g \in G$. Dann ist $|\langle g\rangle| > 1$ ein Teiler von $|G|$ nach 1.6, also $|\langle g\rangle| = |G|$, und daher $\langle g\rangle = G$. □

Die Aufzählung aller Untergruppen einer vorgelegten Gruppe ist nur in seltenen Fällen möglich, etwa in diesen:

1.12 Satz. *Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Mengen $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$ mit $m \in \mathbb{N}_0$.*

Die Gruppe $(C_n, \oplus)$ mit $n \in \mathbb{N}$ hat für jeden positiven Teiler t von n genau eine Untergruppe der Ordnung t, nämlich $\{0\}$ für $t = 1$ und $\langle \frac{n}{t}\rangle = \{j\frac{n}{t} \mid 0 \leq j < t\}$ für $t > 1$.

Beweis. Die angegebenen Mengen sind Untergruppen.

Sei jetzt $U \neq \{0\}$ eine Untergruppe von $\mathbb{Z}$ oder von C_n. Wegen $U = -U$ gilt $U \cap \mathbb{N} \neq \emptyset$. Weil $\mathbb{N}$ wohlgeordnet ist, existiert $m := \min(U \cap \mathbb{N})$. Wegen $m \in U$ gilt $m\mathbb{Z} \subseteq U$.

Für die umgekehrte Inklusion sei $u \in U$. Wir schreiben $u = q \cdot m + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < m$ (Division mit Rest, $q = \lfloor \frac{u}{m} \rfloor$). Es folgt $r = u - qm \in U$, nach Definition von m also $r = 0$ und damit $u = q \cdot m \in m\mathbb{Z}$. Dies beweist $U = m\mathbb{Z} = \langle m\rangle$.

Die Mengen $i + \langle m\rangle$ mit $0 \leq i < m$ sind die verschiedenen Nebenklassen von $\langle m\rangle$. Also hat $U = \langle m\rangle$ den Index m in $\mathbb{Z}$ bzw. C_n. Im Fall von C_n folgt $n = |C_n| = m|U| = mt$, also $m = \frac{n}{t}$. □

1.13 Bemerkung. Für $a, b \in Z$ gilt $a\mathbb{Z} \subseteq b\mathbb{Z}$ genau dann, wenn b ein Teiler von a ist.

[Diagramm für das System (den Verband) der Untergruppen]

Auch in $(C_n, \oplus)$ wird die Inklusion zwischen Untergruppen durch die Teilbarkeit geregelt (wegen der Eindeutigkeit in 1.12).

1.14 Korollar (Lemma von Bézout)**.** *Seien $a, b \in \mathbb{Z}$. Genau dann existieren $x, y \in \mathbb{Z}$ mit $ax + by = 1$, wenn a und b teilerfremd sind.*

Beweis. Sei $ax + by = 1$ mit $x, y \in \mathbb{Z}$, und sei t ein gemeinsamer Teiler von a und b. Dann ist t ein Teiler von $ax + by = 1$, also $t = \pm 1$. Daher sind a und b teilerfremd.

Umgekehrt seien jetzt a, b teilerfremd. Nach 1.12 hat die Untergruppe $U := \langle a, b\rangle = \{ax + by \mid x, y \in \mathbb{Z}\}$ die Form $U = m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$. Wegen $a, b \in U = m\mathbb{Z}$ ist m ein Teiler von a und b, also $m = 1$ wegen der Teilerfremdheit. Daher ist $U = \mathbb{Z}$, insbesondere $1 \in U$. □

Man findet x, y zu gegebenen Zahlen a, b mit dem Euklidischen Algorithmus (wiederholte Division mit Rest), siehe 11.4.

1.15 Lemma. *Sei G eine Gruppe und $g \in G$ ein Element von endlicher Ordnung n. Dann gilt für $k, l \in \mathbb{Z}$:*

(i) $g^n = 1 \neq g^k$ *für* $1 \leq k < n$, *und* $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$.

(ii) $g^k = g^l \Leftrightarrow n$ *teilt* $k - l$.

(iii) $g^k = 1 \Leftrightarrow n$ *teilt* k.

(iv) g^k *erzeugt* $\langle g \rangle \Leftrightarrow k$ *und* n *sind teilerfremd.*

Beweis. Weil $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$ endlich ist, existieren $i, j \in \mathbb{Z}$ mit $g^i = g^j$ und $i > j$, also $g^{i-j} = 1$. Daher ist $U := \{z \in \mathbb{Z} \mid g^z = 1\}$ eine Untergruppe von $(\mathbb{Z}, +)$ mit $U \neq \{0\}$. Nach 1.12 ist $U = m\mathbb{Z}$ für ein $m \in \mathbb{N}$.

Es gilt $g^m = 1$, also $\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Die Elemente $1, g, g^2, \ldots, g^{m-1}$ sind paarweise verschieden, nach Definition von m und U. Also gilt $n = |\langle g \rangle| = m$.

Damit folgen (iii) und (i), und auch (ii) wegen $g^k = g^l \Leftrightarrow g^{k-l} = 1$.

Zu (iv): Wegen $\langle g^k \rangle \subseteq \langle g \rangle$ gilt: g^k erzeugt $\langle g \rangle \Leftrightarrow g \in \langle g^k \rangle \Leftrightarrow \exists x \in \mathbb{Z} : g = (g^k)^x = g^{k \cdot x} \overset{\text{(ii)}}{\Leftrightarrow} \exists x \in \mathbb{Z} : n$ teilt $1 - kx \Leftrightarrow \exists x, y \in \mathbb{Z} : ny = 1 - kx \overset{1.14}{\Leftrightarrow} k$ und n sind teilerfremd. □

1.16 Definition. Für $n \in \mathbb{N}$ sei

$$\varphi(n) := |\{k \in \mathbb{N} \mid 1 \leq k \leq n \text{ und } k, n \text{ sind teilerfremd}\}|.$$

Man nennt diese Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$ die Eulersche φ-Funktion. Nach 1.15(iv) ist $\varphi(n)$ die Anzahl der Erzeuger jeder zyklischen Gruppe der Ordnung n.

Beispiele: $\varphi(n) = n - 1$ für jede Primzahl n, siehe Beweis zu 1.11. Ferner $\varphi(4) = 2$, allgemeiner $\varphi(2^m) = 2^{m-1}$ für $m \in \mathbb{N}$.

1.17 Korollar. *Für alle $n \in \mathbb{N}$ gilt $n = \sum_{t \text{ teilt } n} \varphi(t)$.*

Beweis. Die Ordnung jedes Elements von C_n ist ein Teiler von n, siehe 1.10 und 1.6. Daher gilt

$$n = |C_n| = \sum_{t \text{ teilt } n} |\{a \in C_n \mid a \text{ hat Ordnung } t\}| = \sum_{t \text{ teilt } n} |\{a \in C_n \mid \langle a \rangle \text{ hat Ordnung } t\}|.$$

Nach 1.12 hat C_n für jeden Teiler t von n genau eine Untergruppe der Ordnung t; diese ist zyklisch, enthält also genau $\varphi(t)$ Elemente der Ordnung t (Erzeuger). Damit folgt die Behauptung. □

2. Homomorphismen und Wirkungen

2.1 Definition. Seien G und H Gruppen. Eine Abbildung $f : G \to H$ heißt (Gruppen-) Homomorphismus, falls $f(ab) = f(a)f(b)$ für alle $a, b \in G$ gilt.

Ist $f : G \to H$ injektiv bzw. surjektiv bzw. bijektiv, so nennt man f einen Monomorphismus bzw. Epimorphismus bzw. Isomorphismus.

G und H heißen isomorph, in Zeichen: $G \cong H$, falls ein Isomorphismus von G auf H existiert.

Homomorphismen von G in sich heißen Endomorphismen; man setzt $\operatorname{End} G := \{f \mid f : G \to G \text{ ist Homomorphismus}\}$. Isomorphismen von G auf sich heißen Automorphismen, man schreibt $\operatorname{Aut} G := \{f \mid f : G \to G \text{ ist Isomorphismus}\}$.

2.2 Beispiele.

1. Jede lineare Abbildung $f : V \to W$ zwischen Vektorräumen V und W ist ein Homomorphismus von $(V, +)$ in $(W, +)$.

2. Sei G eine abelsche Gruppe und $n \in \mathbb{Z}$. Dann ist die Abbildung $G \to G : g \mapsto g^n$ (bzw. $g \mapsto ng$ bei additiver Schreibweise) ein Homomorphismus.

3. Sei G eine Gruppe und $g \in G$. Dann ist die Abbildung $i_g : G \to G$ mit $i_g(x) = gxg^{-1}$ für alle $x \in G$ ein Automorphismus von G (mit der Umkehrabbildung $i_{g^{-1}}$), also $i_g \in \operatorname{Aut} G$. Man nennt i_g den inneren Automorphismus, der von g induziert wird. Es gilt $i_1 = \mathrm{id}_G$.

4. Die Determinante $\det : \mathrm{GL}_n \mathbb{R} \to \mathbb{R} \setminus \{0\}$ ist multiplikativ und surjektiv für $n > 0$, also ein Epimorphismus.

5. Die Abbildung $\mathbb{R} \to \mathrm{GL}_2 \mathbb{R} : \alpha \mapsto \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ ist ein Homomorphismus von $(\mathbb{R}, +)$ in $\mathrm{GL}_2 \mathbb{R}$, wegen der Additionstheoreme für $\sin, \cos$.

6. Die Exponentialfunktion exp ist eine Bijektion von $\mathbb{R}$ auf die Menge $\mathbb{R}^{>0}$ aller positiven reellen Zahlen. Die Funktionalgleichung $\exp(x+y) = \exp(x) \cdot \exp(y)$ zeigt, dass exp sogar ein Isomorphismus von $(\mathbb{R}, +)$ auf $(\mathbb{R}^{>0}, \cdot)$ ist. Die Umkehrfunktion ist der natürliche Logarithmus.

2.3 Einfache Folgerungen.
Sei $f : G \to H$ ein Homomorphismus zwischen zwei Gruppen G und H.
Dann gilt $f(1_G) = 1_H$ (denn $f(1) \cdot 1 = f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, kürzen) und $f(g^{-1}) = f(g)^{-1}$ für alle $g \in G$ (wegen $f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$).
Das Bild $f(G) := \{f(g) \mid g \in G\}$ ist eine Untergruppe von H, und der Kern $\ker f := f^{-1}(1) := \{g \in G \mid f(g) = 1\}$ ist eine Untergruppe von G.
Genau dann ist f injektiv, wenn $f^{-1}(1) = \{1\}$ gilt (Begründung: $f(x) = f(y) \Leftrightarrow f(x)f(y)^{-1} = 1 \Leftrightarrow f(xy^{-1}) = 1$).
Ist f ein Isomorphismus, so ist auch die Umkehrabbildung $f^{-1} : H \to G$ ein Isomorphismus (wie in der Linearen Algebra).

2.4 Satz (Cayley)**.** *Jede Gruppe $(G, \cdot)$ ist isomorph zu einer Untergruppe von* $\operatorname{Sym} G$.

Beweis. Für jedes $g \in G$ ist die Linksmultiplikation $L_g : G \to G : x \mapsto g \cdot x$ bijektiv (die Umkehrabbildung ist $L_{g^{-1}}$; im Beweis zu 1.6 wurden Rechtsmultiplikationen benutzt), also $L_g \in \operatorname{Sym} G$.

Die Abbildung $L : G \to \operatorname{Sym} G : g \mapsto L_g$ ist ein Homomorphismus, denn $L_{gh}(x) = (gh)x = g(hx) = L_g(L_h(x))$ für alle $x \in G$, also $L_{gh} = L_g \circ L_h$ für alle $g, h \in G$. Ferner ist L injektiv: $L_g = L_h \Rightarrow L_g(1) = L_h(1) \Rightarrow g = h$. Also ist L ein Isomorphismus von G auf das Bild $L(G) \leq \operatorname{Sym} G$. □

2.5 Definition. Sei G eine Gruppe und M eine Menge. Eine Wirkung (Operation, Aktion, Permutationsdarstellung) von G auf M ist ein Homomorphismus

$$\varphi : G \to \operatorname{Sym} M.$$

Eine Wirkung φ heißt treu (oder effektiv), falls φ injektiv ist; dann gilt $G \cong \varphi(G) \leq \operatorname{Sym} G$ (siehe Beweis zu 2.4).

Statt $\varphi(g)(m)$ schreibt man oft $g(m)$ oder gm (oder m^g), d. h. man unterdrückt φ. Ist $m \in M$, so heißt $G(m) := \{g(m) \mid g \in G\}$ die Bahn (oder der Orbit) von m unter G.

Eine Wirkung von G auf M heißt transitiv, falls $\forall m, m' \in M\ \exists g \in G : g(m) = m'$. Dies bedeutet $G(m) = M$ für alle $m \in M$, d.h. es gibt nur eine Bahn, nämlich M.

Für jedes $m \in M$ ist $G_m := \{g \in G \mid g(m) = m\}$ eine Untergruppe von G, der Stabilisator (oder die Standgruppe) von m.

2.6 Beispiele.

a) Für jede Gruppe G und jede Menge M existiert die triviale Wirkung $G \to \operatorname{Sym} M : g \mapsto \mathrm{id}_M$. Diese Wirkung ist nur für $|G| = 1$ treu. Ferner gilt hier $G(m) = \{m\}$ für jedes $m \in M$, daher ist die triviale Wirkung nur für $|M| = 1$ transitiv.

b) Ist G als eine Gruppe von Bijektionen auf einer Menge M definiert, so ist $\mathrm{id} : G \to \operatorname{Sym} M$ eine Wirkung, die „natürliche“ Wirkung von G.
Spezialfälle: $\operatorname{Sym} M$ wirkt transitiv und treu auf M. Für jeden Vektorraum V wirkt $\mathrm{GL}(V)$ auf der Menge V; dabei ist $\{0\}$ eine Bahn, und $\mathrm{GL}(V)$ wirkt transitiv und treu auf der anderen Bahn $V \setminus \{0\}$, falls $V \neq \{0\}$.

c) Für jede Gruppe G ist $L : G \to \operatorname{Sym} G$ mit $L(g)(x) = gx$ für $g, x \in G$ eine Wirkung, die linksreguläre Wirkung (siehe Beweis zu 2.4). Die rechtsreguläre Wirkung $R : G \to \operatorname{Sym} M$ ist durch $R(g)(x) = xg^{-1}$ definiert. Diese beiden Wirkungen sind treu und transitiv.

d) Sei V ein Vektorraum und P die Menge aller eindimensionalen Unterräume von V. Die Gruppe $\mathrm{GL}(V)$ wirkt transitiv auf P, aber i. A. nicht treu (Vielfache von id_V bewirken id_P).

2.7 Satz. *Die Gruppe G wirke auf der Menge M. Dann bilden die Bahnen von G in M eine Partition von M. Ist G endlich und $m \in M$, so gilt*

$$|G(m)| = |G : G_m| = \frac{|G|}{|G_m|}.$$

(*„Bahnlänge = Stabilisatorindex“*)

Beweis. Durch $m \sim m' \Leftrightarrow \exists g \in G : g(m) = m'$ wird eine Äquivalenzrelation $\sim$ auf M definiert (weil G eine Gruppe ist). Die Bahnen von G in M sind genau die Äquivalenzklassen von $\sim$, bilden also eine Partition von M.

Sei jetzt G endlich und $m \in M$. Die „Auswertungsabbildung“ $A : G \to G(m) : g \mapsto g(m)$ ist surjektiv, und für jedes $g \in G$ hat das Urbild

$$\begin{aligned} A^{-1}(g(m)) &= \{h \in G \mid A(h) = g(m)\} \\ &= \{h \in G \mid h(m) = g(m)\} \\ &= \{h \in G \mid g^{-1}h(m) = m\} \\ &= \{h \in G \mid g^{-1}h \in G_m\} \\ &= \{h \in G \mid h \in gG_m\} = gG_m \end{aligned}$$

genau $|G_m|$ Elemente. Die Urbilder $A^{-1}(x)$ mit $x \in G(m)$ bilden eine Partition von G, daher gilt $|G| = \sum_{x \in G(m)} |A^{-1}(x)| = \sum_{x \in G(m)} |G_m| = |G(m)| \cdot |G_m|$. Dies impliziert $|G(m)| = \frac{|G|}{|G_m|} = |G : G_m|$. □

2.8 Beispiel (Drehungen eines Würfels)**.** Die Gruppe

$$\mathrm{SO}_3\,\mathbb{R} := \{A \in \mathrm{GL}_3\,\mathbb{R} \mid A \cdot A^{\mathrm{transp}} = I \text{ und } \det A = 1\}$$

ist die Gruppe aller Drehungen in $\mathbb{R}^3$, welche den Nullpunkt $0 \in \mathbb{R}^3$ fest lassen.

Zum Würfel $W := \{1, -1\}^3 \subseteq \mathbb{R}^3$ gehört die Gruppe $G := \{g \in \mathrm{SO}_3\,\mathbb{R} \mid g(W) = W\}$ aller Drehungen, welche W invariant lassen. Diese Gruppe G wirkt transitiv auf W, und für $w \in W$ gilt $|G_w| = 3$. Mit 2.7 folgt $|G| = |W| \cdot |G_w| = 8 \cdot 3 = 24$. (Man kann statt der 8 Ecken des Würfels auch die 6 Seitenflächen oder die 12 Kanten betrachten; deren Stabilisatoren haben die Ordnung 4 bzw. 2.)

Sei R die Menge der vier Raumdiagonalen von W (oder Antipodenpaare $\{w, -w\}$ mit $w \in W$). Für $g \in G$, $r \in R$ ist $g(r) \in R$, daher hat man eine Wirkung $\varphi : G \to \mathrm{Sym}\,R$, die durch $\varphi(g)(r) := g(r)$ definiert ist. Diese Wirkung φ ist treu (denn $\varphi(g) = \mathrm{id}_R$ besagt, dass $g(w) = \pm w$ für jedes $w \in W$; hat $g \in \mathrm{GL}_3\,\mathbb{R}$ jedes Element von W als Eigenvektor, so ist $g = rI$ für ein $r \in \mathbb{R}$ (Übung zur Linearen Algebra); wegen $1 = \det g = r^3$ folgt dann $r = 1$, also $g = I$).

Daher ist $\varphi(G) \cong G$ eine Untergruppe von $\mathrm{Sym}\,R \cong S_4$ der Ordnung 24. Wegen $|S_4| = 24$ folgt $\varphi(G) = \mathrm{Sym}\,R$, also $G \cong S_4$.

2.9 Definition. Für jede Gruppe G ist $i : G \to \mathrm{Aut}\,G : g \mapsto i_g$ mit

$$i_g(x) = gxg^{-1}$$

eine Wirkung auf der Menge G (wegen $i_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = i_g(i_h(x)) = i_g \circ i_h(x)$ für $x \in G$, also $i_{gh} = i_g \circ i_h$ für $g, h \in G$), die Konjugationswirkung oder Wirkung durch innere Automorphismen (vgl. 2.2).

Die Bahn $\{gxg^{-1} \mid g \in G\}$ heißt die Konjugiertenklasse von $x \in G$, und alle Elemente dieser Bahn heißen konjugiert zu x (vgl. Ähnlichkeit von Matrizen).

Der Zentralisator $\mathrm{C}_G(x) := \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$ von x ist der Stabilisator von x in der Konjugationswirkung. Der Kern der Konjugationswirkung ist $i^{-1}(\mathrm{id}_G) = \{g \in G \mid i_g = \mathrm{id}_G\} = \{g \in G \mid gxg^{-1} = x \text{ für alle } x \in G\} = \bigcap_{x\in G} \mathrm{C}_G(x) = Z(G)$, das Zentrum von G, vgl. ÜA 6.

2.10 Satz. *Sei G eine endliche Gruppe und $x \in G$. Dann hat die Konjugiertenklasse $\{gxg^{-1} \mid g \in G\}$ von x genau $|G : \mathrm{C}_G(x)|$ Elemente. Ferner gilt die sogenannte Klassengleichung*

$$|G| = |Z(G)| + \sum_{j=1}^{t} |K_j|,$$

wobei $K_1, K_2, ..., K_t$ die verschiedenen Konjugiertenklassen von G mit $|K_j| > 1$ sind.

Beweis. Die Konjugiertenklasse von x ist die Bahn von x in der Konjugationswirkung, und nach 2.7 ist $|G : \mathrm{C}_G(x)|$ die Länge (= Anzahl der Elemente) dieser Bahn. Nach 2.7 bilden die Konjugiertenklassen eine Partition von G, daher ist $|G|$ die Summe der Längen der sämtlichen Konjugiertenklassen.

Die Konjugiertenklasse $K = \{gxg^{-1} \mid g \in G\}$ von x hat genau dann die Länge 1, wenn $K = \{x\}$ gilt, d. h. wenn $gxg^{-1} = x$ für alle $g \in G$ gilt, und dies besagt $x \in Z(G)$. Daher ist $|Z(G)|$ die Anzahl der Konjugiertenklassen der Länge 1. □

2.11 Korollar. *Für jede endliche Gruppe $G \neq \{1\}$ von Primzahlpotenzordnung gilt $Z(G) \neq \{1\}$.*

Beweis. Es gilt $|G| = p^n$ mit einer Primzahl p und $n \in \mathbb{N}$. Nach 2.10 ist $|G| = |Z(G)| + \sum_j |K_j|$ und $|K_j| = |G : \mathrm{C}_G(x_j)| = p^{n_j}$ mit $n_j > 0$ (wegen $|K_j| > 1$), wobei $x_j \in K_j$. Daher ist $|Z(G)| = |G| - \sum_j |K_j|$ durch p teilbar, also $Z(G) \neq \{1\}$. □

3. Normalteiler, Faktorgruppen und Isomorphiesätze

3.1 Definition. Eine Untergruppe U einer Gruppe G heißt Normalteiler von G (auch: normal oder invariant in G), falls $gU = Ug$ für alle $g \in G$ gilt; man schreibt dann $U \trianglelefteq G$.

3.2 Lemma. *Eine Untergruppe U einer Gruppe G ist genau dann normal in G, wenn eine der folgenden Bedingungen gilt:*

(i) $\forall g \in G : gU \subseteq Ug$ (*dies bedeutet* $\forall g \in G\, \forall u \in U\, \exists u' \in U : gu = u'g$).

(ii) $\forall g \in G : i_g(U) := gUg^{-1} \subseteq U$ (*Invarianz unter inneren Automorphismen*).

(iii) *U ist Vereinigung von Konjugiertenklassen von G.*

Beweis. Bedingung (i) folgt aus 3.1. Gilt (i), so folgt $g^{-1}gUg^{-1} \subseteq g^{-1}Ugg^{-1}$ für alle $g \in G$, also $Uh \subseteq hU$ für alle $h \in G$; dies ist die andere Inklusion.
(i) $\Leftrightarrow$ (ii): multipliziere mit g^{-1} bzw. mit g von rechts.
(ii) $\Leftrightarrow$ (iii) gilt wegen $\bigcup_{u\in U}\{gug^{-1} \mid g \in G\} = \bigcup_{g\in G} gUg^{-1}$. □

3.3 Beispiele. a) In jeder Gruppe gilt $\{1\} \trianglelefteq G$ und $G \trianglelefteq G$. Jede Untergruppe U des Zentrums $Z(G)$ einer Gruppe G ist normal in G. Insbesondere ist in einer abelschen Gruppe jede Untergruppe normal (in Q_8 auch, in D_8 aber nicht; also sind D_8 und Q_8 nicht isomorph).

b) Ist $f : G \to H$ ein Homomorphismus zwischen Gruppen G und H, so ist $\ker f$ ein Normalteiler von G, denn:
$a \in \ker f, g \in G \Rightarrow f(a) = 1 \Rightarrow f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)f(g)^{-1} = 1 \Rightarrow gag^{-1} \in \ker f$, also ist $\ker f \trianglelefteq G$ nach 3.2(ii).
Insbesondere ist $\mathrm{SL}_n \mathbb{R} = \ker(\det) \trianglelefteq \mathrm{GL}_n \mathbb{R}$.

c) Jede Untergruppe U vom Index 2 in einer Gruppe G ist normal in G.
(Beweis: Für $g \in U$ gilt $gU = U = Ug$. Sei jetzt $g \in G \setminus U$. Dann ist $gU \neq U \neq Ug$, also $gU \cap U = \emptyset$ und $G = U \cup Ug$ wegen $|G : U| = 2$. Dies impliziert $gU \subseteq G \setminus U = Ug$). Die Behauptung ist auch ein Spezialfall von ÜA 9(d).

3.4 Definition. Sei G eine Gruppe, $N \trianglelefteq G$ und $G/N := \{gN \mid g \in G\}$ die Menge aller Nebenklassen von N in G (also $|G/N| = |G : N| = \frac{|G|}{|N|}$, falls G endlich ist). Wir definieren auf der Menge G/N eine Verknüpfung $*$ durch

$$gN * hN := ghN \quad \text{für alle } g, h \in G.$$

Mit der Schreibweise gN hat man einen Repräsentanten g der Nebenklassen gN gewählt; die Verknüpfung $*$ ist wohldefiniert (d. h. unabhängig von der Wahl der Repräsentanten g, h) wegen $gN = g'N$, $hN = h'N \Rightarrow g' \in gN$, $h' \in hN \Rightarrow g'h' \in gNhN = ghNN = ghN \Rightarrow g'h'N = ghN$ für $g, g', h, h' \in N$.

Wir haben eben das elementweise Produkt $XY := \{xy \mid x \in X, y \in Y\}$ für Teilmengen X, Y von G benutzt; die Gleichung $gNhN = ghN$ zeigt, dass $*$ einfach das elementweise Produkt von zwei Nebenklassen ist. Wir unterdrücken $*$.

3.5 Satz. *Sei G eine Gruppe und N ein Normalteiler von G. Dann ist G/N mit der Verknüpfung aus 3.4 eine Gruppe, die Faktorgruppe von G nach N (auch: der Quotient, oder G modulo N). Ferner ist die kanonische Projektion $p : G \to G/N : g \mapsto gN$ ein Epimorphismus mit dem Kern N.*

Beweis. Die Abbildung $p : G \to G/N$ ist surjektiv (nach Definition von G/N) und multiplikativ (nach 3.4). Daher ist die Verknüpfung von G/N assoziativ, hat $p(1) = 1 \cdot N = N \in G/N$ als Neutralelement, und $p(g^{-1}) = g^{-1}N$ ist invers zu gN. Also ist G/N eine Gruppe und $p : G \to G/N$ ein Epimorphismus. □

3.6 Korollar. *Die Normalteiler einer Gruppe G sind genau die Kerne der Homomorphismen von G in irgendeine Gruppe.*

Beweis. 3.3b) und 3.5. □

Triviale Beispiele: $G/G \cong \{1\}$, $G/\{1\} \cong G$.

3.7 Satz (Homomorphiesatz, Erster Isomorphiesatz)**.** *Sei $f : G \to H$ ein Homomorphismus zwischen Gruppen G und H. Dann gilt: $G/\ker f \cong f(G)$.*
(*„Definitionsbereich modulo Kern ist isomorph zum Bild.“*)

Beweis. Sei $N = \ker f$. Die Abbildung $F : G/N \to H : gN \mapsto f(g)$ ist wohldefiniert und injektiv, denn für $g, g' \in G$ gilt $gN = g'N \Leftrightarrow g^{-1}g' \in N \Leftrightarrow f(g^{-1}g') = 1 \Leftrightarrow f(g)^{-1}f(g') = 1 \Leftrightarrow f(g) = f(g')$. Daher ist $F : G/N \to f(G)$ bijektiv, sogar ein Isomorphismus wegen $F(gNg'N) = F(gg'N) = f(gg') = f(g)f(g') = F(gN)F(g'N)$ für alle $g, g' \in G$. □

Nach 3.7 sind die epimorphen Bilder einer Gruppe G (bis auf Isomorphie) genau die Faktorgruppen von G. Die Konjugationswirkung $i : G \to \operatorname{Aut} G$ hat den Kern $Z(G)$, siehe 2.9; nach 3.7 ist $G/Z(G)$ isomorph zur Gruppe $i(G)$ aller inneren Automorphismen von G.

Anwendung von 3.7 auf zyklische Gruppen:

3.8 Korollar. *Jede unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}, +)$. Jede zyklische Gruppe der Ordnung $n \in \mathbb{N}$ ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$, insbesondere gilt $C_n \cong \mathbb{Z}/n\mathbb{Z}$.*

Beweis. Sei $G = \langle g \rangle$ eine zyklische Gruppe. Dann ist $f : \mathbb{Z} \to G : z \mapsto g^z$ ein Epimorphismus. Im Fall $\ker f = \{0\}$ ist f injektiv, also ein Isomorphismus, also $\mathbb{Z} \cong G$. Andernfalls ist $\ker f = m\mathbb{Z}$ für ein $m \in \mathbb{N}$, siehe 1.12. Mit 3.7 folgt $\mathbb{Z}/m\mathbb{Z} \cong G$. Dabei ist m die Ordnung von g und von G, siehe 1.15, also $|G| = m$. Wegen $|C_n| = n$ folgt auch $C_n \cong \mathbb{Z}/n\mathbb{Z}$. □

3.9 Satz (Zweiter Isomorphiesatz)**.** *Sei G eine Gruppe, $U \leq G$ und $N \trianglelefteq G$. Dann folgt $UN \leq G$ und $U \cap N \trianglelefteq U$, und es gilt $UN/N \cong U/U \cap N$.*

Beweis. $f : U \to G/N : u \mapsto uN$ ist die Einschränkung der kanonischen Projektion p aus 3.5 auf U, also ein Homomorphismus. Nach 3.3b) ist $\ker f = \{u \in U \mid uN = N\} = \{u \in U \mid u \in N\} = U \cap N$ normal in U, und $UN \leq G$ gilt nach ÜA 9(b). Mit 3.7 folgt $U/U \cap N \cong f(U) \cong UN/N$. □

3.10 Satz (Dritter Isomorphiesatz)**.** *Seien U und V Normalteiler einer Gruppe G mit $U \leq V$. Dann ist V/U normal in G/U, und es gilt $(G/U)/(V/U) \cong G/V$.*

Beweis. Die Abbildung $f : G/U \to G/V : gU \mapsto gV$ ist wohldefiniert wegen $U \subseteq V$. Ferner ist f ein Epimorphismus mit dem Kern V/U, also $V/U \trianglelefteq G/U$ nach 3.3b). Mit 3.7 folgt die Behauptung. □

3.11 Definition. Eine Gruppe $G \neq \{1\}$ heißt einfach, wenn $\{1\}$ und G die einzigen Normalteiler von G sind.

Die einfachen abelschen Gruppen sind gerade die zyklischen Gruppen C_p von Primzahlordnung (denn: jedes nichttriviale Element ist ein Erzeuger der Gruppe, 1.12 und 3.8). Weitere Beispiele: $\mathrm{PSL}_n K := \mathrm{SL}_n K/Z(\mathrm{SL}_n K)$ für $n \geq 3$, K ein beliebiger Körper (und für $n = 2$, $|K| \geq 4$). Insbesondere sind die Gruppen $\mathrm{GL}_n \mathbb{F}_2 = \mathrm{SL}_n \mathbb{F}_2 \cong \mathrm{PSL}_n \mathbb{F}_2$ mit $n \geq 3$ einfach (und nicht abelsch und endlich), wobei $\mathbb{F}_2 = \{0, 1\}$). Siehe auch 5.9.

4. Die Sätze von Sylow

Die Umkehrung von 1.6 (Satz von Lagrange) ist falsch: die Gruppen S_5, S_6, S_7 haben keine Untergruppe der Ordnung 15, siehe 5.4(c).

4.1 Satz (Cauchy)**.** *Sei G eine endliche Gruppe und p ein Primteiler von $|G|$. Dann enthält G ein Element (also auch eine Untergruppe) der Ordnung p.*

Beweis. (J. H. McKay, Another proof of Cauchy's group theorem. Amer. Math. Monthly 66, 1959, 119) Die Menge $M := \{(g_1, g_2, \ldots, g_p) \in G^p \mid \prod_{i=1}^{p} g_i = 1\}$ hat genau $|G|^{p-1}$ Elemente, weil g_p durch die anderen g_i eindeutig bestimmt ist: $g_p = (g_1 \cdots g_{p-1})^{-1}$. Aus $(g_1, \ldots, g_p) \in M$ folgt $g_2 \cdot g_3 \cdots g_p = g_1^{-1}$ und dann $g_2 \cdot g_3 \cdots g_p g_1 = 1$, also gilt $(g_2, g_3, \ldots, g_p, g_1) \in M$. Daher haben wir eine Abbildung

$$f : M \to M : (g_1, \ldots, g_p) \mapsto (g_2, g_3, \ldots, g_p, g_1).$$

Es gilt $f^p = \mathrm{id}_M$. Daher hat $f \in \operatorname{Sym} M$ die Ordnung p (und die Abbildung $C_p \to \operatorname{Sym} M : i \mapsto f^i$ ist eine Wirkung von C_p auf M). Die Bahnen von $\langle f \rangle \leq \operatorname{Sym} M$ haben die Länge 1 oder p und bilden eine Partition von M, wegen 2.7 und weil p eine Primzahl ist. Daher gilt

$$|M| = 1 \cdot a_1 + p \cdot a_p$$

wobei a_j die Anzahl der Bahnen der Länge j ist. Weil $|M| = |G|^{p-1}$ durch p teilbar ist, ist auch $a_1 = |\{m \in M \mid f(m) = m\}|$ durch p teilbar. Ferner ist $(1, 1, \ldots, 1) \in M$ ein Fixpunkt von f, also $a_1 > 0$. Es folgt $a_1 \geq p \geq 2$.

Daher hat f einen Fixpunkt $m = (g_1, g_2, \ldots, g_p) \in M$ mit $m \neq (1, 1, \ldots, 1)$. Wegen $f(m) = m$ gilt $g_1 = g_2 = \cdots = g_p$, wegen $m \in M$ ist $g_1^p = 1$, und wegen $m \neq (1, 1, \ldots, 1)$ ist $g_1 \neq 1$. Nach 1.15 hat $g_1 \in G$ die Ordnung p. □

4.2 Satz (Sylow 1872)**.** *Sei G eine endliche Gruppe und p eine Primzahl. Ist $n \in \mathbb{N}$ und p^n ein Teiler von $|G|$, so enthält G eine Untergruppe der Ordnung p^n.*

Beweis. Durch Induktion nach $|G|$. Die Behauptung gilt für $|G| = 1$ (auch für $|G| = 2, 3$).
Induktionsvoraussetzung: Der Satz gilt für alle Gruppen mit einer Ordnung $< |G|$.
1. Fall: p teilt $|Z(G)|$.
Nach 4.1 hat $Z(G)$ eine Untergruppe C der Ordnung p und $C \trianglelefteq G$ nach 3.3(a). Ferner ist p^{n-1} ein Teiler von $|G/C| = \frac{|G|}{p} < |G|$. Nach Induktionsvoraussetzung hat G/C eine Untergruppe der Ordnung p^{n-1}. Diese Untergruppe hat nach ÜA 10 die Form U/C mit $C \leq U \leq G$. Wir erhalten $|U| = |U/C| \cdot |C| = p^{n-1} \cdot p = p^n$.
2. Fall: p ist kein Teiler von $|Z(G)|$.
Nach 2.10 gilt die Klassengleichung $|G| = |Z(G)| + \sum_j |G : U_j|$, wobei $U_j \leq G$ und $|G : U_j| > 1$ für alle j (die U_j sind Zentralisatoren, aber das spielt hier keine Rolle). Weil $|G|$ durch p teilbar ist, $|Z(G)|$ aber nicht, ist für mindestens ein j die Zahl $|G : U_j| = \frac{|G|}{|U_j|}$ nicht durch p teilbar. Dann ist p^n ein Teiler von $|U_j| < |G|$. Nach Induktionsvoraussetzung hat U_j (also auch G) eine Untergruppe der Ordnung p^n. □

4.3 Definition. Sei G eine endliche Gruppe und p eine Primzahl. Sei $m \in \mathbb{N}_0$ der Exponent von p in der Primzahlzerlegung von $|G|$, d. h. p^m teilt $|G|$, p^{m+1} aber nicht. Man nennt dann jede Untergruppe der Ordnung p^m von G eine p-Sylowgruppe von G. Die Menge $\mathrm{Syl}_p G := \{P \mid P \leq G, |P| = p^m\}$ aller p-Sylowgruppen von G ist nach 4.2 nicht leer.

Eine endliche Gruppe H heißt p-Gruppe für eine Primzahl p, falls $|H| = p^k$ mit $k \in \mathbb{N}_0$.

4.4 Satz (Sylow)**.** *Sei G eine endliche Gruppe und p eine Primzahl.*

(a) *Jede p-Untergruppe von G liegt in einer p-Sylowgruppe von G.*

(b) *Je zwei p-Sylowgruppen sind konjugiert in G (zwei Untergruppen sind konjugiert, falls es einen inneren Isomorphismus gibt, welcher die erste auf die zweite abbildet).*

(c) *Die Anzahl $|\mathrm{Syl}_p G|$ der p-Sylowgruppen von G ist ein Teiler von $|G : P|$ von der Form $1 + k \cdot p$ mit $k \in \mathbb{N}_0$, wobei $P \in \mathrm{Syl}_p G$.*

Beweis. Nach 4.2 existiert ein $P \in \mathrm{Syl}_p G$. Wir setzen

$$M := \{gPg^{-1} \mid g \in G\} \subseteq \mathrm{Syl}_p G.$$

Die Gruppe G wirkt durch Konjugation transitiv auf M, mit dem Stabilisator $G_P = \{g \in G \mid gPg^{-1} = P\}$ (der auch als Normalisator von P bezeichnet wird). Nach 2.7 ist $|M| = |G : G_P| = |G|/|G_P|$ ein Teiler von $|G : P|$, da $P \leq G_P$. Wegen $P \in \mathrm{Syl}_p G$ ist $|G : P|$ und dann auch $|M|$ *nicht* durch p teilbar.

Wir beweisen die Behauptungen des Satzes, indem wir verschiedene Untergruppen von G auf M wirken lassen.

(a) Sei $U \leq G$ eine p-Gruppe. Auch U wirkt durch Konjugation auf M; nach 2.7 ist dabei jede Bahnlänge eine Potenz von p. Weil $|M|$ nicht durch p teilbar ist, hat U (mindestens) einen Fixpunkt $Q \in M$. Für $u \in U$ gilt $uQu^{-1} = Q$, also $uQ = Qu$ und daher $UQ = QU$. Nach ÜA 8 ist UQ eine p-Untergruppe von G. Wegen $Q \leq UQ$ und $Q \in \mathrm{Syl}_p G$ folgt $Q = UQ$, also $U \leq Q$.

(b) Sei jetzt $U \in \mathrm{Syl}_p G$. Dann liefert die Argumentation zu (a) ein $Q \in M$ mit $U \leq Q$. Wegen $|U| = |Q|$ folgt $U = Q = gPg^{-1}$ für ein $g \in G$. Dies beweist (b) und $\mathrm{Syl}_p G = M$. Insbesondere ist $|\mathrm{Syl}_p G| = |M|$ ein Teiler von $|G : P|$.

(c) Auch P wirkt auf $M = \mathrm{Syl}_p G$ durch Konjugation und hat dabei den Fixpunkt P. Ist $Q \in \mathrm{Syl}_p G$ ein Fixpunkt dieser Wirkung, so folgt $P \leq Q$ wie bei (a), wegen $|P| = |Q|$ also $Q = P$. Demnach ist $\{P\}$ die einzige Bahn der Länge 1, alle anderen Bahnlängen sind (nach 2.7) durch p teilbar. Daher hat $|\mathrm{Syl}_p G|$ die Form $1 + k \cdot p$ mit $k \in \mathbb{N}_0$. □

4.5 Korollar. *Sei G eine endliche Gruppe, p eine Primzahl und $P \in \mathrm{Syl}_p G$. Genau dann gilt $|\mathrm{Syl}_p G| = 1$, also $\mathrm{Syl}_p G = \{P\}$, wenn P ein Normalteiler von G ist.*

Beweis. $\mathrm{Syl}_p G = \{P\} \Leftrightarrow \forall g \in G : gPg^{-1} = P \Leftrightarrow P \trianglelefteq G$. □

4.6 Beispiele. Sei G eine Gruppe der Ordnung pq mit Primzahlen $p < q$. Nach 4.4 ist $|\operatorname{Syl}_q G|$ ein Teiler von p von der Form $1+kq$, also gleich 1. Nach 4.5 hat G eine normale q-Sylowgruppe $Q \cong C_q$ (insbesondere ist G nicht einfach). Wähle $P \in \operatorname{Syl}_p G$; dann ist $P \cong C_p$. Wegen $P \cap Q = \{1\}$ ist $|PQ| = pq$ nach ÜA 8(c), also $G = PQ$. Nach ÜA 14(a) ist G isomorph zu einem semidirekten Produkt $C_q \rtimes_\varphi C_p$ mit einem Homomorphismus $\varphi : C_p \to \operatorname{Aut} C_q$.

Nach 4.4 ist $|\operatorname{Syl}_p G|$ ein Teiler von q, also gleich 1 oder q. Gilt zusätzlich, dass p kein Teiler von $q-1$ ist, so folgt $|\operatorname{Syl}_p G| = 1$ nach 4.4(c). Nach ÜA 12(b) ist dann G isomorph zum direkten Produkt $C_q \times C_p \cong C_{pq}$, weil $(1,1) \in C_p \times C_q$ die Ordnung pq hat (vgl. auch 6.1).

Insbesondere ist jede Gruppe der Ordnung 15 zyklisch. Jede Gruppe G der Ordnung 6 ist isomorph zu $C_3 \rtimes_\varphi C_2$ mit $\varphi : C_2 \to \operatorname{Aut} C_3 \cong C_2$; es gibt nur zwei Möglichkeiten für φ, also höchstens zwei Isomorphietypen für G, nämlich C_6 und $D_6 \cong S_3$.

5. Die symmetrischen Gruppen

Ist $f : M \to N$ eine Bijektion zwischen zwei Mengen M und N, so ist $\operatorname{Sym} M$ isomorph zu $\operatorname{Sym} N$ (via $g \mapsto f \circ g \circ f^{-1}$). Wir betrachten die endlichen symmetrischen Gruppen $S_n := \operatorname{Sym}\{1, 2, \ldots, n\}$ vom Grad n. Die Elemente von S_n heißen auch Permutationen, und die Untergruppen von S_n Permutationsgruppen.

5.1 Definition. Sind $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ paarweise verschieden, so definiert man $g \in S_n$ durch

$$\begin{aligned} g(a_i) &= a_{i+1} \text{ für } 1 \le i < k \\ g(a_k) &= a_1 \\ g(a) &= a \text{ sonst (d.h. falls } a \ne a_i \text{ für alle } i) \end{aligned}$$

und nennt g einen k-Zyklus; man schreibt dann $g = (a_1\ a_2\ a_3\ \ldots\ a_k)$ oder $g = (a_1, a_2, a_3, \ldots, a_k)$. Die 2-Zyklen heißen auch Transpositionen. Fixpunkte werden in dieser Notation unterdrückt.

5.2 Beispiele und Folgerungen. $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$ in S_n mit $n \ge 4$.

Die Verknüpfung gh bedeutet $g \circ h$ also $(1\ 2)(2\ 3) = (1\ 2\ 3)$ und $(2\ 3)(1\ 2) = (1\ 3\ 2) \ne (1\ 2\ 3)$; bei manchen anderen Autoren bedeutet gh: zuerst g, dann h anwenden.

Jeder k-Zyklus hat die Ordnung k und lässt sich als ein Produkt von $k-1$ Transpositionen schreiben, etwa $(1\ 2\ 3\ \ldots k) = (1\ 2)(2\ 3)\ldots(k-1\ k)$.

Für alle $f \in S_n$ gilt $f(a_1, a_2, \ldots, a_k)f^{-1} = (f(a_1), f(a_2), \ldots, f(a_k))$, denn: beide Seiten bilden $f(a_i)$ ab auf $f(a_{i+1})$ für $i < k$, und $f(a_k)$ auf $f(a_1)$, und fixieren die restlichen Ziffern.

Insbesondere folgt aus $f(a_i) = a_i$ für $1 \le i \le k$, dass f mit $(a_1, a_2, \ldots, a_k)$ vertauschbar ist. Daher sind zwei Zyklen $(a_1, a_2, \ldots, a_k)$ und $(b_1, b_2, \ldots, b_l)$ mit $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \emptyset$ (disjunkte Zyklen) vertauschbar.

5.3 Zyklenzerlegung. Sei $g \in S_n$ beliebig, sei $B \subseteq \{1, 2, \ldots, n\}$ eine Bahn von $\langle g \rangle$ und $b \in B$. Dann ist die Einschränkung $g|_B$ ein Zyklus der Länge $k = |B|$, nämlich

$$g|_B = \big(b, g(b), g^2(b), \ldots, g^{k-1}(b)\big) .$$

Die sämtlichen Bahnen von $\langle g \rangle$ bilden nach 2.7 eine Partition von $\{1, 2, \ldots, n\}$. Daher ist

$$g = \prod_{i=1}^{t} g_i$$

ein Produkt von paarweise disjunkten Zyklen g_i, wobei t die Anzahl der Bahnen von $\langle g \rangle$ ist (Bahnen der Länge 1 kann man weglassen, vgl. 5.1). Diese Produktdarstellung für g ist die Zyklenzerlegung von g; sie ist eindeutig bestimmt bis auf die Reihenfolge der vertauschbaren Zyklen g_i (denn die g_i sind die Einschränkungen von g auf die Bahnen von $\langle g \rangle$).
Beispiel: $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4) = (2\ 4)(1\ 2)$.

5.4 Folgerungen. (a) Die Gruppe S_n wird von ihren Transpositionen erzeugt (siehe 5.3 und 5.2).

(b) Zwei Permutationen $g, g' \in S_n$ sind genau dann konjugiert in S_n, wenn die Zyklenzerlegungen von g und g' vom „gleichen Typ“ sind, d. h. beide Zerlegungen erhalten gleich viele k-Zyklen für jedes k.
Beispiel: $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ und $(1\ 2\ 3\ 4)(5\ 6)(7\ 8)$ sind nicht konjugiert.

(c) Ist $g = \prod_{i=1}^{t} g_i$ mit paarweise disjunkten Zyklen g_i, so ist die Ordnung von g das kleinste gemeinsame Vielfache der Ordnungen (Zyklenlängen) der g_i (wegen $g^m = \prod_{i=1}^{t} g_i^m$ für alle $m \in \mathbb{N}$).
Beispiel: S_7 enthält kein Element der Ordnung 15, denn als Zyklenlängen einer solchen Permutation sind nur $1, 3, 5, 15$ möglich, wegen $3 + 5 > 7$ bleiben nur $1, 3$ oder $1, 5$, ein Widerspruch. Nach 4.6 hat S_7 dann keine Untergruppe der Ordnung 15, und S_5 und S_6 auch nicht.

5.5 Satz. *Für jedes $n \in \mathbb{N}$ gibt es genau einen Homomorphismus* $\operatorname{sgn} : S_n \to (\{1, -1\}, \cdot)$ *mit* $\operatorname{sgn}(t) = -1$ *für jede Transposition $t \in S_n$.*

Beweis. Sei $g \in S_n$. Dann ist $\prod_{n \geq i > j \geq 1}(i - j) = \pm \prod_{i>j}(g(i) - g(j))$, also

$$\operatorname{sgn}(g) := \prod_{i>j} \frac{g(i) - g(j)}{i - j} \in \{1, -1\}.$$

Die Anzahl $N(g)$ der negativen Zähler in diesem Produkt ist die Anzahl der Paare (i, j) mit $i > j$ und $g(i) < g(j)$, also gilt $\operatorname{sgn}(g) = (-1)^{N(g)}$.

Zur Multiplikativität: für $g, h \in S_n$ gilt

$$\operatorname{sgn}(g \circ h) = \prod_{i>j} \frac{g(h(i)) - g(h(j))}{h(i) - h(j)} \cdot \prod_{i>j} \frac{h(i) - h(j)}{i - j}.$$

Das zweite Produkt ist $\operatorname{sgn}(h)$. Das erste Produkt stimmt überein mit $\prod_{k>l} \frac{g(k)-g(l)}{k-l} = \operatorname{sgn}(g)$, wegen $\frac{x}{y} = \frac{-x}{-y}$ für $x, y \in \mathbb{Z} \setminus \{0\}$. Also ist sgn ein Homomorphismus.

Für die Transposition $g = (1,2)$ gilt $N(g) = 1$, also $\operatorname{sgn}(g) = (-1)^1 = -1$. Für alle $h \in S_n$ gilt dann $\operatorname{sgn}((h(1), h(2)) = \operatorname{sgn}(h \circ (1,2) \circ h^{-1}) = \operatorname{sgn}(h) \cdot \operatorname{sgn}(1,2) \cdot \operatorname{sgn}(h)^{-1} = -1$, also $\operatorname{sgn}(t) = -1$ für alle Transpositionen $t \in S_n$.

Der Homomorphismus ist durch die Werte auf den Transpositionen eindeutig bestimmt, weil die Transpositionen die S_n erzeugen, siehe 5.4(a). □

5.6 Definition. Man nennt $g \in S_n$ gerade, falls $\operatorname{sgn}(g) = 1$, und ungerade, falls $\operatorname{sgn}(g) = -1$. Nach 5.5 bedeutet dies, dass g sich als Produkt einer geraden bzw. ungeraden Anzahl von Transpositionen schreiben lässt.

Der Homomorphismus sgn aus 5.5 heißt Signum oder Parität, und der zugehörige Kern $A_n := \ker \operatorname{sgn} = \{\operatorname{sgn} \in S_n \mid g \text{ ist gerade}\}$ heißt alternierende Gruppe vom Grad n.

Nach 3.3(b) ist A_n ein Normalteiler von S_n, und $S_n/A_n \cong \operatorname{sgn}(S_n)$ nach 3.7. Für $n \geq 2$ gibt es Transpositionen, d. h. sgn ist surjektiv, also $2 = |S_n/A_n| = |S_n : A_n| = \frac{|S_n|}{|A_n|}$ und daher $|A_n| = \frac{1}{2}n!$.

Warnung: Ein k-Zyklus ist Produkt von $k-1$ Transpositionen und hat daher das Signum $(-1)^{k-1}$, d. h. ein Zyklus gerader Länge ist eine ungerade Permutation, und umgekehrt. Insbesondere enthält A_n alle Zyklen von ungerader Länge, und die Transpositionen liegen in $S_n \setminus A_n$.

5.7 Lemma. (i) *A_n wird von den sämtlichen 3-Zyklen von S_n erzeugt.*

(ii) *Für $n \geq 5$ sind alle 3-Zyklen in A_n konjugiert.*

Beweis. (i) Jedes Element von A_n ist Produkt einer geraden Anzahl von Transpositionen. Daher genügt es zu zeigen, dass jedes Produkt $(a\ b)(c\ d)$ ein Produkt von 3-Zyklen ist. Im Fall $\{a,b\} \cap \{c,d\} = \emptyset$ gilt $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$. Andernfalls dürfen wir $a = c$ annehmen, und dann auch $b \neq d$ (sonst ist $(a\ b)(c\ d) = (a\ b)^2 = 1 = (1\ 2\ 3)^3$); damit folgt $(a\ b)(c\ d) = (a\ b)(a\ d) = (a\ d\ b)$.

(ii) Nach 5.2 sind je zwei 3-Zyklen $d, d' \in S_n$ in S_n konjugiert, d. h. es existiert ein $g \in S_n$ mit $d' = gdg^{-1}$. Im Fall $g \in A_n$ sind wir fertig. Sei jetzt $g \in S_n \setminus A_n$. Wegen $n \geq 5$ existiert eine Transposition t, welche zu d disjunkt ist. Nach 5.2 gilt $tdt^{-1} = d$, also $d' = gdg^{-1} = gtdt^{-1}g^{-1} = (gt)d(gt)^{-1}$ und $gt \in A_n$. □

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

Beweis. Sei $N \neq \{1\}$ ein Normalteiler von A_n. Wenn N einen 3-Zyklus enthält, so enthält N alle 3-Zyklen von S_n (wegen 5.7(ii) und 3.2), und mit 5.7(i) folgt $N = A_n$. Daher genügt es, die Existenz eines 3-Zyklus in N nachzuweisen.

Es existiert ein $x \in N \setminus \{1\}$. Für alle $g \in A_n$ gilt $x(gx^{-1}g^{-1}) \in N$. Es liegt einer der folgenden 3 Fälle vor:

Fall 1: In der Zyklenzerlegung von x kommt ein Zyklus der Länge ≥ 4 vor, d. h. $x = (a\ b\ c\ d\ \ldots)\ldots$ mit vier verschiedenen Ziffern a, b, c, d. Für $g := (a\ b\ c) \in A_n$ gilt

dann $xgx^{-1} = (b\ c\ d)$, siehe 5.2. Wir erhalten $N \ni (xgx^{-1})g^{-1} = (b\ c\ d)(a\ c\ b) = (a\ d\ b)$, ein 3-Zyklus wie gewünscht.

Fall 2: In der Zyklenzerlegung von x kommt ein 3-Zyklus vor.

Man darf annehmen, dass x kein 3-Zyklus ist, also $x = (abc)(de\dots)\dots$ mit fünf verschiedenen Ziffern a, b, c, d, e. Für $g := (abd) \in A_n$ gilt dann $xgx^{-1} = (bce)$, also $N \ni xgx^{-1}g^{-1} = (bce)(adb) = (adceb)$. Gemäß Fall 1 findet man einen 3-Zyklus in N.

Fall 3: In der Zyklenzerlegung von x kommen nur 2-Zyklen und 1-Zyklen vor.

Weil x keine Transposition ist, hat man $x = (ab)(cd)\dots$. Wegen $n \geq 5$ existiert eine Ziffer $e \notin \{a, b, c, d\}$. Für $g := (ace) \in A_n$ gilt dann $xgx^{-1} = (bde')$ mit $e' := x(e)$. Es gilt $e' \neq x(b) = a$ und $e' \neq x(d) = c$. Wir erhalten $N \ni xgx^{-1}g^{-1} = (bde')(aec)$. Im Fall $e = e'$ enthält N die Permutation $(bde)(aec) = (abdec)$, und man findet einen 3-Zyklus in N gemäß Fall 1. Im Fall $e \neq e'$ ist $(bde')(aec) \in N$ das Produkt von zwei disjunkten 3-Zyklen, und man findet einen 3-Zyklus in N gemäß Fall 2. □

5.9 Bemerkung (Endliche einfache Gruppen)**.** Sei G eine endliche einfache Gruppe, welche nicht abelsch ist. Dann ist $|G|$ gerade (Feit und Thompson, Pacific J. Math. 13, 1963, 775–1029) und durch drei verschiedene Primzahlen teilbar (Burnside 1904).

Satz (ca. 1981). Jede endliche einfache Gruppe ist isomorph zu einer der folgenden Gruppen:
(a) C_p mit einer Primzahl p
(b) A_n mit $n \geq 5$
(c) $\mathrm{PSL}_n K$ mit einem endlichen Körper K, oder eine geometrisch definierte Untergruppe davon (16 Familien; siehe Carter, Simple groups of Lie type, Wiley 1989)
(d) die 26 „sporadischen“ Gruppen.[1]

Die kleinste sporadische Gruppe ist die Mathieu-Gruppe $M_{11} := \langle a, b\rangle \leq S_{11}$ mit $a = (1, 2, 3, \dots, 10, 11)$ und $b = (3, 7, 11, 8)(4, 10, 5, 6)$. Es gilt $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7920$. Die größte sporadische Gruppe ist das Monster M mit $|M| = 2^{46} \cdot 3^{10} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}$, das von Bernd Fischer „vorhergesagt“ wurde. [M wird von zwei Elementen mit den Ordnungen 2 und 3 erzeugt (deren Produkt die Ordnung 7 hat), daher ist M eine Faktorgruppe von $\mathrm{SL}_2 \mathbb{Z}$.] Die zweitgrößte sporadische Gruppe ist das Babymonster $BM < M$ mit $|BM| \approx 4 \cdot 10^{33}$. Es gilt $BM \leq S_{13\ 571\ 955\ 000}$ und $M \leq S_n$ mit $n \approx 10^{20}$, ferner $BM < \mathrm{GL}_{4370}\mathbb{F}_2$ und $M < \mathrm{GL}_{196882}\mathbb{F}_2$.

Populäre Bücher dazu: Ronan, Symmetry and the monster, Oxford 2007; Du Sautoy, Die Mondscheinsucher, Beck 2008. (Siehe auch Solomon, A brief history of the classification of the finite simple groups, Bull. Amer. Math. Soc. 38, 2001, 315–352; Steingart, A group theory of group theory, Social Studies of Science 42, 2012, 185–213.)

6. Endlich erzeugte abelsche Gruppen

Eine Gruppe G heißt endlich erzeugt, falls $G = \langle E\rangle$ für eine endliche Teilmenge $E \subseteq G$ gilt. Jedes direkte Produkt von endlich vielen zyklischen Gruppen ist eine endlich erzeugte abelsche Gruppe (und umgekehrt, siehe 6.3).

[1] Warum 26? Für Kabbalisten: 26 ist der Zahlenwert des göttlichen Namens JHWH.

Die Gruppe $(\mathbb{R}, +)$ ist nicht endlich erzeugt (weil sie überabzählbar ist, vgl. 1.8), und $(\mathbb{Q}, +)$ auch nicht: endlich viele Brüche $b_1, \ldots, b_n$ haben einen Hauptnenner $N > 0$, und $\frac{1}{N+1} \notin \langle b_1, \ldots, b_n \rangle = \{\sum_{j=1}^{t} z_j b_j \mid z_j \in \mathbb{Z}\}$.

6.1 Lemma. *Für $a, b \in \mathbb{N}$ gilt $C_a \times C_b \cong C_{ab}$ genau dann, wenn a, b teilerfremd sind.*

Beweis. Sind a und b teilerfremd, so hat $(1, 1) \in C_a \times C_b$ die Ordnung ab (siehe 1.15); also ist $C_a \times C_b$ zyklisch und nach 3.8 isomorph zu C_{ab}.

Sind a und b nicht teilerfremd, so existiert eine Primzahl p, welche a und b teilt. Nach 1.12 hat dann $C_a \times C_b$ eine zu $C_p \times C_p$ isomorphe Untergruppe, aber C_{ab} hat keine solche Untergruppe. □

6.2 Lemma. *Sei $e_1, \ldots, e_k$ ein Erzeugendensystem der abelschen (additiv geschriebenen) Gruppe G. Ferner seien $n_1, \ldots, n_k \in \mathbb{N}_0$ mit dem grössten gemeinsamen Teiler $\mathrm{ggT}(n_1, \ldots, n_k) = 1$. Dann hat G auch ein Erzeugendensystem $f_1, \ldots, f_k$ mit $f_1 = \sum_{j=1}^{k} n_j e_j$.*

Beweis. Durch Induktion nach $s := \sum_{j=1}^{k} n_j$. Für $s = 1$ sind fast alle $n_j = 0$, nur ein $n_j = 1$, und es genügt, das gegebene Erzeugendensystem umzuordnen.

Sei jetzt $s > 1$. Dann sind mindestens zwei der n_j positiv [wegen ggT $= 1$], etwa $n_1 \geq n_2 > 0$. Die Gruppe G hat das Erzeugendensystem $e_1, e_1 + e_2, e_3, \ldots, e_k$, es gilt $\mathrm{ggT}(n_1 - n_2, n_2, n_3, \ldots, n_k) = 1$ und $(n_1 - n_2) + n_2 + n_3 + \cdots + n_k = s - n_2 < s$. Nach Induktion hat G ein Erzeugendensystem $f_1, \ldots, f_k$ mit $f_1 = (n_1 - n_2)e_1 + n_2(e_1 + e_2) + n_3 e_3 + \cdots + n_k e_k = n_1 e_1 + n_2 e_2 + \cdots + n_k e_k$. □

6.3 Satz. *Sei $k \in \mathbb{N}_0$ und G eine abelsche Gruppe, welche von k Elementen erzeugt wird. Dann ist G isomorph zu einem direkten Produkt von (höchstens) k zyklischen Gruppen.*

Beweis. Durch Induktion nach k. Die Behauptung gilt für $k \leq 1$. Sei jetzt $k > 1$ und $G = \langle e_1, \ldots, e_k \rangle$. Das Erzeugendensystem $e_1, \ldots, e_k$ sei so gewählt, dass $|\langle e_1 \rangle|$ möglichst klein ist. Wir setzen $U := \langle e_2, e_3, \ldots, e_k \rangle$ und schreiben G additiv (direkte Produkte werden dadurch zu direkten Summen). Es gilt $G = \langle e_1 \rangle + U$, und nach Induktion ist U eine direkte Summe von $k - 1$ zyklischen Gruppen. Wir behaupten, dass $G = \langle e_1 \rangle \oplus U$; daraus folgt die Behauptung.

Andernfalls ist $\langle e_1 \rangle \cap U \neq \{0\}$, also existieren $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ mit

$$\sum_{j=1}^{k} m_j e_j = 0 \quad \text{und} \quad m_1 e_1 \neq 0.$$

Man darf $m_j \in \mathbb{N}_0$ für alle j annehmen (ersetze manche e_j durch $-e_j$), ferner $m_1 < |\langle e_1 \rangle|$. Es gilt $d := \mathrm{ggT}(m_1, m_2, \ldots, m_k) > 0$ wegen $m_1 \neq 0$, und für die Zahlen $n_j := m_j/d$ ist $\mathrm{ggT}(n_1, \ldots, n_k) = 1$. Nach 6.2 hat G ein Erzeugendensystem $f_1, \ldots, f_k$ mit $f_1 = \sum_{j=1}^{k} n_j e_j$. Es gilt

$$d f_1 = \sum_j d n_j e_j = \sum_j m_j e_j = 0,$$

also $|\langle f_1 \rangle| \leq d \leq m_1 < |\langle e_1 \rangle|$. Das ist ein Widerspruch zur Wahl von $e_1, \ldots, e_k$. □

[Die Beweise zu 6.2 und 6.3 folgen Milne, Group theory, Version 2013]

6.4 Satz (Struktursatz für endlich erzeugte abelsche Gruppen)**.** *Jede endlich erzeugte abelsche Gruppe G ist isomorph zu einer Gruppe*

$$\mathbb{Z}^r \times C_{q_1} \times C_{q_2} \times \cdots \times C_{q_t}$$

mit $r \in \mathbb{N}_0$, $t \in \mathbb{N}_0$ und mit Primzahlpotenzen $q_1, \ldots, q_t$. Dabei sind r, t und die $q_j > 1$ (bis auf Umnummerierung der q_j) durch G eindeutig bestimmt.

Beweis. Nach 6.3 ist $G \cong \mathbb{Z}^r \times C_a \times C_b \times \cdots$ mit endlich vielen zyklischen Gruppen $C_a, C_b, \ldots$. Jede dieser endlichen zyklischen Gruppen ist nach 6.1 isomorph zu einem direkten Produkt von zyklischen Gruppen mit Primzahlpotenzordnungen. Daher hat G eine Zerlegung wie behauptet.

Zur Eindeutigkeit: In jeder (additiv geschriebenen) abelschen Gruppe G ist $G_{\text{endl}} = \{g \in G \mid \exists n \in \mathbb{N} : ng = 0\}$ eine Untergruppe (die sog. Torsionsuntergruppe von G). Für G wie in 6.4 ist $G_{\text{endl}} \cong C_{q_1} \times C_{q_2} \times \cdots \times C_{q_t}$ und $G/G_{\text{endl}} \cong \mathbb{Z}^r$.

Aus $\mathbb{Z}^r \cong \mathbb{Z}^s$ mit $r, s \in \mathbb{N}_0$ folgt $r = s$, denn: jeder Isomorphismus von $\mathbb{Z}^r$ auf $\mathbb{Z}^s$ bildet die Untergruppe $2\mathbb{Z}^r = (2\mathbb{Z})^r$ ab auf $2\mathbb{Z}^s = (2\mathbb{Z})^s$ und liefert daher einen Isomorphismus zwischen den Faktorgruppen $\mathbb{Z}^r/(2\mathbb{Z})^r \cong (\mathbb{Z}/2\mathbb{Z})^r \cong C_2^r$ und $\mathbb{Z}^s/(2\mathbb{Z})^s \cong (\mathbb{Z}/2\mathbb{Z})^s \cong C_2^s$ mit den Ordnungen 2^r bzw. 2^s.

Sei p eine beliebige Primzahl. Die (einzige) p-Sylowgruppe von $G_{\text{endl}} \cong C_{q_1} \times C_{q_2} \times C_{q_3} \times \cdots \times C_{q_t}$ ist isomorph zum direkten Produkt aller C_{q_j} mit p-Potenzordnung. Daher genügt es, im Spezialfall

$$G = \prod_{i=1}^{t} C_{p^{e_i}} \quad \text{mit } t \in \mathbb{N}_0 \text{ und } e_i \in \mathbb{N}$$

zu zeigen, dass t und die e_i (bis auf Umnummerierung) durch G eindeutig bestimmt sind. Für $e, k \in \mathbb{N}_0$ gilt

$$p^k C_{p^e} := \{p^k c \mid c \in C_{p^e}\} = \langle p^k \rangle \cong \begin{cases} C_{p^{e-k}} & \text{falls } e > k \\ \{0\} & \text{falls } e \le k \end{cases}$$

und daher

$$p^k C_{p^e} / p^{k+1} C_{p^e} = \begin{cases} C_p & \text{falls } e > k \\ \{0\} & \text{falls } e \le k. \end{cases}$$

Deshalb hat $p^k G/p^{k+1}G \cong \prod_{i=1}^{t} p^k C_{p^{e_i}}/p^{k+1}C_{p^{e_i}}$ die Ordnung $p^{a(k)}$, wobei $a(k)$ die Anzahl der Indices i mit $e_i > k$ ist, insbesondere $a(0) = t$. Die Gruppe G bestimmt die Folge $(a(k))_{k \in \mathbb{N}_0}$, und damit t und die e_i (bis auf Umnummerierung). □

6.5 Beispiel. Welche Isomorphietypen von abelschen Gruppen der Ordnung $200 = 2^3 5^2$ gibt es? Nach 6.4 muss man direkte Produkte der Gruppen $C_2, C_4, C_8, C_5, C_{25}$ betrachten; man erhält:

$$\begin{aligned} C_8 \times C_{25} &\cong C_{200} & \qquad C_8 \times C_5 \times C_5 \\ C_4 \times C_2 \times C_{25} & & C_4 \times C_2 \times C_5 \times C_5 \\ C_2 \times C_2 \times C_2 \times C_{25} & & C_2 \times C_2 \times C_2 \times C_5 \times C_5 \end{aligned}$$

Die Struktur der Sylowgruppen ergibt sich aus den additiven Zerlegungen der Exponenten $3 = 2 + 1 = 1 + 1 + 1$ und $2 = 1 + 1$.

Teil II.
RINGE

Ringe und Körper sind Mengen mit zwei algebraischen Verknüpfungen. Ein Leitmotiv der Ringtheorie ist die Untersuchung der gemeinsamen Eigenschaften von ganzen Zahlen und Polynomen.

7. Ringe und Körper

7.1 Definition. Ein (kommutativer) Ring ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$ mit folgenden Eigenschaften:

(i) $(R, +)$ ist eine abelsche Gruppe mit Neutralelement 0.

(ii) Die Multiplikation $\cdot$ ist assoziativ (und kommutativ), und es existiert ein Element $1 \in R$ mit $a \cdot 1 = a = 1 \cdot a$ für alle $a \in R$.

(iii) Die Distributivgesetze $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ gelten für alle $a, b, c \in R$.

Ist zusätzlich $R^* := R \setminus \{0\}$ bzgl. der Multiplikation eine Gruppe, so spricht man von einen Schiefkörper (Englisch: skew field), im kommutativen Fall von einem Körper (field). Statt $a \cdot b$ schreibt man ab, und statt $(R, +, \cdot)$ einfach R.

7.2 Beispiele. (a) $\mathbb{Z}$ ist ein kommutativer Ring, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.

(b) Ist R ein Ring, so ist die Menge

$$R[x] := \{ \textstyle\sum_{i=0}^{n} r_i x^i \mid n \in \mathbb{N}_0, r_i \in R \text{ für } 0 \leq i \leq n\}$$

aller Polynome mit Koeffizienten aus R ein Ring, der Polynomring über R in der Unbestimmten x (mit der üblichen Addition und Multiplikation von Polynomen); dieser Ring wird in 8.1 genauer definiert.

(c) Sind R und S Ringe, so ist auch das direkte Produkt $R \times S$ ein Ring mit den komponentweisen Verknüpfungen, d. h. mit den Definitionen $(r, s) + (r', s') := (r + r', s + s')$ und $(r, s)(r', s') := (rr', ss')$.

(d) Ist R ein Ring und $n \in \mathbb{N}$, so ist die Menge $R^{n\times n}$ aller $n \times n$-Matrizen mit Einträgen aus R ein Ring, mit der üblichen Addition und Multiplikation von Matrizen. Für $n \geq 2$ und $R \neq \{0\}$ ist $R^{n\times n}$ nicht kommutativ.

(e) Eine Boolesche Algebra ist ein Ring R mit $r^2 = r$ für jedes $r \in R$ (nach M. H. Stone 1935).

7.3 Einfache Folgerungen. In jedem Ring sind die Elemente 0 und 1 eindeutig bestimmt (siehe 1.1), und es gelten die folgenden drei Identitäten:
$a0 = 0a = 0$, wegen $a0 = a(0+0) = a0 + a0$);
$a(-b) = (-a)b = -(ab)$, wegen $0 = a0 = a(b + (-b)) = ab + a(-b)$ und $0 = 0b = (a + (-a))b = ab + (-a)b$;
$(-a)(-b) = ab$, wegen $(-a)(-b) = -(-(ab)) = ab$.

$R = \{0\}$ ist der einzige Ring mit $0 = 1$ (denn dies impliziert $a = a1 = a0 = 0$ für alle $a \in R$). Bei Körpern und Schiefkörpern ist $0 \neq 1$, weil die leere Menge keine Gruppe ist.

7.4 Definition. Für jeden Ring R ist die Menge

$$E(R) := \{r \in R \mid \exists s \in R : rs = 1 = sr\}$$

eine Gruppe bezüglich der Multiplikation, die sog. Einheitengruppe von R; ihre Elemente heißen Einheiten oder invertierbare Elemente von R.

Für Körper und Schiefkörper gilt $E(R) = R \setminus \{0\}$. Ferner ist $E(\mathbb{Z}) = \{1, -1\}$ und $E(\mathbb{R}^{n\times n}) = \mathrm{GL}_n(\mathbb{R})$.

7.5 Definition. Eine Teilmenge T eines Rings R heißt Teilring von R, falls $1 \in T$ und $t - t' \in T$ und $tt' \in T$ für alle $t, t' \in T$ gilt. Dann ist T mit den (eingeschränkten) Verknüpfungen von R ein Ring (wegen $0 = 1-1$ und $t+t' = t-t'(0-1)$). Ein Teilkörper ist ein Teilring, der ein Körper ist.

Beispiele: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Der Ring $\mathbb{Z} \times \{0\}$ ist kein Teilring von $\mathbb{Z} \times \mathbb{Z}$, wegen $(1, 0) \neq (1, 1)$.

Ist R ein Ring und $a \in R$, so ist $\{\sum_{k=0}^{n} z_k a^k \mid n \in \mathbb{N}_0, z_k \in \mathbb{Z}\}$ der kleinste Teilring von R, welcher a enthält (also der von a „erzeugte“ Teilring); dabei ist za und a^k für $z \in \mathbb{Z}$ und $k \in \mathbb{N}_0$ wie in 1.3 definiert. Dieser Teilring ist kommutativ.

7.6 Definition. Eine Abbildung $f : R \to R'$ zwischen Ringen R und R' heißt (Ring-) Homomorphismus, falls $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ für alle $a, b \in R$ und $f(1) = 1'$ gilt. (Die Gleichung $f(1) = 1'$ muss man extra verlangen, wie die Abbildung $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} : z \mapsto (z, 0)$ zeigt).

Ring-Mono-/Epi-/Iso-/Endo-/Auto-morphismen sind dann wie in 2.1 definiert. Zwei Ringe R und R' heißen isomorph (als Ringe), im Zeichen $R \cong R'$, falls ein Ringisomorphismus $f : R \to R'$ existiert.

Beispiel: $\mathbb{C}$ ist isomorph zu dem Teilkörper $\left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix} \right) \mid a, b \in \mathbb{R} \right\}$ von $\mathbb{R}^{2\times 2}$.

7.7 Definition. Ein Element $a \neq 0$ eines Rings R heißt Nullteiler, falls ein $b \in R \setminus \{0\}$ existiert mit $ab = 0$ oder $ba = 0$. Wenn R keine Nullteiler enthält und $R \neq \{0\}$ gilt, heißt R nullteilerfrei. Ein nullteilerfreier, kommutativer Ring wird als Integritätsring (oder Integritätsbereich, Engl. integral domain) bezeichnet.

Beispiele: Matrizenringe und direkte Produkte von Ringen enthalten typischerweise Nullteiler, wegen $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix} \right)^2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix} \right)$ und $(1, 0)(0, 1) = (0, 0)$. Jeder Körper ist ein Integritätsring, ebenso jeder Teilring eines Körpers (etwa $\mathbb{Z} \subseteq \mathbb{Q}$).

Ist $a \in R \setminus \{0\}$ kein Nullteiler, so darf man in R „durch a kürzen“, d. h. für $b, c \in R$ gilt $ab = ac \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$.

Welche Ringe sind Teilringe von Körpern? Die folgende Konstruktion zeigt, dass dies genau die Integritätsringe sind.

7.8 Definition (Quotientenkörper)**.** Sei R ein Integritätsring. Wir definieren auf der Menge $R \times (R \setminus \{0\})$ eine Äquivalenzrelation $\sim$ (nachrechnen) durch

$$(r, s) \sim (r', s') \Leftrightarrow rs' = r's.$$

Sei $\frac{r}{s}$ die Äquivalenzklasse von (r, s) und $Q(R) := \{\frac{r}{s} \mid r, s \in R, s \neq 0\}$ die Menge aller Äquivalenzklassen. Die Verknüpfungen

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'} \quad \text{und} \quad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

sind wohldefiniert (nachrechnen) und machen $Q(R)$ zu einem kommutativen Ring mit dem Nullelement $\frac{0}{1}$ und dem Einselement $\frac{1}{1}$. Wegen $\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = \frac{1}{1}$ für $r, s \neq 0$ ist $Q(R)$ ein Körper.

Ferner ist $R \to Q(R) : r \mapsto \frac{r}{1}$ ein Monomorphismus von Ringen. Daher kann man R als Teilring von $Q(R)$ betrachten. Man nennt $Q(R)$ den Quotientenkörper von R.

Beispiele: $\mathbb{Z}$ und $\mathbb{Z}[\frac{1}{2}] := \{\frac{z}{2^k} \mid z \in \mathbb{Z}, k \in \mathbb{N}_0\}$ haben beide den Quotientenkörper $\mathbb{Q}$. Der Polynomring $\mathbb{Q}[x]$ hat den Quotientenkörper $\mathbb{Q}(x) := \{\frac{f}{g} \mid f, g \in \mathbb{Q}[x], g \neq 0\}$, der auch als „Körper der rationalen Funktionen“ über $\mathbb{Q}$ bezeichnet wird.

8. Polynome

8.1 Definition (Potenzreihen und Polynome)**.** Sei R ein Ring. Die Menge $R^{\mathbb{N}_0} = \{(a_i)_{i\geq 0} \mid a_i \in R\}$ aller Folgen in R ist mit der komponentenweisen Addition $+$ eine abelsche Gruppe. Die Multiplikation (Faltung)

$$(a_i)_{i\geq 0} \cdot (b_i)_{i\geq 0} = (c_i)_{i\geq 0} \text{ mit } c_i := \textstyle\sum_{j=0}^{i} a_j b_{i-j} \text{ für } i \in \mathbb{N}_0$$

macht $R^{\mathbb{N}_0}$ zu einem Ring (nachrechnen) mit dem Einselement $(1, 0, 0, \dots)$. Die Abbildung $R \to R^{\mathbb{N}_0} : r \mapsto (r, 0, 0, \dots)$ ist ein Ring-Monomorphismus. Man identifiziert r mit $(r, 0, 0, \dots)$; dann gilt $r \cdot (a_i)_{i\geq 0} = (ra_i)_{i\geq 0}$ für $r, a_i \in R$.

Ferner ist $R^{(\mathbb{N}_0)} := \{(a_i)_{i\geq 0} \mid a_i \in R \text{ und } a_i \neq 0 \text{ nur für endlich viele } i\}$ ein Teilring dieses Rings $R^{\mathbb{N}_0}$.

Übliche Notation: Für $x := (0, 1, 0, 0, \dots) \in R^{\mathbb{N}_0}$ und $n \in \mathbb{N}_0$ gilt

$$x^n = (\underbrace{0, 0, \dots, 0}_{n \text{ Nullen}}, 1, 0, 0, \dots),$$

wie man per Induktion zeigt. Daher hat jedes Element $p \in R^{(\mathbb{N}_0)}$ die Form

$$p = \sum_{i=0}^{n} a_i x^i \quad \text{mit } n \in \mathbb{N}_0 \text{ und } a_i \in R.$$

Im Fall $p \neq 0$ kann man zusätzlich $a_n \neq 0$ verlangen; dann sind n und $a_0, a_1, \ldots, a_n$ eindeutig bestimmt. Man nennt $n = \mathrm{Grad}(p)$ den Grad von p, die a_i heißen Koeffizienten von p, und a_n ist der Leitkoeffizient von p. Ferner nennt man p normiert, wenn sein Leitkoeffizient 1 ist. Wir setzen $\mathrm{Grad}(0) := -\infty$.

Der Ring $R[x] := \big(R^{(\mathbb{N}_0)}, +, \cdot\big)$ wird als Polynomring über R in der „Variablen“ x bezeichnet. Der größere Ring $R[[x]] := \big(R^{\mathbb{N}_0}, +, \cdot\big)$ wird als Ring der formalen Potenzreihen über R bezeichnet; man schreibt statt $(a_i)_{i\geq 0}$ auch $\sum_{i\geq 0} a_i x^i$. Mit R ist auch $R[[x]]$ kommutativ.

8.2 Lemma. *Sei R ein nullteilerfreier Ring und $f, g \in R[x]$.*

(a) *Es gilt* $\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$.

(b) *Der Polynomring $R[x]$ ist nullteilerfrei.*

(c) *Ist g normiert, so existieren eindeutig bestimmte Polynome $q, r \in R[x]$ mit $f = g \cdot q + r$ und* $\mathrm{Grad}(r) < \mathrm{Grad}(g)$. (*Division mit Rest*)

Beweis. (a) Für $f = 0$ oder $g = 0$ gilt die Gradformel per Konvention.
Ist $f = a_0 + a_1 x + \cdots + a_n x^n$ und $g = b_0 + b_1 x + \cdots + b_m x^m$ mit $a_n \neq 0 \neq b_m$, so folgt $fg = a_n b_m x^{n+m} + h$ mit $\mathrm{Grad}(h) < n + m$. Wegen der Nullteilerfreiheit von R ist $a_n b_m \neq 0$, also $\mathrm{Grad}(fg) = n + m = \mathrm{Grad}(f) + \mathrm{Grad}(g)$.
(b) folgt aus (a).
(c) Wähle $q \in R[x]$ so, dass $\mathrm{Grad}(f - g \cdot q)$ möglichst klein ist (Wohlordnung der natürlichen Zahlen). Schreibe $f - g \cdot q = a_0 + a_1 x + \cdots + a_n x^n$ mit $a_i \in R$. Wäre $n \geq \mathrm{Grad}(g)$, so folgte

$$\mathrm{Grad}\left(f - g \cdot q - a_n \cdot g \cdot x^{n-\mathrm{Grad}(g)}\right) < n,$$

ein Widerspruch zur Wahl von q. Daher gilt für $r := f - g \cdot q$ die Ungleichung $\mathrm{Grad}(r) < \mathrm{Grad}(g)$, und $f = g \cdot q + r$.
Eindeutigkeit: $f = g \cdot q + r = g \cdot \tilde{q} + \tilde{r} \Rightarrow g \cdot (q - \tilde{q}) = \tilde{r} - r \overset{(a)}{\Rightarrow} \mathrm{Grad}(g) + \mathrm{Grad}(q - \tilde{q}) = \mathrm{Grad}(r - \tilde{r}) < \mathrm{Grad}(g) \Rightarrow \mathrm{Grad}(q - \tilde{q}) < 0 \Rightarrow q - \tilde{q} = 0 \Rightarrow q = \tilde{q} \Rightarrow r = \tilde{r}$. □

Beispiel für eine Division mit Rest in $\mathbb{Z}[x]$, mit $f = x^4 + x$ und $g = x^2 + 1$:

$$\begin{array}{r} \big(\quad x^4 \qquad + x\big) \div \big(x^2 + 1\big) = x^2 - 1 + \dfrac{x+1}{x^2+1} \\ \underline{-\,x^4 - x^2} \\ -\,x^2 + x \\ \underline{\quad x^2 \qquad + 1} \\ x + 1 \end{array}$$

Also gilt $\underbrace{(x^4 + x)}_{f} = \underbrace{(x^2 + 1)}_{g}\underbrace{(x^2 - 1)}_{q} + \underbrace{(x + 1)}_{r}$.

8.3 Definition (Einsetzen in Polynome)**.** Sei R ein Ring und $r \in R$. Für $p = \sum_{i=0}^{n} a_i x^i \in R[x]$ definieren wir

$$p(r) := \sum_{i=0}^{n} a_i r^i \in R.$$

Die Abbildung $e_r : R[x] \to R : p \mapsto p(r)$, die Auswertung bei r oder das Einsetzen von r, ist ein Ringhomomorphismus, falls $r \in Z(R) := \{a \in R \mid ab = ba \text{ für alle } b \in R\}$ (diese Bedingung an r ist nötig wegen $e_r(x \cdot bx^0) = e_r(bx) = br$ und $e_r(x) \cdot e_r(bx^0) = rb$ für jedes $b \in R$).

Ist $p(r) = 0$, so sagt man: r ist eine Nullstelle von p (oder: r wird von p annulliert).

8.4 Lemma. *Sei R ein kommutativer Ring und $p \in R[x]$.*

(i) *Ist $a \in R$ eine Nullstelle von p, so existiert ein $q \in R[x]$ mit $p = (x - a) \cdot q$.*

(ii) *Ist R ein Integritätsring (etwa ein Körper), so hat jedes Polynom $p \in R[x]$ mit $p \neq 0$ höchstens* $\mathrm{Grad}(p)$ *viele Nullstellen in R.*

Beweis. (i) Nach 8.2(c) existieren $q, r \in R[x]$ mit $p = (x - a) \cdot q + r$ und $\mathrm{Grad}(r) < \mathrm{Grad}(x - a) = 1$ (falls $R \neq \{0\}$, aber die Behauptung ist trivial für $R = \{0\}$). Also ist $r = a_0 x^0$ mit $a_0 \in R$. Einsetzen von a liefert $0 = p(a) = (a - a) \cdot q(a) + r(a) = a_0$, also $r = 0$.

(ii) Wir benutzen Induktion nach $\mathrm{Grad}(p)$; die Behauptung gilt für $\mathrm{Grad}(p) \leq 1$. Sei a eine Nullstelle von p und $p = (x - a) \cdot q$ gemäß (i). Jede von a verschiedene Nullstelle b von p erfüllt $0 = p(b) = (b - a) \cdot q(b)$, also $q(b) = 0$ wegen der Nullteilerfreiheit. Nach 8.2(a) ist $\mathrm{Grad}(q) = \mathrm{Grad}(p) - 1$, und per Induktion hat q höchstens $\mathrm{Grad}(p) - 1$ viele Nullstellen in R. □

8.5 Satz. *Sei R ein Integritätsring. Dann ist jede endliche Untergruppe G der Einheitengruppe $E(R)$ zyklisch. Insbesondere ist die multiplikative Gruppe jedes endlichen Körpers zyklisch.*

Erster Beweis. Ist die abelsche Gruppe G nicht zyklisch, so enthält G wegen 6.4 und 6.1 eine zu $C_p \times C_p$ isomorphe Untergruppe für eine Primzahl p. Die p^2 Elemente dieser Untergruppe sind Nullstellen von $x^p - 1$, im Widerspruch zu 8.4(ii). □

Zweiter Beweis. (Gauß, ohne 6.4) Sei $|G| = n$ und $\psi(d) := |\{g \in G \mid g \text{ hat Ordnung } d\}|$ für jeden Teiler d von n. Hat $g \in G$ die Ordnung d, so ist $\langle g \rangle \cong C_d$ nach 8.4(ii) die Menge aller Nullstellen von $x^d - 1$ in R; daher enthält G dann genau $\varphi(d)$ Elemente der Ordnung d (vgl. 1.16). Also gilt $\psi(d) \in \{0, \varphi(d)\}$ für jeden Teiler d von n. Es folgt

$$\sum_{d \text{ teilt } n} \psi(d) = |G| = n = \sum_{d \text{ teilt } n} \varphi(d),$$

siehe 1.17, also $\psi(d) = \varphi(d)$ für alle Teiler d von n. Insbesondere ist $\psi(n) = \varphi(n) > 0$, also ist G zyklisch. □

8.6 Bemerkung (Polynomfunktionen)**.** Sei R ein kommutativer Ring. Jedes $p \in R[x]$ liefert eine Polynomfunktion $\bar{p} : R \to R$, die durch $\bar{p}(r) := p(r)$ definiert ist; vgl. 8.3. Die Abbildung $^-$ ist ein Ringhomomorphismus von $R[x]$ in den Ring R^R aller Abbildungen von R in sich (mit den punktweisen Verknüpfungen, wie in der Analysis).

Ist der Ring R unendlich und nullteilerfrei (etwa $R = \mathbb{Z}$ oder $R = \mathbb{R}$), so ist $\ker(^-) = \{p \in R[x] \mid \forall r \in R : p(r) = 0\} = \{0\}$ nach 8.4(ii). Demnach ist $^-$ injektiv, und man kann (wenn man will) das Polynom p mit der Polynomfunktion $\bar{p}$ identifizieren.

Ist R endlich, so existieren Polynome $p \neq 0$ mit $\bar{p} = 0$, etwa $p = \prod_{r \in R}(x - r)$, und man muss Polynome und Polynomfunktionen unterscheiden. Konkret: $R = \mathbb{F}_2 = \{0, 1\}$ und $p = x(x-1) = x^2 - x$.

9. Kreisteilungspolynome und ein Satz von Wedderburn

9.1 Definition. Für $n \in \mathbb{N}$ ist das n-te Kreisteilungspolynom (Engl. cyclotomic polynomial) definiert durch

$$\Phi_n := \prod_{\substack{c \in \mathbb{C}^* \text{ hat} \\ \text{Ordnung } n}} (x - c) = \prod_{\substack{1 \le k \le n \\ k,n \text{ teilerfremd}}} (x - e^{2\pi i k/n}).$$

Es hat den Grad $\varphi(n)$. Wegen

$$x^n - 1 = \prod_{\substack{c \in \mathbb{C}^* \\ c^n = 1}} (x - c) = \prod_{1 \le k \le n} (x - e^{2\pi i k/n}) = \prod_{d \text{ teilt } n} \Phi_d,$$

gilt

$$\Phi_n = \frac{x^n - 1}{\prod\limits_{\substack{d \text{ teilt } n \\ d \neq n}} \Phi_d}.$$

Mit dieser Rekursionsgleichung kann man die Φ_n berechnen, etwa

$$\Phi_1 = x - 1, \quad \Phi_2 = \frac{x^2 - 1}{\Phi_1} = x + 1, \quad \Phi_4 = \frac{x^4 - 1}{\Phi_1 \cdot \Phi_2} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1 = (x - i)(x + i).$$

Aus dieser Rekursionsgleichung folgt auch $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$ (per Induktion, weil alle Φ_n normiert sind; vgl. 8.2(c)).

9.2 Satz (Wedderburn 1905)**.** *Endliche Schiefkörper sind kommutativ.*

Beweis. (Witt 1931) Sei S ein endlicher Schiefkörper. Das Zentrum $Z := Z(S)$ ist ein Teilkörper von S. Wegen $0, 1 \in Z$ ist $q := |Z| \geq 2$. Ferner ist S ein Z-Vektorraum. Mit $n := \dim_Z S$ gilt also $|S| = q^n$.

Wir werden $n = 1$ zeigen (dann folgt $S = Z$, also die Behauptung).

Die Klassengleichung (2.10) für $S^* = S \setminus \{0\}$ lautet

$$q^n - 1 = |S^*| = q - 1 + \sum_i |S^* : \mathrm{C}_{S^*}(s_i)|$$

mit geeigneten Elementen $s_i \in S \setminus Z$. Jeder Zentralisator $\mathrm{C}_S(s_i)$ ist ein Teilring von S und enthält Z. Daher ist $\mathrm{C}_S(s_i)$ ein Z-Vektorraum, also

$$|\,\mathrm{C}_S(s_i)| = q^{n_i}$$

mit $n_i = \dim_Z \mathrm{C}_S(s_i)$. Wegen $s_i \notin Z$ ist $n_i < n$.

Ferner ist $\mathrm{C}_{S^*}(s_i)$ eine Untergruppe von S^*, also $q^{n_i} - 1$ ein Teiler von $q^n - 1$ nach 1.6. Dies impliziert, dass n_i ein Teiler von n ist (denn: schreibe $n = n_i \cdot a + b$ mit $0 \le b < n_i$, dann ist $q^{n_i} - 1$ ein Teiler von $q^n - 1 = ((q^{n_i})^a - 1)q^b + q^b - 1$, also auch ein Teiler von $q^b - 1 < q^{n_i} - 1$; es folgt $q^b - 1 = 0$, also $b = 0$). Wir erhalten

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{n_i} - 1}.$$

Es gilt $q^n - 1 = \prod_{d \text{ teilt } n} \Phi_d(q)$ und $q^{n_i} - 1 = \prod_{d \text{ teilt } n_i} \Phi_d(q)$. Wegen $n_i < n$ ist die ganze Zahl $\Phi_n(q)$ ein Teiler von $q^n - 1$ und von jedem Summanden $\frac{q^n-1}{q^{n_i}-1}$, also auch ein Teiler von $q - 1$. Insbesondere folgt $|\Phi_n(q)| \le q - 1$.

Für $n \ge 2$ gilt (Bild malen)

$$|\Phi_n(q)| = \prod_{\substack{c \in \mathbb{C}^* \text{ hat} \\ \text{Ordnung } n}} |q - c| > q - 1.$$

Daher ist $n = 1$, also $S = Z$. □

[Komplexe Zahlen lassen sich beim Beweis von 9.2 vermeiden, siehe Meixner, Eine Bemerkung zu den Kreisteilungspolynomen, Math. Semesterberichte 36 (1989) 125–138.]

9.3 Korollar. *Jeder endliche, nullteilerfreie Ring ist ein Körper.*

Beweis. In jedem solchen Ring R gilt $0 \ne 1$. Ist $0 \ne a \in R$, so sind die beiden Abbildungen $R \to R : r \mapsto ar$ und $R \to R : r \mapsto ra$ injektiv (vgl. 7.7), also surjektiv wegen der Endlichkeit. Demnach existieren $b, b' \in R$ mit $ab = 1 = b'a$. Es folgt $b' = b'1 = b'ab = 1b = b$. Also ist $R \setminus \{0\}$ eine Gruppe, d. h. R ist ein Schiefkörper. Nach 9.2 ist R kommutativ. □

10. Ideale und Faktorringe

10.1 Definition. Eine additive Untergruppe I eines Ringes R heißt Ideal von R, falls für alle $i \in I$, $r \in R$ gilt: $ri \in I$ und $ir \in I$ (also $RI \subseteq I$ und $IR \subseteq I$). Man schreibt dann $I \trianglelefteq R$.

Beispiele: $\{0\} \trianglelefteq R$ und $R \trianglelefteq R$. Ist $f : R \to S$ ein Homomorphismus zwischen Ringen R und S, so ist $\ker f = f^{-1}(0)$ ein Ideal von R, denn: $\ker f$ ist eine additive Untergruppe von $(R, +)$ nach 2.3, und $i \in \ker f$, $r \in R \Rightarrow f(i) = 0 \Rightarrow f(ri) = f(r)f(i) = f(r) \cdot 0 = 0$ nach 7.3; analog folgt $f(ir) = 0$.

Ist R ein kommutativer Ring und $a \in R$, so ist $I = aR$ ein Ideal von R; man nennt aR das von a erzeugte Hauptideal (Engl. principal ideal). Insbesondere ist $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$ für jedes $n \in \mathbb{Z}$.

Aus $1 \in I \trianglelefteq R$ folgt $I = R$.

Ist R ein Körper oder Schiefkörper, so sind $\{0\}$ und R die einzigen Ideale von R. Daher sind alle Ring-Homomorphismen zwischen Körpern injektiv.

10.2 Definition (Faktorringe)**.** Sei R ein Ring und $I \trianglelefteq R$. Nach 3.4 ist

$$R/I := \{r + I \mid r \in R\}$$

eine abelsche Gruppe mit der Addition

$$(r + I) + (s + I) := r + s + I \text{ für } r, s \in R.$$

Wir definieren eine Multiplikation auf R/I durch

$$(r + I) \cdot (s + I) := rs + I \text{ für } r, s \in R;$$

diese Multiplikation ist wohldefiniert: aus $r+I = r'+I,\ s+I = s'+I$ folgt $r-r', s-s' \in I$ und dann $rs - r's' = (r - r')s + r'(s - s') \in Is + r'I \subseteq I + I \subseteq I$, also $rs + I = r's' + I$ für alle $r, s, r', s' \in R$.

Die kanonische Projektion $p : R \to R/I : r \mapsto r + I$ ist additiv und hat den Kern I, siehe 3.5. Nach Definition der Multiplikation ist p auch multiplikativ. Daher ist R/I mit diesen Verknüpfungen ein Ring, der Faktorring (oder Quotient) von R modulo I, und $p : R \to R/I$ ist ein Ringepimorphismus mit Kern I. (Demnach sind die Ideale genau die Kerne von Ringhomomorphismen.)

Es gilt $R/\{0\} \cong R$ und $R/R \cong \{0\}$.

10.3 Satz (Homomorphiesatz)**.** *Sei $f : R \to S$ ein Homomorphismus zwischen Ringen R und S. Dann gilt $R/\ker f \cong f(R)$.*

Beweis. Die Abbildung $r + \ker f \mapsto f(r)$ ist ein wohldefinierter Isomorphismus zwischen den additiven Gruppen von $R/\ker f$ und $f(R)$, siehe Beweis zu 3.7. Nach 10.2 ist diese Abbildung auch multiplikativ, und $1 + \ker f \mapsto f(1) = 1$. □

10.4 Satz. *Sei R ein kommutativer Ring und $I \trianglelefteq R$. Genau dann ist R/I ein Körper, wenn I ein maximales Ideal von R ist (d. h. aus $I \neq R$ und $I \subseteq J \trianglelefteq R$ folgt $J = I$ oder $J = R$).*

Beweis. Sei I maximal und $a + I \in R/I$ nicht das Nullelement, also $a \in R \setminus I$. Weil R kommutativ ist, ist $J := aR + I$ ein Ideal von R, und $J \neq I$ wegen $a \in J$. Wegen der

Maximalität von I ist $J = R$; insbesondere existieren $b \in R$ und $i \in I$ mit $ab + i = 1$. Es folgt $(a + I)(b + I) = ab + I = 1 + I$, also ist $b + I$ invers zu $a + I$ in R/I.

Sei jetzt I nicht maximal und J ein Ideal echt zwischen I und R. Für $a \in J \setminus I$ und für alle $r \in R$ gilt dann $(a+I)(r+I) = ar + I \subseteq J + I \subseteq J$, also $1 \notin (a+I)(r+I)$ und daher ist $a + I \neq 0 + I$ in R/I keine Einheit. □

10.5 Bemerkung. (Was sind die reellen Zahlen, für Algebraiker?)
Die rationalen Cauchyfolgen bilden mit den komponentenweisen Verknüpfungen einen kommutativen Ring C. Die Menge N aller rationalen Nullfolgen ist ein maximales Ideal von C (Übung).

Wenn man $\mathbb{R}$ schon kennt, stellt man fest: die Grenzwertbildung $\lim_{n\to\infty} : C \to \mathbb{R}$ ist ein Ringepimorphismus mit Kern N, also gilt $C/N \cong \mathbb{R}$ nach 10.3. Will man den Körper $\mathbb{R}$ der reellen Zahlen aus $\mathbb{Q}$ konstruieren, kann man $\mathbb{R} := C/N$ definieren.

10.6 Definition (Restklassenringe)**.** Für jedes $n \in \mathbb{N}$ ist

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$$

ein kommutativer Ring mit $|\mathbb{Z}_n| = n$, der Ring der Restklassen modulo n. Die additive Gruppe von $\mathbb{Z}_n$ ist die zyklische Gruppe C_n, siehe 3.8. Mit der kanonischen Projektion $^- : \mathbb{Z} \to \mathbb{Z}_n : a \mapsto \bar{a} := a + n\mathbb{Z}$ gilt

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\},$$

und die Verknüpfungen von $\mathbb{Z}_n$ sind durch $\bar{a} + \bar{b} = \overline{a+b}$ und $\bar{a}\bar{b} = \overline{ab}$ für $a, b \in \mathbb{Z}$ definiert. Man schreibt $a \equiv b \mod n$, falls $\bar{a} = \bar{b}$ in $\mathbb{Z}_n$, d. h. falls n ein Teiler von $a - b$ ist, für $a, b \in \mathbb{Z}$.

[9er Probe, 11er Probe als Ring-Homomorphismen, $10 \equiv 1 \bmod 9$, $10 \equiv -1 \bmod 1$]

10.7 Satz. *Der Ring $\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. 10.4 und 1.12, 1.13. □

Für Primzahlen p schreibt man auch $\mathbb{F}_p := \mathrm{GF}(p) := \mathbb{Z}_p$. Es gibt weitere endliche Körper, etwa $\{0, 1, a, a+1\}$ mit $1 + 1 = 0$ und $a^2 = a + 1$; vgl. 16.5. Der Ring $\mathbb{Z}_4$ hat Nullteiler: $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$.

10.8 Bemerkung (Einheiten von $\mathbb{Z}_n$)**.** Es gilt

$$\begin{aligned} E(\mathbb{Z}_n) &= \{\bar{a} \in \mathbb{Z}_n \mid \exists b \in \mathbb{Z} : \bar{a}\bar{b} = \bar{1}\} = \{\bar{a} \in \mathbb{Z}_n \mid \exists b, z \in \mathbb{Z} : ab = 1 + nz\} \\ &\overset{1.14}{=} \{\bar{a} \in \mathbb{Z}_n \mid a, n \text{ sind teilerfremd}\}, \end{aligned}$$

also $|E(\mathbb{Z}_n)| = \varphi(n)$ nach 1.16. Mit ÜA 7 folgt auch $E(\mathbb{Z}_n) \cong \mathrm{Aut}\, C_n$.

Nach dem Satz von Lagrange (1.6) ist die multiplikative Ordnung von $\bar{a} \in E(\mathbb{Z}_n)$ ein Teiler von $\varphi(n)$; also gilt $\bar{a}^{\varphi(n)} = \bar{1}$, d. h. $a^{\varphi(n)} \equiv 1 \mod n$, falls a und n teilerfremd sind (*Satz von Fermat–Euler*). Ist $n = p$ eine Primzahl, so gilt $\varphi(p) = p - 1$, und man erhält $a^p \equiv a \mod p$ für alle $a \in \mathbb{Z}$ (*kleiner Satz von Fermat*).

10.9 Satz (Chinesischer Restsatz)**.** *Sei $n = n_1 n_2 \cdots n_t$ mit paarweise teilerfremden natürlichen Zahlen n_i. Dann ist die Abbildung*

$$g : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t} : a + n\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \ldots, a + n_t\mathbb{Z})$$

ein Ring-Isomorphismus.

Beweis. Die Abbildung

$$f : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t} : a \mapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \ldots, a + n_t\mathbb{Z})$$

ist ein Ring-Homomorphismus (simultane Anwendung von kanonischen Projektionen). Es gilt $\ker f = n_1\mathbb{Z} \cap n_2\mathbb{Z} \cap \cdots \cap n_t\mathbb{Z} = n\mathbb{Z}$, weil die n_i paarweise teilerfremd sind. Nach 10.3 (mit Beweis) ist $g : \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \to g(\mathbb{Z}_n)$ ein Ring-Isomorphisms. Wegen $|g(\mathbb{Z}_n)| = |\mathbb{Z}_n| = n = |\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}|$ ist $g(\mathbb{Z}_n) = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}$. □

10.10 Korollar (Naiver Chinesischer Restsatz)**.** *Seien $n_1, n_2, \ldots, n_t$ paarweise teilerfremde natürliche Zahlen und $r_1, r_2, \ldots, r_t \in \mathbb{Z}$. Dann existiert eine Zahl $a \in \mathbb{Z}$ mit $a \equiv r_i \bmod n_i$ für $1 \leq i \leq t$.*

Beweis. Das ist die Surjektivität der Abbildung g aus 10.9. □

Ein chinesisches Manuskript aus dem 3. Jahrhundert fragt nach einer Zahl a mit $a \equiv 2 \bmod 3$, $a \equiv 3 \bmod 5$ und $a \equiv 2 \bmod 7$. Die kleinste positive Lösung ist $a = 23$ (die zweitkleinste $a = 23 + 3 \cdot 5 \cdot 7 = 128$).

10.11 Korollar. *Für teilerfremde $a, b \in \mathbb{N}$ gilt $\varphi(ab) = \varphi(a)\varphi(b)$.*

Beweis. Wegen 10.8 und 10.9 gilt $\varphi(ab) = |E(\mathbb{Z}_{ab})| = |E(\mathbb{Z}_a \times \mathbb{Z}_b)| = |E(\mathbb{Z}_a) \times E(\mathbb{Z}_b)| = |E(\mathbb{Z}_a)| \cdot |E(\mathbb{Z}_b)| = \varphi(a) \cdot \varphi(b)$. □

Ist p eine Primzahl und $n \in \mathbb{N}$, so gilt $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$, weil die nicht zu p^n teilerfremden Zahlen genau die Vielfachen von p sind. Damit und mit 10.11 kann man $\varphi(a)$ berechnen, wenn man die Primfaktorzerlegung von a kennt.

10.12 Bemerkung (Restklassenringe in der Kryptographie)**.** Grundproblem der Kryptographie: ein Sender S möchte eine Nachricht an einen Empfänger E schicken, die so verschlüsselt ist, dass ein Angreifer X sie nicht (oder nur mit großem Aufwand) entschlüsseln kann. Bei der public-key-Kryptographie ist dabei das Verschlüsselungsverfahren und der Schlüssel zum Verschlüsseln öffentlich bekannt.

RSA-Verfahren (nach Rivest, Shamir, Adleman 1977; eigentlich schon Clifford Cocks 1973): Der Empfänger E wählt zwei verschiedene, große Primzahlen p und q und setzt $n = p \cdot q$. Ferner wählt E eine natürliche Zahl $s \leq \varphi(n) = (p-1)(q-1)$, welche teilerfremd zu $\varphi(n)$ ist, und berechnet ein $t \in \mathbb{N}$ mit $st \equiv 1 \bmod \varphi(n)$; ein solches t existiert nach dem Lemma von Bezout 1.14. Das Paar (n, s) wird veröffentlicht, aber p, q, t bleiben geheim (E kann p und q nach Berechnung von t löschen).

Der Sender S möchte eine Nachricht $a \in \mathbb{Z}_n$ an E schicken. Dazu berechnet er $a^s \in \mathbb{Z}_n$ und schickt a^s an E.

Der Empfänger E kennt t, erhält a^s und berechnet daraus $(a^s)^t = a^{st}$. In $\mathbb{Z}_n$ gilt $a^{st} = a$ für alle $a \in \mathbb{Z}_n$, daher hat E die Nachricht entschlüsselt. (Beweis: wegen $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$ genügt es, die Gleichung $a^{st} = a$ in $\mathbb{Z}_p$ und $\mathbb{Z}_q$ nachzuweisen. Diese gilt für $a = \bar{0}$, und für $\bar{0} \neq a \in \mathbb{Z}_p$ ist $a^{p-1} = \bar{1}$ nach 10.8. Ferner ist $p-1$ ein Teiler von $\varphi(n)$, also auch ein Teiler von $st-1$. Damit folgt $a^{st-1} = \bar{1}$, also $a^{st} = a$.)

Ein Angreifer X kennt n, s, a^s und will hieraus a berechnen. Alle heute dafür bekannten Verfahren erfordern die Berechnung von t und von $\varphi(n)$. Wegen $n = pq$ und $\varphi(n) = n-p-q+1$ ist die Bestimmung von $\varphi(n)$ äquivalent zur Bestimmung von p und q, also zur Faktorisierung von n. Die Sicherheit des RSA-Verfahren beruht darauf, dass man kein effektives Verfahren kennt, um große Zahlen n (etwa $n > 10^{150}$) zu faktorisieren.
Literatur: Salomaa, Public-Key Cryptography, Springer 1996.
Katz, Lindell, Introduction to Modern Cryptography, CRC Press 2007.

11. Euklidische und faktorielle Ringe

Welche Ringe gestatten ein Analogon zur Primfaktorzerlegung? (Wir betrachten nur kommutative Ringe ohne Nullteiler, denn aus $ab = 0$ folgt $ac = a(b+c)$ für jedes c).

11.1 Definition. Sei R ein Integritätsring.
R heißt Hauptidealring, falls jedes Ideal von R ein Hauptideal ist.
R heißt euklidisch, wenn eine Abbildung $\gamma : R \setminus \{0\} \to \mathbb{N}_0$ existiert mit

(i) $\gamma(a) \leq \gamma(ab)$ für alle $a, b \in R \setminus \{0\}$;

(ii) zu $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit $a = bq + r$, wobei $r = 0$ oder $\gamma(r) < \gamma(b)$. (Division mit Rest)

Die Eigenschaft (i), die nicht immer verlangt wird, ist harmlos in folgendem Sinn: gilt (ii) für γ, so wird durch $\gamma'(a) = \min\{\gamma(ab) \mid 0 \neq b \in R\}$ eine Abbildung γ' definiert, welche (i) und (ii) erfüllt; vgl. etwa Lüneburg, Zahlentheorie, Oldenbourg 2010.

Beispiele: $\mathbb{Z}$ ist ein Hauptidealring (1.12) und euklidisch mit $\gamma(z) = |z|$. Für jeden Körper K ist der Polynomring $K[x]$ euklidisch mit $\gamma = \text{Grad}$, siehe 8.2. Der Ring $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ ist euklidisch, mit $\gamma(a+ib) = (a+ib)(a-ib) = a^2 + b^2$ (Übung).

11.2 Satz. *Jeder euklidische Ring R ist ein Hauptidealring. Insbesondere ist $K[x]$ ein Hauptidealring für jeden Körper K.*

Beweis. (Vgl. den Beweis zu 1.12) Es gilt $\{0\} = 0R$. Sei $I \neq \{0\}$ ein Ideal von R, und $b \in I \setminus \{0\}$ sei so gewählt, dass $\gamma(b)$ minimal ist. Wegen $b \in I$ gilt $bR \subseteq I$. Für die andere Inklusion schreibe $a \in I$ in der Form $a = bq + r$ wie in 11.1. Der Fall $r \neq 0$ führt auf einen Widerspruch, wegen $r = a - bq \in I$ und $\gamma(r) < \gamma(b)$ und der Wahl von b. Also ist $r = 0$ und daher $a = bq \in bR$. Dies zeigt $I = bR$. □

Es gibt Hauptidealringe, die nicht euklidisch sind, etwa

$$\mathbb{Z}\left[\tfrac{1}{2}(1+\sqrt{-19})\right] = \left\{\tfrac{1}{2}(a+b\sqrt{-19}) \mid a,b \in \mathbb{Z} \text{ und } a \equiv b \bmod 2\right\},$$

siehe Stroth, Algebra, de Gruyter 1998, S. 15–19 (oder Motzkin, The euclidean algorithm, Bull. Amer. Math. Soc. 55, 1949, 1142–1146; J. C. Wilson, A principal ideal ring that is not a euclidean ring, Math. Mag. 46, 1973, 34–38; Campoli, Amer. Math. Monthly 95, 1988, 868–871; R. A. Wilson, An example of a PID which is not a Euclidean domain, 2011; Perić, Vuković, Novi Sad J. Math. 38, 2008, 137–154; Kevin McGerty, A pid which is not a euclidean domain, 2014). Ein weiteres Beispiel dieser Art ist der Faktorring $\mathbb{R}[x,y]/(x^2+y^2+1)\mathbb{R}[x,y]$, siehe Perrin, Cours d'algèbre, Paris 1996, Chap. II, § 5.

11.3 Definition. Sei R ein Integritätsring und $a, b \in R$.
Man definiert $a \mid b \Leftrightarrow \exists r \in R : ar = b \Leftrightarrow b \in aR \Leftrightarrow bR \subseteq aR$, und sagt dann: a teilt b.

Man nennt a und b assoziiert, wenn $a \mid b \mid a$. Dies ist äquivalent zu $aR = bR$, und zu $ae = b$ für eine Einheit $e \in E(R)$ (wegen $ar = b$, $bs = a \Rightarrow ars = bs = a \Rightarrow a = 0 = b$ oder $rs = 1$, also $r \in E(R)$).

Sei K ein Körper; genau dann sind zwei Polynome $a, b \in K[x]$ assoziiert, wen $a = bc$ mit $0 \neq c \in K$, wegen $E(K[x]) = K^* x^0$.

Ein Element $p \in R \setminus E(R)$ heißt irreduzibel in R, falls aus $p = ab$ mit $a, b \in R$ folgt, dass $a \in E(R)$ oder $b \in E(R)$. Reduzibel bedeutet: nicht irreduzibel. [Also ist $0 = 0 \cdot 0$ reduzibel.]

Der Integritätsring R heißt faktoriell (oder ZPE-Ring, engl. unique factorization domain, UFD), falls gilt: jedes Element von $R \setminus (E(R) \cup \{0\})$ ist ein Produkt von (endlich vielen) irreduziblen Elementen, und diese Produktdarstellung ist im Wesentlichen eindeutig (d. h. aus $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$ mit irreduziblen $a_i, b_j \in R$ folgt $n = m$, und a_i ist assoziiert zu $b_{\pi(i)}$ für eine Permutation $\pi \in S_n$).

Beispiele: Ist K ein Körper, so sind $a, b \in K[x]$ genau dann assoziiert, wenn $a = bc$ mit $0 \neq c \in K$, wegen $E(K[x]) = K^* \cdot x^0$. Die irreduziblen Elemente von $\mathbb{Z}$ sind $\pm p$, wobei p eine Primzahl ist.

11.4 Bemerkung. Sei R ein euklidischer Ring und seien $r_1, r_2 \in R$ mit $r_2 \neq 0$. Dann kann man den euklidischen Algorithmus anwenden, d. h. die Division mit Rest iterieren:

$$\begin{aligned} r_1 &= q_1 r_2 + r_3, \\ r_2 &= q_2 r_3 + r_4, \text{ etc., allgemein} \\ r_{n-1} &= q_{n-1} r_n + r_{n+1}, \end{aligned}$$

solange die $r_i \neq 0$ sind. Wegen $\gamma(r_{i+1}) < \gamma(r_i)$ wird irgendwann $r_{n+1} = 0 \neq r_n$ erreicht. Dann ist r_n ein Teiler von $r_{n-1}, r_{n-2}, \ldots, r_3, r_2, r_1$, also ein gemeinsamer Teiler von r_1 und r_2. Jeder gemeinsame Teiler von r_1 und r_2 teilt r_3, also auch $r_4, \ldots$, also auch r_n. Man sagt dafür: r_n ist ein größter gemeinsamer Teiler von r_1 und r_2.

[Wechselwegnahme bei den alten Griechen: Sind zwei Strecken gegeben, so nimmt man von der grösseren die kleinere mehrmals weg, sooft es geht, und fährt dann mit

vertauschten Rollen fort. Die Frage, ob dieser Prozess immer ein Ende findet, führte zur Entdeckung der Inkommensurabilität zwischen Seite und Diagonale im regelmässigen Fünfeck durch die Pythagoräer, ca. 450 vor Chr.]

11.5 Lemma. *Sei R ein Hauptidealring und $p \in R$ sei irreduzibel.*

(i) *Dann ist pR ein maximales Ideal von R (also ist R/pR ein Körper nach 10.4).*

(ii) *Aus $p \mid ab$ mit $a, b \in R$ folgt $p \mid a$ oder $p \mid b$ (also ist p ist ein sog. Primelement).*

Beweis. (i) Sei $pR \subseteq I \trianglelefteq R$. Es gibt ein $a \in R$ mit $I = aR$. Wegen $p \in pR \subseteq I = aR$ ist $p = ab$ für ein $b \in R$. Die Irreduzibilität impliziert $a \in E(R)$ oder $b \in E(R)$, also $I = aR = R$ oder $I = aR = pb^{-1}R = pR$.
(ii) Sei p kein Teiler von a, also $a \notin pR$. Dann ist das Ideal $pR + aR$ echt größer als pR, also gilt $pR + aR = R$ nach (i). Daher existieren $r, s \in R$ mit $pr + as = 1$. Es folgt $p \mid prb + abs = (pr + as)b = b$. □

11.6 Satz. *Jeder euklidische Ring R ist faktoriell. Insbesondere ist $K[x]$ faktoriell für jeden Körper K.*

Beweis. Eindeutigkeit: Sei $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$ mit irreduziblen $a_i, b_j \in R$. Mit 11.2 und 11.5(ii) folgt $a_1 \mid b_j$ für ein j. Wegen der Irreduzibilität von b_j sind a_1 und b_j assoziiert. Man kann a_1 kürzen und die Einheit $a_1^{-1} b_j \in Q(R)$ einem anderen Faktor zuschlagen. Daher führt Induktion nach n zum Ziel.

Existenz einer Faktorisierung: Angenommen $a \in R \setminus (E(R) \cup \{0\})$ lässt sich nicht als Produkt von irreduziblen Elementen schreiben; wähle a so, dass $\gamma(a)$ möglichst klein ist. Dann ist a nicht irreduzibel, also $a = bc$ mit $b, c \in R \setminus (E(R) \cup \{0\})$. Im Fall $\gamma(a) > \gamma(b)$ und $\gamma(a) > \gamma(c)$ sind b und c Produkte von irreduziblen Elementen, also auch $a = bc$. Daher dürfen wir $\gamma(a) \leq \gamma(b)$ annehmen (ggf. nach Vertauschen von b und c).

Wegen 11.1(ii) existieren $q, r \in R$ mit $b = aq + r$ und $r = 0$ oder $\gamma(r) < \gamma(a)$. Wegen $b = aq + r = bcq + r$ gilt $b \mid r$. Im Fall $r \neq 0$ folgt $\gamma(b) \leq \gamma(r)$ nach 11.1(i), ein Widerspruch zu $\gamma(r) < \gamma(a) \leq \gamma(b)$. Also gilt $r = 0$ und $b = aq = bcq$. Wir erhalten $1 = cq$, also $c \in E(R)$, ein Widerspruch. □

11.7 Bemerkungen. Man kann zeigen, dass jeder Hauptidealring faktoriell ist (siehe etwa Stroth, Algebra, de Gruyter 1998, Hauptsatz 1.28; Jacobson, Basic algebra I, Freeman 1985, Theorem 2.23). Also gelten die folgenden Implikationen:

$$\text{euklidisch} \Rightarrow \text{Hauptidealring} \Rightarrow \text{faktoriell}.$$

Ferner ist mit R auch $R[x]$ faktoriell (siehe Stroth, Algebra, de Gruyter 1998, Satz 1.45; Jacobson, Basic algebra I, Freeman 1985, Theorem 2.25). Demnach sind die Ringe $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ und $K[x_1, x_2, \ldots, x_n]$ für jeden Körper K faktoriell.

$R = \mathbb{Z}[x]$ ist kein Hauptidealring, denn das Ideal $2R + xR = \{p \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$ ist kein Hauptideal. $R = K[x, y]$ mit einem Körper K ist auch kein Hauptidealring, weil das Ideal $xR + yR = \{p \in R \mid p(0, 0) = 0\}$ kein Hauptideal ist. Nach 11.2 sind diese Ringe auch nicht euklidisch.

11.8 Beispiele. Die folgenden Ringe sind nicht faktoriell (nach 11.6 also nicht euklidisch, und nach 11.7 auch keine Hauptidealringe):
(a) Der Ring $R := \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5} \subseteq \mathbb{C}$ hat die Einheitengruppe $E(R) = \{1, -1\}$, und die Elemente $2, 3, 1 \pm \sqrt{-5}$ sind irreduzibel in R. Wegen $2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, oder wegen $3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$, ist die Faktorisierung in irreduzible Elemente nicht eindeutig. Ähnlich zeigt man: $\mathbb{Z}[\sqrt{10}]$ ist nicht faktoriell, wegen $3^2 = (\sqrt{10}+1)(\sqrt{10}-1)$.
(b) Für $R := \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[i]$ gilt $E(R) = \{\pm 1\}$, und $2, 2i$ sind irreduzibel und nicht assoziiert (wegen $i \notin R$). Wegen $2 \cdot 2 = -(2i)(2i)$ ist R nicht faktoriell. [Aber $\mathbb{Z}[i]$ ist euklidisch und daher faktoriell.]
(c) Sei K ein Körper und $R := K[x^2, x^3] = K + x^2K[x] \subseteq K[x]$. Wegen $x^6 = (x^2)^3 = (x^3)^2$ ist R nicht faktoriell, denn x^2 und x^3 sind irreduzibel in R und nicht assoziiert (wegen $x \notin R$).
(d) Die irreduziblen Elemente von $R := \mathbb{Z} + x\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$ sind $\pm p$ für eine Primzahl p und die irreduziblen Polynome $f \in \mathbb{Q}[x]$ mit $f(0) = \pm 1$. Daher lässt sich $x \in R$ nicht als Produkt von irreduziblen Elementen von R schreiben (x ist nicht irreduzibel, wegen $x = 2 \cdot (\frac{1}{2}x) = 3 \cdot (\frac{1}{3}x) = \ldots$; beachte $\frac{1}{2}, \frac{1}{3} \notin R$).

12. Irreduzible Polynome

Das Polynom $2x + 2 = 2(x + 1)$ ist irreduzibel in $\mathbb{Q}[x]$, aber nicht in $\mathbb{Z}[x]$, wegen $2 \in E(\mathbb{Q}[x])$ und $2 \notin E(\mathbb{Z}[x])$. Das Polynom $2 = 2 \cdot x^0$ ist irreduzibel in $\mathbb{Z}[x]$, aber nicht in $\mathbb{Q}[x]$.

12.1 Definition. Ein Polynom $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ heißt primitiv, falls $a_0, a_1, \ldots, a_n$ teilerfremd sind (d. h. ± 1 sind die einzigen gemeinsamen Teiler von $a_0, a_1, \ldots, a_n$). Dann ist $f \neq 0$.

12.2 Lemma (Lemma von Gauß)**.** *Sind $f, g \in \mathbb{Z}[x]$ primitiv, so ist auch fg primitiv.*

Beweis. Ist fg nicht primitiv, so existiert eine Primzahl p, welche alle Koeffizienten von fg teilt. Die kanonische Projektion $^- : \mathbb{Z} \to \mathbb{Z}_p$ setzt sich fort zu dem Ringhomomorphismus $^- : \mathbb{Z}[x] \to \mathbb{Z}_p[x] : \sum_i a_i x^i \mapsto \sum_i \bar{a}_i x^i$ (koeffizientenweises Anwenden). Es gilt $0 = \overline{fg} = \bar{f}\bar{g}$. Nach 10.7 und 8.2(b) ist $\mathbb{Z}_p[x]$ nullteilerfrei, daher folgt $\bar{f} = 0$ oder $\bar{g} = 0$. Also ist f oder g nicht primitiv. □

12.3 Proposition. (i) *Ist $f \in \mathbb{Z}[x]$ irreduzibel in $\mathbb{Z}[x]$ und* $\mathrm{Grad}(f) > 0$*, so ist f auch irreduzibel in $\mathbb{Q}[x]$.*

(ii) *Ist $f \in \mathbb{Z}[x]$ primitiv (etwa normiert) und irreduzibel in $\mathbb{Q}[x]$, so ist f auch irreduzibel in $\mathbb{Z}[x]$.*

Beweis. (i) f ist primitiv. Sei $f = g_1 g_2$ mit $g_i \in \mathbb{Q}[x]$. Es existieren primitive Polynome $h_i \in \mathbb{Z}[x]$ und $a_i \in \mathbb{Z}, b_i \in \mathbb{N}$ mit $g_i = \frac{a_i}{b_i} h_i$ für $i = 1, 2$. Wir erhalten

$$b_1 b_2 f = a_1 a_2 h_1 h_2.$$

Nach 12.2 ist h_1h_2 primitiv. Daher ist b_1b_2 bzw. a_1a_2 ein größter gemeinsamer Teiler aller Koeffizienten des linken bzw. rechten Polynoms, also $b_1b_2 = \pm a_1a_2$. Es folgt $f = \pm h_1h_2$. Wegen der Irreduzibilität von f in $\mathbb{Z}[x]$ ist h_1 oder h_2 eine Einheit in $\mathbb{Z}[x]$, also gleich ± 1. Daher ist g_1 oder g_2 eine Einheit in $\mathbb{Q}[x]$.
(ii) Faktorisiert f in $\mathbb{Z}[x]$, so ist einer der Faktoren eine Einheit in $\mathbb{Q}[x]$ und hat daher den Grad 0, also die Form ax^0 mit $a \in \mathbb{Z}$. Daher teilt a alle Koeffizienten von f. Weil f primitiv ist, folgt $a = \pm 1$. Daher ist ax^0 eine Einheit in $\mathbb{Z}[x]$. □

12.4 Satz (Irreduzibilitätskriterium von Eisenstein)**.** *Sei $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Wenn eine Primzahl p existiert mit $p \nmid a_n$, $p \mid a_i$ für $0 \le i \le n-1$ und $p^2 \nmid a_0$, dann ist f irreduzibel in $\mathbb{Q}[x]$.*

Beweis. Man darf annehmen, dass f primitiv ist (Division durch den ggT der Koeffizienten lässt die Bedingungen an die Koeffizienten unverändert wegen $p \nmid a_n$). Wegen $p \mid a_0$ und $p \nmid a_n$ ist $n > 0$, und nach 12.3(i) genügt es zu zeigen, dass f in $\mathbb{Z}[x]$ irreduzibel ist.

Sei $f = gh$ mit $g, h \in \mathbb{Z}[x]$. Wegen $p^2 \nmid a_0 = f(0) = g(0)h(0)$ ist $p \nmid g(0)$ oder $p \nmid h(0)$. Wir dürfen $p \nmid g(0)$ annehmen (und werden zeigen, dass g eine Einheit von $\mathbb{Z}[x]$ ist). Anwenden des Ringhomomorphismus $\bar{} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ wie in 12.2 ergibt

$$\bar{g}\bar{h} = \bar{f} = \overline{a_n} x^n \neq 0.$$

Nach 11.6 ist $\mathbb{Z}_p[x]$ faktoriell. Daher ist $\bar{g} = cx^k$ mit $k \in \mathbb{N}_0$ und $0 \neq c \in \mathbb{Z}_p$. Wegen $\bar{g}(\bar{0}) = \overline{g(0)} \neq \bar{0}$ ist $\mathrm{Grad}(\bar{g}) = k = 0$. Es folgt $n = \mathrm{Grad}(\bar{h}) \le \mathrm{Grad}(h) \le \mathrm{Grad}(f) = n$, also $\mathrm{Grad}(h) = n$ und $\mathrm{Grad}(g) = 0$. Daher ist $f = g_0 h$ mit $g_0 \in \mathbb{Z}$. Weil f primitiv ist, folgt $g_0 = \pm 1$ und $g = g_0 x^0 \in E(\mathbb{Z}[x])$. □

12.5 Beispiele. (a) Für $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ ist das Polynom $x^n - a$ ist nach 12.4 irreduzibel in $\mathbb{Q}[x]$ und $\mathbb{Z}[x]$, falls $p \mid a$, $p^2 \nmid a$ für eine Primzahl p gilt. (Insbesondere ist dann $\sqrt[n]{a} \notin \mathbb{Q}$ für $n \ge 2$, denn $\sqrt[n]{a}$ ist eine Nullstelle von $x^n - a$, vgl. 8.4(i).)
(b) Für jede Primzahl p ist das Kreisteilungspolynom $\Phi_p = \frac{x^p-1}{x-1} = \sum_{j=0}^{p-1} x^j$ irreduzibel in $\mathbb{Q}[x]$ und in $\mathbb{Z}[x]$, denn:

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{j=1}^{p} \binom{p}{j} x^{j-1}$$

ist irreduzibel in $\mathbb{Q}[x]$ nach 12.4, und mit $\Phi_p(x+1)$ ist auch Φ_p irreduzibel (weil $f \mapsto f(x+1)$ ein Ringautomorphismus von $\mathbb{Q}[x]$ und daher mit dem Begriff „irreduzibel“ verträglich ist).
(c) Mit der gleichen Methode kann man Φ_n für Primzahlpotenzen n behandeln; beispielsweise gilt für jede Primzahl p

$$\Phi_{p^2} = \frac{x^{p^2}-1}{\Phi_1\Phi_p} = \frac{x^{p^2}-1}{x^p-1} = \Phi_p(x^p) = \sum_{j=0}^{p-1} x^{jp},$$

also $(x^p - 1)\Phi_{p^2} = x^{p^2} - 1$. Die letzte Gleichung gilt auch in $\mathbb{Z}_p[x]$ für das Polynom $\overline{\Phi_{p^2}} \in \mathbb{Z}_p[x]$, das man durch Reduzieren aller Koeffizienten modulo p erhält (weil das koeffzientenweise Reduzieren ein Ringhomomorphismus $\bar{} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ ist, vgl. die Beweise

zu 12.2 und 12.4). In $\mathbb{Z}_p[x]$ gilt aber $(x-1)^p = x^p - 1$, also $(x-1)^p\overline{\Phi_{p^2}} = (x-1)^{p^2}$ und daher $\overline{\Phi_{p^2}} = (x-1)^{p^2-p}$. Dies impliziert $\overline{\Phi_{p^2}(x+1)} = \overline{\Phi_{p^2}}(x+1) = x^{p^2-p}$, also sind alle Koeffizienten von $\Phi_{p^2}(x+1)$ außer dem Leitkoeffizienten durch p teilbar. Ferner ist $\Phi_{p^2}(0+1) = \Phi_p((0+1)^p) = \Phi_p(1) = p$ nicht durch p^2 teilbar. Nach 12.4 ist $\Phi_{p^2}(x+1)$ irreduzibel in $\mathbb{Q}[x]$, also auch Φ_{p^2}.

Es ist schwerer zu zeigen, dass alle Φ_n irreduzibel in $\mathbb{Q}[x]$ sind (siehe etwa Stroth, Algebra, de Gruyter 1998, Satz 11.11, oder Jacobson, Basic algebra I, Freeman 1985, Theorem 4.17, oder Weintraub, Several proofs of the irreducibilty of the cyclotomic polynomials, Amer. Math. Monthly 120 (2013) 537–545). Demnach ist $x^n - 1 = \prod_{d \text{ teilt } n} \Phi_d$ die Zerlegung von $x^n - 1$ in normierte irreduzible Polynome im Polynomring $\mathbb{Q}[x]$.

Versionen von 12.2–12.4 für faktorielle Ringe findet man etwa bei Stroth, Algebra, de Gruyter 1998, 1.42–1.44 und 1.48.

Teil III.
KÖRPER

13. Körpererweiterungen

13.1 Definition. Sei K ein Körper. Der Durchschnitt K_0 aller Teilkörper von K ist der kleinste Teilkörper von K, der sogenannte Primkörper von K.

Hat K die Charakteristik 0 (d. h. die additive Ordnung von 1_K ist unendlich), so gilt $\mathbb{Z} \cdot 1_K \cong \mathbb{Z}$ und $K_0 \cong \mathbb{Q}$. Andernfalls ist die Charakteristik von K eine Primzahl p, siehe ÜA 18, und dann gilt $\mathbb{Z} \cdot 1_K \cong \mathbb{Z}_p$ und $K_0 = \mathbb{Z} \cdot 1_k \cong \mathbb{Z}_p$.

13.2 Definition. Ist K ein Teilkörper eines Körpers L, so spricht man von der Körpererweiterung $L|K$ oder $K \subseteq L$. Dann ist L ein K-Vektorraum (mit der Einschränkung der Körpermultiplikation von $L \times L$ auf $K \times L$ als Skalarmultiplikation), und man nennt $[L : K] := \dim_K L$ den Grad von $L|K$.

Die Körpererweiterung $L|K$ heißt endlich, falls $[L : K]$ endlich ist, und quadratisch bzw. kubisch, falls $[L : K] = 2$ bzw. 3.

Jeder Teilkörper von L, der K enthält, heißt ein Zwischenkörper von $L|K$. Für jedes $a \in L$ ist $K(a) := \left\{ \frac{p(a)}{q(a)} \mid p, q \in K[x],\ q(a) \neq 0 \right\}$, gelesen „$K$ adjungiert a“, der kleinste Zwischenkörper, welcher a enthält. Für $a, b \in L$ setzt man $K(a, b) := K(a)(b)$, etc.

Beispiele: Jeder Körper ist eine Erweiterung seines Primkörpers. Es gilt $[\mathbb{C} : \mathbb{R}] = 2$, weil $\{1, i\}$ eine Basis des $\mathbb{R}$-Vektorraums $\mathbb{C}$ ist. Für den Körper $K(x)$ der rationalen Funktionen über einem Körper K ist der Grad $[K(x) : K]$ unendlich, weil schon $\dim_K K[x]$ unendlich ist.

13.3 Satz (Gradformel)**.** *Seien $M|L$ und $L|K$ endliche Köpererweiterungen. Dann ist $M|K$ endlich und $[M : K] = [M : L][L : K]$.*

Beweis. Sei $m_1, m_2, \ldots, m_r$ eine Basis von M über L und $l_1, l_2, \ldots, l_s$ eine Basis von L über K. Wir zeigen, dass die Folge $(l_i m_j)_{1 \leq i \leq s,\, 1 \leq j \leq r}$ eine Basis von M über K ist; dann folgt $[M : K] = rs = [M : L][L : K]$.

Wegen $M = Lm_1 \oplus Lm_2 \oplus \cdots \oplus Lm_r$ und $L = Kl_1 \oplus Kl_2 \oplus \cdots \oplus Kl_s$ wird M als K-Vektorraum von den Elementen $l_i m_j$ erzeugt. Diese Elemente sind auch K-linear unabhängig, denn aus $k_{ij} \in K$ und

$$0 = \sum_{i=1}^{s} \sum_{j=1}^{r} k_{ij} l_i m_j = \sum_{j=1}^{r} \underbrace{\left(\sum_{i=1}^{s} k_{ij} l_i \right)}_{\in L} m_j$$

folgt $\sum_{i=1}^{s} k_{ij} l_i = 0$ für jedes j, und dann $k_{ij} = 0$ für alle i, j. □

13.4 Definition. Sei $L|K$ eine Körpererweiterung. Ein Element $a \in L$ heißt algebraisch über K, falls ein Polynom $p \in K[x]$ existiert mit $p(a) = 0$ und $p \neq 0$; andernfalls heißt a transzendent über K.

Die Auswertung $e_a : K[x] \to L : p \mapsto p(a)$ ist ein Ringhomomorphismus mit dem Kern $\ker e_a := \{p \in K[x] \mid p(a) = 0\}$. Nach 11.2 ist das Ideal $\ker e_a$ ein Hauptideal. Ist $a \in L$ algebraisch über K, so ist $\ker e_a \neq \{0\}$, und es existiert genau ein normiertes Polynom $m \in K[x]$ mit $\ker e_a = mK[x]$; man nennt m das Minimalpolynom von a über K. Mit anderen Worten: m ist das normierte Polynom aus $K[x]$ mit $m(a) = 0$, welches den kleinstmöglichen Grad hat (vgl. Beweis zu 11.2). Ist $a \in L$ transzendent über K, so gilt $K[a] \cong K[x]$ und $K(a) \cong K(x)$.

Ist $L|K$ endlich, so ist jedes Element von L algebraisch über K, siehe ÜA 28.

Beispiel: $a = \sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, und $x^2 - 2$ ist das Minimalpolynom von a über $\mathbb{Q}$.

13.5 Definition. Seien $L|K$ und $M|K$ Körpererweiterungen. Ein (Ring-) Homomorphismus $f : L \to M$ heißt K-Homomorphismus, falls $f|_K = \mathrm{id}_K$. Wegen $f(1) = 1$ ist dies äquivalent dazu, dass f eine K-lineare Abbildung ist. Ist zusätzlich $f : L \to M$ bijektiv, so heißt f ein K-Isomorphismus.

13.6 Satz. *Sei $L|K$ eine Körpererweiterung, und $a \in L$ sei algebraisch über K. Dann ist $n := [K(a) : K]$ endlich, und $1, a, a^2, \dots a^{n-1}$ ist eine K-Basis von $K(a) = K[a]$, also*

$$K(a) = K \oplus Ka \oplus Ka^2 \oplus \cdots \oplus Ka^{n-1}.$$

Ferner ist das Minimalpolynom m von a über K irreduzibel in $K[x]$ und hat den Grad n, und der Körper $K(a)$ ist K-isomorph zu $K[x]/mK[x]$.

Beweis. m ist irreduzibel, denn aus $m = fg$ mit $f, g \in K[x]$ und $\mathrm{Grad}(f), \mathrm{Grad}(g) < \mathrm{Grad}(m)$ folgt $0 = m(a) = f(a)g(a)$, also $f(a) = 0$ oder $g(a) = 0$, ein Widerspruch zur Definition von m.

Die Auswertung $e_a : K[x] \to L : p \mapsto p(a)$ hat den Kern $mK[x]$ und das Bild $K[a] = \{p(a) \mid p \in K[x]\} \subseteq L$. Nach 10.3 (mit Beweis) ist die Abbildung $K[x]/mK[x] \to K[a] : p + mK[x] \mapsto p(a)$ ein Ringisomorphismus; diese Abbildung ist auch K-linear. Nach 11.5(i) und 10.4 ist $K[x]/mK[x]$ ein Körper, also auch $K[a]$. Wegen $a \in K[a]$ folgt $K(a) \subseteq K[a]$, also $K(a) = K[a]$.

Sei $d = \mathrm{Grad}(m)$. Wegen $m(a) = 0$ gilt $a^d \in K + Ka + \cdots + Ka^{d-1}$ und daher $K(a) = K[a] = K + Ka + \cdots + Ka^{d-1}$. Nach Definition von m sind die Potenzen $1, a, a^2, \dots, a^{d-1}$ über K linear unabhängig, also $K[a] = K \oplus Ka \oplus \cdots \oplus Ka^{d-1}$ und $n = [K(a) : K] = \dim_K K[a] = d$. □

13.7 Beispiele. $\sqrt[3]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, und $1, \sqrt[3]{2}, \sqrt[3]{4}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt[3]{2})$. Ferner ist $m = x^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, und $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)\mathbb{Q}[x]$.

Die komplexe Zahl $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, mit dem Minimalpolynom $x^2 + 1$, und $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$.

14. Exkurs: Konstruktionen mit Zirkel und Lineal

Dieser Abschnitt enthält Anwendungen von Ergebnissen aus Kapitel 12 und 13 auf klassische geometrische Probleme.

14.1 Definition (Konstruktion mit Zirkel und Lineal)**.** Man konstruiert (wie Euklid) aus gegebenen Punkten der (reellen euklidischen) Ebene $\mathbb{R}^2$ weitere Objekte „mit Zirkel und Lineal“: mit dem Lineal kann man die Gerade durch zwei gegebene Punkte zeichnen, und mit dem Zirkel kann man einen Kreis mit gegebenem Mittelpunkt und gegebenem Randpunkt zeichnen. Weitere Punkte entstehen als Schnitte von Geraden und Kreisen. Eine solche Konstruktion hat immer endlich viele Schritte.

Wir reden nur von konstruierten Punkten, weil man jede Gerade durch zwei Punkte ersetzen kann, jeden Winkel durch zwei Geraden, und jeden Kreis durch seinen Mittelpunkt und einen Randpunkt.

14.2 Satz. *Sei der Punkt $(a, b) \in \mathbb{R}^2$ durch endlich viele Konstruktionsschritte mit Zirkel und Lineal aus den Punkten $(0, 0)$ und $(1, 0)$ konstruierbar. Dann sind a und b algebraisch über $\mathbb{Q}$, und $[\mathbb{Q}(a, b) : \mathbb{Q}]$ und auch die Grade $[\mathbb{Q}(a) : \mathbb{Q}]$ und $[\mathbb{Q}(b) : \mathbb{Q}]$ der Minimalpolynome von a und b über $\mathbb{Q}$ sind Potenzen von 2.*

Beweis. Die Gerade durch zwei verschiedene Punkte (a_1, b_1) und (a_2, b_2) wird beschrieben durch die Gleichung

$$0 = (x - a_1)(b_1 - b_2) - (y - b_1)(a_1 - a_2).$$

Seien jetzt $P_i = (a_i, b_i) \in \mathbb{R}^2$ für $1 \leq i \leq n$ und sei $K := \mathbb{Q}(a_1, \ldots, a_n, b_1, \ldots, b_n)$. Entsteht der Punkt $(a, b) \in \mathbb{R}^2$ aus den Punkten $P_1, \ldots, P_n$ durch *einen* Konstruktionsschritt mit Zirkel und Lineal, dann gilt $[K(a, b) : K] \leq 2$, denn dieser Konstruktionsschritt ist von einem der drei folgenden Typen:

(1) (a, b) ist der Schnittpunkt von zwei verschiedenen Geraden P_iP_j und P_kP_l. Dann ist (a, b) die einzige Lösung eines linearen Gleichungssystems (zwei Gleichungen mit zwei Unbekannten) mit Koeffizienten aus K. Daher gilt $a, b \in K$ (wie der Gauß-Algorithmus oder die Cramersche Regel zeigt), also $K(a, b) = K$.

(2) (a, b) ist ein Schnittpunkt einer Geraden P_iP_j mit dem Kreis um P_k durch P_l. Dann löst (a, b) ein Gleichungssystem von der Form

$$\begin{aligned} \alpha x + \beta y + \gamma &= 0 \quad \text{mit } \alpha, \beta, \gamma \in K \\ (x - a_k)^2 + (y - b_k)^2 &= (a_l - a_k)^2 + (b_l - b_k)^2. \end{aligned}$$

Wegen $(\alpha, \beta) \neq (0, 0)$ kann man die erste Gleichung nach x oder nach y auflösen. Einsetzen in die zweite Gleichung liefert eine quadratische Gleichung für y bzw. x mit Koeffizienten aus K; das Minimalpolynom von b bzw. a über K hat also einen Grad ≤ 2. Also gilt $[K(b) : K] \leq 2$ bzw. $[K(a) : K] \leq 2$. Wegen $\alpha a + \beta b + \gamma = 0$ ist $a \in K(b)$ oder $b \in K(a)$, also stets $[K(a, b) : K] \leq 2$.

(3) (a, b) ist ein Schnittpunkt von zwei Kreisen mit den Gleichungen

$$(x - \alpha_j)^2 + (y - \beta_j)^2 = r_j^2 \qquad \text{für } j = 1, 2, \text{ wobei } \alpha_j, \beta_j, r_j^2 \in K.$$

Dann löst (a, b) insbesondere die erste Kreisgleichung (mit $j = 1$) und die Differenzengleichung

$$2(-\alpha_1 + \alpha_2)x + 2(-\beta_1 + \beta_2)y = r_1^2 - r_2^2 - \alpha_1^2 + \alpha_2^2 - \beta_1^2 + \beta_2^2.$$

Es gilt $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$, sonst hätten die zwei Kreise den gleichen Mittelpunkt, und wie bei Typ (2) folgt $[K(a, b) : K] \leq 2$.

Entsteht der Punkt (a, b) durch endlich viele Konstruktionsschritte aus $(0, 0)$ und $(1, 0)$, dann erhält man rekursiv eine Kette von Körpern $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t$ mit $[K_{i+1} : K_i] \leq 2$ für $0 \leq i \leq t - 1$ und $a, b \in K_t$. Nach der Gradformel 13.3 ist $[K_t : \mathbb{Q}] = \prod_{i=0}^{t-1} [K_{i+1} : K_i]$ eine Potenz von 2. Wegen $[K_t : \mathbb{Q}] = [K_t : \mathbb{Q}(a, b)][\mathbb{Q}(a, b) : \mathbb{Q}]$ ist auch $[\mathbb{Q}(a, b) : \mathbb{Q}]$ eine Potenz von 2; genauso argumentiert man für $[\mathbb{Q}(a) : \mathbb{Q}]$ und $[\mathbb{Q}(b) : \mathbb{Q}]$. Nach 13.6 sind die Körpergrade von $\mathbb{Q}(a)$ und $\mathbb{Q}(b)$ auch die Grade der Minimalpolynome. □

[Ist a eine reelle Nullstelle von $x^4 - 4x + 2$, so hat $\mathbb{Q}(a)|\mathbb{Q}$ den Grad 4, aber keinen quadratischen Zwischenkörper. Daher ist der Punkt $(a, 0)$ nicht aus den Punkten $(0, 0)$ und $(1, 0)$ mit Zirkel und Lineal konstruierbar. Weitere Beispiele dieser Art bei Brandl, Alle Algebra-Aufgaben, Hof 2000, S. 294, 341.]

Anwendung auf Probleme aus der Antike:

14.3 Beispiel (Das Delische Problem der Würfelverdopplung)**.** Um Athen im Jahr 430 v. Chr. von der Pest zu befreien, verlangte das Orakel von Delos, dass der würfelförmige Apollo-Altar verdoppelt werden müsse. Die Athener konstruierten einen Altar mit der doppelten Kantenlänge (worauf die Pest angeblich noch schlimmer wurde). Verlangt war die Verdopplung des Volumens, also die Konstruktion von $\sqrt[3]{2}$, wenn der alte Altar die Kantenlänge 1 hatte. Diese Konstruktion ist mit Zirkel und Lineal nach 14.2 nicht möglich, denn $\sqrt[3]{2}$ hat über $\mathbb{Q}$ das Minimalpolynom $x^3 - 2$ (irreduzibel nach 12.5(a)) und daher gilt $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ nach 13.6.

14.4 Beispiel (Quadratur des Kreises)**.** Zu einem Kreis mit Radius 1, also mit der Fläche π, soll ein flächengleiches Quadrat konstruiert werden,[2] also ein Quadrat mit der Seitenlänge $\sqrt{\pi}$. Dies ist nach 14.2 mit Zirkel und Lineal nicht möglich: π ist über $\mathbb{Q}$ transzendent (nach Lindemann[3] 1882; siehe etwa Stroth, Algebra, de Gruyter 1998, Seite 277–280; Jacobson, Basic Algebra I, Freeman 1985, Section 4.12, Seite 277–286; Hadlock, Field theory and its classical problems, Amer. Math. Assoc. 1978, Section 1.7; Drinfeld, Quadratur des Kreises und Transzendenz von π, VEB Dt. Verlag der Wiss. Berlin 1980), daher ist auch $\sqrt{\pi}$ über $\mathbb{Q}$ transzendent, wegen $\pi \in \mathbb{Q}(\sqrt{\pi})$.

[2] Mit diesem Problem hat sich z. B. Anaxagoras um 434 v. Chr. beschäftigt, als er wegen Gottlosigkeit im Athener Gefängnis saß. Sein Schüler Perikles hat die Todesstrafe verhindert, aber Anaxagoras wurde verbannt oder ist geflohen (und so der Pest in Athen entkommen, an der Perikles starb).

[3] 1877 in Würzburg habilitiert, Doktorvater von Hilbert, ab 1918 Ferdinand Ritter von Lindemann

14.5 Beispiel (Winkeldreiteilung)**.** Bei der Dreiteilung eines gegebenen Winkels α ist der Winkel $\beta = \alpha/3$ zu konstruieren, d. h. der Punkt $(\cos\beta, 0)$ ist aus den Punkten $(0,0)$, $(1,0)$ und $(\cos\alpha, 0)$ zu konstruieren. Wegen

$$\begin{aligned}\cos\alpha = \cos 3\beta = \mathrm{Re}(e^{i3\beta}) = \mathrm{Re}((\cos\beta + i\sin\beta)^3) = (\cos\beta)^3 - 3\cos\beta(\sin\beta)^2 \\ = (\cos\beta)^3 - 3\cos\beta\,(1-(\cos\beta)^2) = 4(\cos\beta)^3 - 3\cos\beta\end{aligned}$$

ist $\cos\beta$ eine Nullstelle des Polynoms $4x^3 - 3x - \cos\alpha$.

Sei jetzt $\alpha = 60°$. Dann ist $\cos\alpha = \frac{1}{2}$ und $f(x) = 4x^3 - 3x - \frac{1}{2}$ ist irreduzibel in $\mathbb{Q}[x]$ (denn $2f(\frac{x}{2}) = x^3 - 3x - 1$ ist irreduzibel nach ÜA 24). Also ist $\cos 20°$ und damit der Winkel $\beta = 20°$ nach 14.2 nicht mit Zirkel und Lineal aus den Punkten $(0,0)$, $(1,0)$ konstruierbar (Wantzel 1837).

[Es gibt gute Näherungskonstruktionen, siehe Vahlen, Konstruktion und Approximation, Teubner 1911; Perron, Eine neue Winkeldreiteilung des Schneidermeisters KOPF, Sitzungsber. bayr. Akad. Wiss. 1933, 439–445; Dudley, What to do when the trisector comes, Math. Intelligencer 5 (1983) 20–25; Baptist, Winkeldreiteilung und Trisektierer, Praxis der Math. 29, 19871, 43–50; Dudley, A budget of trisections, Springer 1987.]

14.6 Beispiel (Kreisteilung)**.** Man konstruiere ein regelmäßiges n-Eck in einem gegebenen Kreis, also den Winkel $360°/n$. Wir beschränken uns auf den Einheitskreis; dann ist der Punkt $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ aus den Punkten $(0,0)$ und $(1,0)$ zu konstruieren.

[Pythagoras und seine Schule, ca. 600 v. Chr.; Euklid beschreibt in seinen Elementen die Konstruktion für $n = 3, 4, 5, 6, 15$.

Konstruktion für $n = 3$: Der Einheitskreis schneidet den Kreis um $(-1,0)$ durch $(0,0)$ in zwei Punkten P_1 und P_2, die zusammen mit $(1,0)$ ein regelmässiges Dreieck bilden (weil die zwei Dreiecke $(0,0)$, P_i, $(-1,0)$ gleichseitig sind). Bild

Konstruktion für $n = 5$, nach Ptolemaios, 2. Jahrhundert n. Chr.: Der Kreis um $(0, \frac{1}{2})$ durch $(1,0)$ schneidet die y-Achse in einem Punkt P. Dann ist der Abstand zwischen P und $(1,0)$ die gesuchte Seitenlänge des regelmässigen 5-Ecks (ÜA; diese Seitenlänge ist $\frac{1}{2}\sqrt{10-2\sqrt{5}}$, und $\cos\frac{2\pi}{5} = -\frac{1}{4} + \frac{1}{4}\sqrt{5}$). Bild]

14.7 Satz (Wantzel 1837)**.** *Das regelmäßige n-Eck sei mit Zirkel und Lineal konstruierbar. Dann ist $n = 2^e \cdot p_1 \cdots p_t$ mit $e \in \mathbb{N}_0$ und mit paarweise verschiedenen Primzahlen $p_j > 2$ von der Form $2^k + 1$ (sogenannte Fermat-Primzahlen; man kennt nur*[4] 3, 5, 17, 257, 65537).

Also ist das regelmässige n-Eck für $n = 7, 9, 11, 13, 14, 18, 19, \ldots$ nicht mit Zirkel und Lineal konstruierbar.

Beweis. Sei $(c,s) := (\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$. Wir identifizieren die Punkte der Ebene mit den komplexen Zahlen, also insbesondere (c,s) mit $z_n := c + is = e^{2\pi i/n}$. Dann gilt $z_n \in \mathbb{Q}(i,c,s)$, also ist $[\mathbb{Q}(z_n) : \mathbb{Q}]$ nach 13.3 ein Teiler von $[\mathbb{Q}(i,c,s) : \mathbb{Q}] = [\mathbb{Q}(i,c,s) : \mathbb{Q}(c,s)] \cdot [\mathbb{Q}(c,s) : \mathbb{Q}] = 2[\mathbb{Q}(c,s) : \mathbb{Q}]$. Aus der Konstruierbarkeit folgt mit 14.2, dass $[\mathbb{Q}(z_n) : \mathbb{Q}]$ eine Potenz von 2 ist.

[4] Derzeit ist offen, ob die nächste Kandidatin $2^{2^{33}} + 1$ eine Primzahl ist.

Für jeden Teiler t von n ist auch das regelmäßige t-Eck und die Zahl $z_t = e^{2\pi i/t}$ konstruierbar (durch Auslassen von Punkten); also ist auch $[\mathbb{Q}(z_t) : \mathbb{Q}]$ eine Potenz von 2.

Sei jetzt p eine ungerade Primzahl, welche n teilt. Dann ist $[\mathbb{Q}(z_p) : \mathbb{Q}]$ eine Potenz von 2. Es gilt $\Phi_p(z_p) = 0$ (nach Definition der Kreisteilungspolynome in 9.1), und $\Phi_p = \frac{x^p-1}{x-1}$ ist irreduzibel in $\mathbb{Q}[x]$ nach 12.5(b). Also ist Φ_p das Minimalpolynom von z_p über $\mathbb{Q}$, und mit 13.6 folgt $[\mathbb{Q}(z_p) : \mathbb{Q}] = \mathrm{Grad}(\Phi_p) = p-1$. Daher ist p eine Fermat-Primzahl.

Wäre sogar $p^2 \mid n$, dann wäre das regelmässige p^2-Eck konstruierbar, also $[\mathbb{Q}(z_{p^2}) : \mathbb{Q}]$ eine Potenz von 2. Das Polynom $\Phi_{p^2} = \frac{x^{p^2}-1}{x^p-1}$ annulliert z_{p^2} und ist irreduzibel in $\mathbb{Q}[x]$ nach 12.5(c). Also ist Φ_{p^2} das Minimalpolynom von z_{p^2} über $\mathbb{Q}$, und mit 13.6 folgt $[\mathbb{Q}(z_{p^2}) : \mathbb{Q}] = \mathrm{Grad}(\Phi_{p^2}) = p^2 - p = p(p-1)$. Wegen $p > 2$ ist diese Zahl keine Potenz von 2, ein Widerspruch. □

Nach Gauß[5] gilt auch die Umkehrung von 14.7 [mit etwas Galois-Theorie kann man die Existenz von allen Zwischenkörpern wie im Beweis von 14.2 zeigen, vgl. Stroth, Algebra, de Gruyter 1998, Satz 10.3; Jacobson, Basic algebra I, Freeman 1985, Section 4.11; für einen direkteren Beweis siehe Hadlock, Field theory and its classical problems, Amer. Math. Assoc. 1978]. Insbesondere ist das regelmäßige 17-Eck mit Zirkel und Lineal konstruierbar (Gauß 1796, mit 18 Jahren); es gilt $\cos\frac{2\pi}{17} =$

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

[vgl. etwa Stroth, loc. cit., Seite 150; Hadlock, loc. cit., Seite 113f; eine Konstruktion wird beschrieben in Dummit, Foote, Abstract Algebra, 2004, Seite 604f und in Strommer, Zur Konstruktion des regulären Siebzehnecks, Studia Math. Hungar. 30 (1995) 433–441.

Zum 257-Eck: Richelot 1832; Strommer, Acta Math. Hungar. 70 (1996) 259–292; Gottlieb, Math. Intelligencer 21, (1) (1999) 31–37.

Johann Gustav Hermes, Ueber die Teilung des Kreises in 65537 gleiche Teile, Nachr. Ges. Wiss. Göttingen, Math.-Physikal. Klasse, 1894, 170–186 (Zusammenfassung einer Konstruktion, an der Hermes 10 Jahre lang gearbeitet hat; die Details liegen in einem Koffer im Mathematischen Institut in Göttingen, vgl. DIE ZEIT 16. 8. 2012).

Literatur: Martin, Geometric constructions, Springer 1998.
Laugwitz, Eine elementare Methode für Unmöglichkeitsbeweise bei Konstruktionen mit Zirkel und Lineal, Elem. Math. 17 (1962) 54–58; Halter-Koch, Über Konstruktionen mit Zirkel, Lineal und Winkeleinteilungen, Elem. Math. 42 (1987) 47–150; Duncan, Barnier, Amer. Math. Monthly 89 (1982) 693; Gleason, Amer. Math. Monthly 95 (1988) 185–194, 911; Grölz, Zur algebraischen Kennzeichnung geometrischer Konstruktionen – ein elementarer Zugang, Math. Semesterberichte 36 (1989) 227–243; DeTemple, Amer. Math. Monthly 98 (1991) 97–108.]

[5] Disquisitiones Arithmeticae 1796; dort wird auch 14.7 behauptet, aber Gauß hat nie einen Beweis dafür publiziert. Vgl. Lützen, Why was Wantzel overlooked ..., Historia Math. 36, 2009, 374–394.

15. Zerfällungskörper

Wir konstruieren Körper, in welchen ein vorgegebenes Polynom Nullstellen hat.

15.1 Satz (Kronecker, Cauchy)**.** *Sei K ein Körper, und $f \in K[x]$ sei irreduzibel vom Grad n. Wir setzen $L := K[x]/fK[x]$ und identifizieren $k \in K$ mit $\bar{k} := k + fK[x] \in L$. Dann ist $L|K$ eine Körpererweiterung vom Grad n, und $\bar{x} := x + fK[x] \in L$ ist eine Nullstelle von f.*

Beweis. $K[x]$ ist ein Hauptidealring nach 11.2, also ist $fK[x]$ ein maximales Ideal in $K[x]$ nach 11.5(i). Nach 10.4 ist L ein Körper.

Ferner ist $\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ ist eine K-Basis von L, also $[L : K] = n$, und $f(\bar{x}) = f(x + fK[x]) = f + fK[x] = fK[x] = \bar{0}$ in L. □

Satz 15.1 verallgemeinert den Übergang von $K = \mathbb{R}$ zu $L = \mathbb{C} = \mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$.

15.2 Definition. Sei $L|K$ eine Körpererweiterung und $f \in K[x]$ von Grad $n > 0$. Man nennt L einen Zerfällungskörper von f über K, falls gilt:

(i) $f = c\prod_{j=1}^{n}(x - a_j)$ mit $c \in K, a_j \in L$ und

(ii) $L = K(a_1, \ldots, a_n)$.

Bedingung (i) besagt, dass f über L in Linearfaktoren zerfällt, und nach (ii) ist L nicht unnötig groß.

Beispiele: $\mathbb{C} = \mathbb{R}(i)$ ist ein Zerfällungskörper von $x^2 + 1$ über $\mathbb{R}$, und $\mathbb{Q}(i) = \mathbb{Q} \oplus i\mathbb{Q}$ ist ein Zerfällungskörper von $x^2 + 1$ über $\mathbb{Q}$.

15.3 Satz. *Sei K ein Körper und $f \in K[x]$ vom Grad $n > 0$. Dann existiert ein Zerfällungskörper L von f über K mit $[L : K] \mid n!$.*

Beweis. Dies gilt für $n = 1$, mit $L = K$. Wir verwenden Induktion nach n und setzen die Gültigkeit für Polynome vom Grad $< n$ voraus.

Ist f reduzibel, also $f = gh$ mit $g, h \in K[x]$ mit Graden $d, n-d < n$, so existieren nach Induktion ein Zerfällungskörper Z von g über K mit $[Z : K] \mid d!$ und ein Zerfällungskörper L von h über Z mit $[L : Z] \mid (n-d)!$. Wegen 15.2(ii) ist L auch ein Zerfällungskörper von $f = gh$ über K. Nach der Gradformel 13.3 ist $[L : K] = [L : Z] \cdot [Z : K]$ ein Teiler von $(n-d)! \cdot d!$, also auch von $\binom{n}{d}(n-d)!d! = n!$.

Ist f irreduzibel, so existiert nach 15.1 eine Körpererweiterung $E|K$ vom Grad n, sodass E eine Nullstelle a_1 von f enthält. Nach 13.6 ist $[K(a_1) : K] = \mathrm{Grad}(f) = n$, also $E = K(a_1)$. Nach 8.4(i) ist $f = (x - a_1) \cdot g$ mit $g \in E[x]$ vom Grad $n - 1$. Nach Induktion hat g einen Zerfällungskörper L über E mit $[L : E] \mid (n-1)!$. Sind $a_2, \ldots, a_t$ die Nullstellen von g in L, so gilt $L = E(a_2, \ldots, a_t) = K(a_1, \ldots, a_t)$. Daher ist L ein Zerfällungskörper von f über K, und $[L : K] = [L : E] \cdot [E : K]$ teilt $(n-1)!n = n!$. □

Die Eindeutigkeit des Zerfällungskörpers (bis auf K-Isomorphie) wird mit folgendem Lemma gezeigt:

15.4 Fortsetzungslemma. *Sei $\alpha : K \to E$ ein Homomorphismus zwischen Körpern K und E, und sei $\alpha^* : K[x] \to E[x]$ der induzierte Homomorphismus von Polynomringen, also $\alpha^*(\sum a_j x^j) := \sum \alpha(a_j) x^j$ für $a_j \in K$.*

(i) *Sei $f \in K[x]$ irreduzibel, sei $L|K$ eine Körpererweiterung, sei $a \in L$ eine Nullstelle von f und $a' \in E$ eine Nullstelle von $\alpha^*(f)$. Dann hat α genau eine Fortsetzung zu einem Homomorphismus $\beta : K(a) \to E$ mit $\beta(a) = a'$.*

(ii) *Sei $g \in K[x]$, sei L ein Zerfällungskörper von g über K und L' ein Zerfällungskörper von $\alpha^*(g)$ über E. Dann hat α eine Fortsetzung zu einem Homomorphismus $\gamma : L \to L'$.*

Beweis. (i) Man darf annehmen, dass f normiert ist. Dann ist f das Minimalpolynom von a über K, und $\alpha^*(f)$ ist das Minimalpolynom von a' über $K' := \alpha(K) \subseteq E$. Nach 13.6 gibt es einen K-Isomorphismus $K(a) \to K[x]/fK[x]$ mit $a \mapsto x + fK[x]$ und einen K'-Isomorphismus $K'(a') \to K'[x]/\alpha^*(f)K'[x]$ mit $a' \mapsto x + \alpha^*(f)K'[x]$. Ferner liefert α^* einen Homomorphismus $K[x]/fK[x] \to K'[x]/\alpha^*(f)K'[x]$. Die Komposition $K(a) \to K[x]/fK[x] \to K'[x]/\alpha^*(f)K'[x] \leftarrow K'(a')$ ist ein Homomorphismus $\beta : K(a) \to K'(a') \subseteq E$ mit $\beta(a) = a'$ und $\beta|_K = \alpha$. Durch diese beiden Bedingungen ist β eindeutig festgelegt.
(ii) Wir verwenden Induktion nach $n := \mathrm{Grad}(g)$. Für $n = 1$ gilt $L = K = L'$, und wir setzen $\gamma = \alpha$. Sei jetzt $n > 1$.

L enthält eine Nullstelle a von g, und das Minimalpolynom m_a von a über K ist ein Teiler von g. Daher ist $\alpha^*(m_a)$ ein Teiler von $\alpha^*(g)$ im Polynomring $\alpha(K)[x] \subseteq E[x]$, und L' enthält eine Nullstelle a' von $\alpha^*(m_a)$. Nach (i), angewandt mit $f = m_a$, hat α eine Fortsetzung $\beta : K(a) \to L'$ mit $\beta(a) = a'$. Nach 8.4(i) ist $g = (x-a) \cdot h$ mit $h \in K(a)[x]$ und $\mathrm{Grad}(h) = n-1$. Es folgt $\alpha^*(g) = \beta^*(g) = \beta^*((x-a) \cdot h) = (x-a') \cdot \beta^*(h)$. Ferner ist L bzw. L' ein Zerfällungskörper von h bzw. $\beta^*(h)$ über $K(a)$ bzw. $E(a')$. Nach Induktion hat β (also auch α) eine Fortsetzung zu einem Homomorphismus $\gamma : L \to L'$. □

15.5 Korollar. *Je zwei Zerfällungskörper L und L' eines Polynoms g über einem Körper K sind K-isomorph zueinander. (Daher darf man von dem Zerfällungskörper von g über K sprechen, er ist eindeutig bis auf K-Isomorphie.)*

Beweis. Setze $E = K$ und $\alpha = \mathrm{id}_K$ in 15.4(ii). Man erhält K-Homomorphismen $L \to L'$ und $L' \to L$, die beide injektiv sind. Die Grade $[L : K]$ und $[L' : K]$ sind endlich (nach 15.2) und erfüllen $[L : K] \leq [L' : K] \leq [L : K]$ wegen der Injektivität. Daher sind die Grade gleich, und die K-Homomorphismen sind bijektiv. □

15.6 Bemerkung (Algebraisch abgeschlossene Körper)**.** Ein Körper K heißt algebraisch abgeschlossen, falls jedes nichtkonstante Polynom aus $K[x]$ eine Nullstelle in K hat. Äquivalente Bedingungen: K ist Zerfällungskörper jedes nichtkonstanten Polynoms aus $K[x]$, oder: jedes irreduzible Polynom aus $K[x]$ hat den Grad 1, oder: K hat keine endliche echte Körpererweiterung (vgl. ÜA 28a).

Beispiele: $\mathbb{C}$ ist algebraisch abgeschlossen (sog. Fundamentalsatz der Algebra; siehe 18.11 oder Fine-Rosenberger, The fundamental theorem of algebra, Springer 1997 oder

Wolfart, Einführung in die Zahlentheorie und Algebra, Vieweg 2011, S. 145). Der Körper $A := \{a \in \mathbb{C} \mid a \text{ ist algebraisch über } \mathbb{Q}\}$ ist abzählbar und algebraisch abgeschlossen.

Ist $L|K$ eine Körpererweiterung, ist jedes Element von L algebraisch über K, und ist L algebraisch abgeschlossen, so nennt man L einen algebraischen Abschluss von K. Nach Steinitz 1910 hat jeder Körper K einen algebraischen Abschluss, und alle algebraischen Abschlüsse von K sind K-isomorph zueinander. $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$, und A ist ein algebraischer Abschluss von $\mathbb{Q}$.

16. Anwendung: Endliche Körper

Als Anwendung von 15.5 erhält man:

16.1 Satz (E. H. Moore 1893)**.**
(a) *Ist K ein endlicher Körper, so ist $|K| > 1$ eine Primzahlpotenz.*
(b) *Ist $q > 1$ eine Potenz einer Primzahl p, so existiert bis auf Isomorphie genau ein Körper mit q Elementen, nämlich der Zerfällungskörper von $x^q - x$ über $\mathbb{Z}_p$.*

Man bezeichnet den Körper in 16.1(b) mit $\mathbb{F}_q$ oder $\mathrm{GF}(q)$ (für Galois Field).

Beweis. (a) K hat den Primkörper $\mathbb{F}_p = \mathbb{Z}_p$ für eine Primzahl p, siehe 13.1. Mit dem Grad $n := [K : \mathbb{F}_p] \geq 1$ gilt dann $K \cong {\mathbb{F}_p}^n$ als $\mathbb{F}_p$-Vektorräume, also $|K| = |{\mathbb{F}_p}^n| = p^n$.

(b) Sei K ein Körper mit $|K| = q$. Dann ist $|K^*| = q-1$, also $k^{q-1} = 1$ für alle $k \in K^*$ (nach 1.6) und daher $k^q = k$ für alle $k \in K$. Demnach ist K die Menge aller Nullstellen von $x^q - x$ (in jeder Körpererweiterung von K), also ein Zerfällungskörper von $x^q - x$ über $\mathbb{F}_p$. Nach 15.5 ist K bis auf Isomorphie eindeutig bestimmt.

Für die Existenz zeigen wir, dass der Zerfällungskörper Z von $x^q - x$ über $\mathbb{F}_p$ genau q Elemente hat. Die Nullstellen von $x^q - x$ in Z bilden einen Teilkörper von Z (weil $z \mapsto z^q$ additiv und multiplikativ ist). Daher ist Z die Menge all dieser Nullstellen, also $|Z| \leq q$ nach 8.4(ii). Hätte $x^q - x$ eine mehrfache Nullstelle $c \in Z$, so wäre $(x-c)^2 \mid x^q - x = (x-c)^q + c^q - x$, also $(x-c)^2 \mid c^q - x$, ein Widerspruch. Also gilt $|Z| = q$. □

16.2 Satz. *Sei p eine Primzahl und seien $a, b \in \mathbb{N}$. Genau dann hat $\mathbb{F}_{p^b}$ einen, und dann auch nur einen, zu $\mathbb{F}_{p^a}$ isomorphen Teilkörper, wenn a ein Teiler von b ist.*

Beweis. Wir benutzen die Äquivalenz $p^a - 1 \mid p^b - 1 \Leftrightarrow a \mid b$, siehe Beweis zu 9.2.

Hat $\mathbb{F}_{p^b}$ einen Teilkörper mit p^a Elementen, dann hat $\mathbb{F}_{p^b}^*$ eine Untergruppe der Ordnung $p^a - 1$. Mit 1.6 folgt $p^a - 1 \mid p^b - 1$, also $a \mid b$. Ein solcher Teilkörper ist eindeutig bestimmt, weil $\mathbb{F}_{p^b}^*$ zyklisch ist, siehe 8.5 und 1.12.

Sei jetzt $a \mid b$. Dann gilt $p^a - 1 \mid p^b - 1$ und $x^{p^a-1} - 1 \mid x^{p^b-1} - 1$ (geometrische Summe) und daher $x^{p^a} - x \mid x^{p^b} - x$. Deshalb enthält der Zerfällungskörper $\mathbb{F}_{p^b}$ von $x^{p^b} - x$ über $\mathbb{F}_p$ einen Zerfällungskörper von $x^{p^a} - x$ über $\mathbb{F}_p$, also eine Kopie von $\mathbb{F}_{p^a}$. □

16.3 Korollar. *Ist $q > 1$ eine Primzahlpotenz und $n \in \mathbb{N}$, so enthält $\mathbb{F}_q[x]$ ein irreduzibles Polynom vom Grad n.*

Beweis. Nach 8.5 wird $\mathbb{F}_{q^n}{}^*$ von einem Element a erzeugt. Nach 16.2 ist $\mathbb{F}_q$ ein Teilkörper von $\mathbb{F}_{q^n}$, und daher $\mathbb{F}_{q^n} = \mathbb{F}_q(a)$. Das Minimalpolynom von a über $\mathbb{F}_q$ ist irreduzibel und hat den Grad n, siehe 13.6. □

16.4 Satz. *Sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist* $\operatorname{Aut}\mathbb{F}_{p^n}$ *die zyklische Gruppe der Ordnung n, welche von dem sog. Frobenius-Automorphismus $\varphi : a \mapsto a^p$ erzeugt wird.*

Beweis. φ ist multiplikativ, additiv und injektiv (denn $a^p = 0 \Rightarrow a = 0$), also $\varphi \in \operatorname{Aut}\mathbb{F}_{p^n}$ wegen der Endlichkeit von $\mathbb{F}_{p^n}$. Es gilt $\varphi^n(a) = a^{p^n} = a$ für alle $a \in \mathbb{F}_{p^n}$, also $\varphi^n = \mathrm{id}$. Ferner hat $\varphi^k(x) = x^{p^k} = x$ höchstens p^k Lösungen nach 8.4(ii), daher ist $\varphi^k \neq \mathrm{id}$ für $1 \leq k < n$. Also hat φ die Ordnung n.

Daher genügt es, $|\operatorname{Aut}\mathbb{F}_{p^n}| \leq n$ nachzuweisen. Nach 8.5 gilt $\mathbb{F}_{p^n}{}^* = \langle a \rangle$ für ein geeignetes Element a, also erst recht $\mathbb{F}_{p^n} = \mathbb{F}_p(a)$. Nach 13.6 hat das Minimalpolynom $f \in \mathbb{F}_p[x]$ von a den Grad n, also höchstens n Nullstellen in $\mathbb{F}_{p^n}$ nach 8.4(ii). Für $\alpha \in \operatorname{Aut}\mathbb{F}_{p^n}$ gilt $f(\alpha(a)) = \alpha(f(a)) = \alpha(0) = 0$, weil α jedes Element des Primkörpers $\mathbb{F}_p$ festlässt. Daher gibt es höchstens n Möglichkeiten für $\alpha(a)$. Weil α durch $\alpha(a)$ eindeutig festgelegt ist, gibt es höchstens n Automorphismen $\alpha \in \operatorname{Aut}\mathbb{F}_{p^n}$. □

16.5 Beispiele. Das Polynom $x^2 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$, siehe ÜA 24(a). Also ist $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)\mathbb{F}_2[x] = \{0, 1, \bar{x}, \bar{x} + 1\}$ mit $\bar{x}^2 = \bar{x} + 1$.

Der Körper $\mathbb{F}_9$ ist der Zerfällungskörper von $x^9 - x$ über $\mathbb{F}_3$; man hat die Zerlegung $x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$, und $x^2 + 1$ und $x^2 \pm x - 1$ sind die irreduziblen quadratischen normierten Polynome in $\mathbb{F}_3[x]$. Demnach gilt $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+1)\mathbb{F}_3[x] = \mathbb{F}_3 \oplus \mathbb{F}_3\bar{x}$ mit $\bar{x}^2 = -1$; vgl. $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$.

[Die Polynome (Trinome) $x^{10} + x^3 + 1$, $x^{127} + x + 1$ und $x^{521} + x^{32} + 1$ sind irreduzibel in $\mathbb{F}_2[x]$ und liefern daher Körper mit 2^{10} bzw. 2^{127} bzw. 2^{521} Elementen.]

17. Normalität und Separabilität

17.1 Definition. Eine Körpererweiterung $L|K$ heißt normal, falls L ein Zerfällungskörper über K eines Polynoms $f \in K[x]$ ist.

Dann ist $L|K$ endlich, und für jeden Zwischenkörper Z von $L|K$ ist auch $L|Z$ normal (weil L auch ein Zerfällungskörper von f über Z ist).

17.2 Satz. *Für jede endliche Körpererweiterung $L|K$ sind äquivalent:*

(i) *$L|K$ ist normal.*

(ii) *Jedes irreduzible Polynom $g \in K[x]$ mit einer Nullstelle in L ist ein Produkt von Linearfaktoren in $L[x]$.*

Beweis. (i) ⇒ (ii): L ist Zerfällungskörper eines Polynoms $f \in K[x]$. Sei $g \in K[x]$ irreduzibel mit einer Nullstelle $a \in L$, und sei a' eine weitere Nullstelle von g in einem Erweiterungskörper von L (etwa in einem Zerfällungskörper von g über L). 13.6 mit Beweis liefert einen K-Isomorphismus $\alpha : K(a) \to K(a')$ mit $\alpha(a) = a'$.

L ist auch ein Zerfällungskörper von f über $K(a)$, und $L(a')$ ist ein Zerfällungskörper von f über $K(a')$. Nach 15.4(ii) hat α^{-1} eine Fortsetzung zu einem K-Homomorphismus $\gamma : L(a') \to L$. Weil γ injektiv ist, folgt $[L(a') : K] \leq [L : K]$, also $L(a') = L$ und dann $a' \in L$. Daher ist g ein Produkt von Linearfaktoren in $L[x]$.

(ii) $\Rightarrow$ (i): Weil $L|K$ endlich ist, existieren $a_j \in L$ mit $L = K(a_1, a_2, \ldots, a_t)$. Wegen (ii) zerfällt das (irreduzible) Minimalpolynom $m_j \in K[x]$ von a_j in $L[x]$ in Linearfaktoren, also auch das Produkt $f := \prod_{j=1}^{t} m_j \in K[x]$. Wegen $L = K(a_1, a_2, \ldots, a_t)$ ist L ein Zerfällungskörper von f über K. □

17.3 Beispiele. Jede quadratische Körpererweiterung $L|K$ ist normal.

$\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal, weil das irreduzible Polynom $x^3-2 \in \mathbb{Q}[x]$ genau eine reelle Nullstelle hat, also nur eine Nullstelle in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Der zugehörige Zerfällungskörper ist $\mathbb{Q}(\sqrt[3]{2}, c\sqrt[3]{2}, c^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, c)$ mit der Einheitswurzel $c = e^{2\pi i/3}$ der Ordnung 3.

Die Normalität ist nicht transitiv: $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ sind quadratisch, also normal, aber $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ ist nicht normal (weil nicht alle Nullstellen von $x^4 - 2$ reell sind).

17.4 Definition. Sei K ein Körper. Ein Polynom $f \in K[x]$ vom Grad $n \geq 0$ heißt separabel, falls f in einem geeigneten Erweiterungskörper von K genau n verschiedene Nullstellen hat (etwa in einem Zerfällungskörper, d. h. die a_j in 15.2(i) sollen paarweise verschieden sein).[6] Jeder Teiler eines separablen Polynom ist separabel.

Eine endliche Körpererweiterung $L|K$ heißt separabel, falls für jedes $a \in L$ das Minimalpolynom $m_a \in K[x]$ von a separabel ist.

Für jeden Zwischenkörper Z von $L|K$ sind dann auch $Z|K$ und $L|Z$ separabel (weil das Minimalpolynom von a über Z ein Teiler des Minimalpolynoms über K ist).

[Im Beweis zu 16.1 wurde gezeigt, dass $x^q - x \in \mathbb{F}_p[x]$ für jede Potenz $q > 1$ der Primzahl p separabel ist.]

17.5 Beispiel. Sei p eine Primzahl, sei $L := \mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$ in der Variablen t, und sei $K := \mathbb{F}_p(t^p)$. Dann gilt $L = K(t)$. Die Körpererweiterung $L|K$ hat den Grad p und ist nicht separabel, weil das Element t über K das Minimalpolynom $x^p - t^p = (x-t)^p$ hat (dieses Polynom ist irreduzibel in $K[x]$, weil die normierten Teiler dieses Polynoms in $L[x]$ von der Form $(x-t)^j$ sind und $t^j \notin K$ für $1 \leq j < p$).

Dieses Beispiel ist nicht untypisch:

17.6 Lemma. *Sei K ein Körper, und $f \in K[x]$ sei irreduzibel und nicht separabel. Dann hat K eine Charakteristik $p \neq 0$, und $f = g(x^p)$ für ein $g \in K[x]$.*

Beweis. Ein Zerfällungskörper L von f über K enthält ein Element a mit $(x-a)^2 \mid f$. Wir dürfen annehmen, dass f normiert ist. Wegen der Irreduzibilität ist f das Minimalpolynom von a über K. Sei $f = \sum_{j=0}^{n} a_j x^j$ mit $a_j \in K$ und $\mathrm{Grad}(f) = n$. Das Einsetzen von $x + a$ für x ist ein Ringautomorphismus von $L[x]$, daher ist

$$x^2 \mid f(x+a) = \sum_{j=0}^{n} a_j (x+a)^j = \sum_{j=0}^{n} \sum_{k=0}^{j} \binom{j}{k} a_j a^{j-k} x^k.$$

[6] Manchmal wird dies nur für die in $K[x]$ irreduziblen Faktoren von f gefordert.

Insbesondere hat x^1 in diesem Polynom den Koeffizienten $0 = \sum_{j=1}^{n} \binom{j}{1} a_j a^{j-1}$, also ist a eine Nullstelle von $\sum_{j=1}^{n} j a_j x^{j-1} \in K[x]$ (mit anderen Worten: a ist auch eine Nullstelle der Ableitung von f, siehe ÜA 32). Weil das Minimalpolynom f von a über K den Grad n hat, folgt $ja_j = 0$ für $1 \leq j \leq n$. Wegen $a_n \neq 0$ und $na_n = 0$ hat K eine Charakteristik $p \neq 0$, und für $p \nmid j$ ist $a_j = 0$. Demnach ist $f = \sum_{j \leq n/p} a_{jp} x^{jp} = g(x^p)$ mit $g := \sum_{j \leq n/p} a_{jp} x^j \in K[x]$. □

Inseparabilität ist selten:

17.7 Korollar. *Eine endliche Körpererweiterung $L|K$ ist jedenfalls dann separabel, wenn K die Charakteristik 0 hat, oder wenn der Grad $[L : K]$ nicht durch die Charakteristik von K teilbar ist.*

Beweis. Hat ein Element von L ein nicht separables Minimalpolynom $f \in K[x]$, so hat K nach 17.6 eine Charakteristik $p \neq 0$, und $\mathrm{Grad}(f)$ ist durch p teilbar. Nach 13.6 und 13.3 ist $\mathrm{Grad}(f)$ ein Teiler von $[L : K]$. □

[Wir beweisen nicht die Transitivität der Separabilität; nach 18.5 sind Zerfällungskörper von separablen Polynomen separabel.]

18. Galois-Theorie

[Wir variieren den Zugang von Geck, Algebra: Gruppen, Ringe, Körper, edition delkhofen 2014; siehe auch Geck, Amer. Math. Monthly 121 (2014) 637–639. Geck lässt § 17 weg und definiert Galois-Erweiterungen durch 18.5(iii).]

Zunächst ein Lemma aus der Linearen Algebra:

18.1 Lemma. *Sei V ein Vektorraum über einem unendlichen Körper K. Dann ist V nicht die Vereinigung von endlich vielen echten Unterräumen von V.*

Beweis. Sei $V = U_1 \cup U_2 \cup \cdots \cup U_t$ mit Unterräumen $U_j < V$ und mit minimalem t. Dann gilt $t \geq 2$ und $U_t \not\subseteq U_1 \cup \cdots \cup U_{t-1}$, und es existieren Vektoren $v \in V \setminus U_t$ und $w \in U_t \setminus (U_1 \cup \cdots \cup U_{t-1})$. Zu jedem $k \in K$ existiert ein Index j mit $v + kw \in U_j$. Weil K unendlich ist, existieren zwei verschiedene $k, k' \in K$ und ein Index j mit $v + kw, v + k'w \in U_j$ (Schubfachprinzip). Differenzbildung liefert $(k - k')w \in U_j$, also $w \in U_j$ und daher $j = t$. Wegen $v + kw \in U_t$ und $w \in U_t$ folgt $v \in U_t$, ein Widerspruch zur Wahl von v. □

18.2 Definition. Ist $L|K$ eine Körpererweiterung, so nennt man die Gruppe

$$\mathrm{Aut}(L|K) := \{\alpha \in \mathrm{Aut}\, L \mid \alpha|_K = \mathrm{id}_K\} = \{\alpha \in \mathrm{Aut}\, L \mid \alpha \text{ ist } K\text{-linear}\}$$

aller K-Automorphismen von L die (relative) Automorphismengruppe[7] von $L|K$; vgl. 13.5. Die Galois-Theorie studiert Körpererweiterungen mit Hilfe ihrer relativen Automorphismengruppen.

[7] manchmal auch die Galois-Gruppe

18.3 Lemma. *Sei $L|K$ eine endliche Körpererweiterung und $G = \mathrm{Aut}(L|K)$. Dann gilt $|G| \leq [L : K]$ und es existiert ein $a \in L$ mit $|G(a)| = |G|$.*

Beweis. Wir zeigen zunächst, dass G endlich ist. Weil $L|K$ endlich ist, existieren Elemente $a_j \in L$ mit $L = K(a_1, a_2, \ldots, a_t)$, und jedes a_j ist algebraisch über K (nach ÜA 32(a)), also Nullstelle eines Polynoms $p_j \in K[x] \setminus \{0\}$ vom Grad höchstens $n := [L : K]$. Für jedes $g \in G$ gilt $p_j(g(a_j)) = g(p_j(a_j)) = g(0) = 0$, also ist $g(a_j)$ eine von den höchstens n Nullstellen von p_j (nach 8.4(ii)). Der K-Automorphismus g ist durch seine Bilder $g(a_1), \ldots, g(a_t)$ eindeutig festgelegt. Also gilt $|G| \leq n^t$. [Wir wollen $|G| \leq n$ zeigen; man kann nicht immer $t = 1$ wählen, siehe Bemerkung nach 18.12.]

Für jedes $g \in G$ ist $\mathrm{Fix}\, g := \{l \in L \mid g(l) = l\}$ ein Zwischenkörper von $L|K$, also insbesondere ein K-Unterraum von L, und für $g \neq 1$ ist $\mathrm{Fix}\, g \neq L$.

Ist K endlich, so auch L, und die multiplikative Gruppe L^* ist zyklisch nach 8.5, also $L^* = \langle a \rangle$ für ein $a \in L$; dann gilt $G_a = \{1\}$. Ist K unendlich, so ist $L \setminus \bigcup_{1 \neq g \in G} \mathrm{Fix}\, g \neq \emptyset$ nach 18.1, und für jedes a in dieser Differenzmenge gilt $G_a = \{1\}$. Aus $G_a = \{1\}$ folgt $|G| = |G : G_a| = |G(a)|$ wegen 2.7.

Für das Minimalpolynom m_a über K eines solchen Elements a gilt $x - a \mid m_a$ im Polynomring $L[x]$ und daher auch $x - g(a) \mid m_a$ für jedes $g \in G$. Diese Linearfaktoren sind irreduzibel in dem faktoriellen Ring $L[x]$, siehe 11.6, daher folgt $\prod_{b \in G(a)}(x - b) \mid m_a$. Also ist $|G| = |G(a)| \leq \mathrm{Grad}(m_a) = [K(a) : K] \leq [L : K]$; die letzte Gleichung gilt nach 13.6. □

[Nach Białynicki-Birula, Browkin, Schinzel, On the representation of fields as finite unions of subfields, Colloq. Math. 7 (1959) 31–32, ist kein Körper die Vereinigung von endlich vielen echten Teilkörpern. Dies könnte man statt 18.1 im Beweis zu 18.3 verwenden, als overkill. Die Gruppenordnung $|G| = [L : \mathrm{Fix}\, G]$ ist sogar ein Teiler von $[L : K]$, siehe 18.13 und 18.5.]

18.4 Definition. Eine Galois-Erweiterung ist eine endliche Körpererweiterung $L|K$, welche normal und separabel ist. Die zugehörige Gruppe $\mathrm{Aut}(L|K)$ wie in 18.2 wird auch als Galois-Gruppe $\mathrm{Gal}(L|K)$ von $L|K$ bezeichnet (nach Évariste Galois, 1811–1832).

Erste Beispiele: Hat K nicht die Charakteristik 2, so ist jede quadratische Erweiterung von K separabel (nach 17.7) und normal (nach 17.3), also eine Galois-Erweiterung. Insbesondere gilt dies für $\mathbb{C}|\mathbb{R}$, und $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, {}^-\}$. Hat K die Charakteristik 0, so sind die Galois-Erweiterungen von K genau die Zerfällungskörper von Polynomen aus $K[x]$, wegen 17.7.

18.5 Satz (Charakterisierung[8] von Galois-Erweiterungen)**.** *Sei $L|K$ eine endliche Körpererweiterung und $G = \mathrm{Aut}(L|K)$. Dann sind äquivalent:*

(i) *$L|K$ ist eine Galois-Erweiterung.*

(ii) *L ist ein Zerfällungskörper über K eines separablen Polynoms $f \in K[x]$.*

[8] Die Punkte (ii)–(iv) sind wichtig. Eine weitere Charakterisierung findet man in 18.13.

(iii) $|G| = [L : K]$.

(iv) *K stimmt überein mit dem Fixkörper* $\operatorname{Fix} G := \{l \in L \mid \forall g \in G : g(l) = l\}$ *von G.*

(v) *Für jedes $a \in L$ gehört das Polynom $\prod_{b \in G(a)}(x - b)$ zu $K[x]$.*

(vi) *Für jedes $a \in L$ ist $\prod_{b \in G(a)}(x - b)$ das Minimalpolynom von a über K.*

(vii) *Es existiert ein $a \in L$ mit $|G(a)| = [L : K]$.*

(viii) *Es gilt $L = K[a]$ für ein Element $a \in L$, dessen Minimalpolynom m_a über K separabel ist und in $L[x]$ in Linearfaktoren zerfällt.*

Beweis. (i) $\Rightarrow$ (ii): Weil $L|K$ endlich ist, existieren $a_j \in L$ mit $L = K(a_1, a_2, \ldots, a_t)$, und jedes a_j ist algebraisch über K (nach ÜA 32(a)). Sei f_j das Minimalpolynom von a_j über K. Wegen (i) und 17.2 ist f_j ein Produkt von verschiedenen Linearfaktoren in $L[x]$. Jedes f_j ist das Minimalpolynom über K von jeder seiner Nullstellen; daher haben verschiedene f_j keine Nullstelle gemeinsam. Also ist das Produkt der verschiedenen Polynome in der Liste $f_1, f_2, \ldots, f_t$ (also das kgV der f_j) ein separables Polynom $f \in K[x]$, und $L = K(a_1, \ldots, a_t)$ ist ein Zerfällungskörper von f über K.

(ii) $\Rightarrow$ (iii): Seien $b_1, \ldots, b_s$ die verschiedenen Nullstellen von f in L, sei $K_0 = K$ und $K_j = K(b_1, b_2, \ldots, b_j)$, also $K_s = L$. Ferner sei $m_{j+1} \in K_j[x]$ das Minimalpolynom von b_{j+1} über K_j.

Für jedes $g \in G$ ist $g|_{K_j} : K_j \to L$ ein K-Homomorphismus, und $g|_{K_{j+1}}$ ist eine Fortsetzung davon; dies motiviert die folgenden Überlegungen.

Sei $\alpha : K_j \to L$ ein K-Homomorphismus und $\beta : K_{j+1} \to L$ eine Fortsetzung von α. Dann ist $\beta(b_{j+1})$ eine Nullstelle von $\alpha^*(m_{j+1})$ mit der Notation von 15.4, denn $0 = \beta(0) = \beta(m_{j+1}(b_{j+1})) = \beta^*(m_{j+1})(\beta(b_{j+1})) = \alpha^*(m_{j+1})(\beta(b_{j+1}))$. Wegen $m_{j+1} \mid f$ gilt $\alpha^*(m_{j+1}) \mid \alpha^*(f) = f$. Weil f separabel ist, hat $\alpha^*(m_{j+1})$ in L genau $\operatorname{Grad}(\alpha^*(m_{j+1})) = \operatorname{Grad}(m_{j+1}) = [K_{j+1} : K_j]$ viele Nullstellen. Nach 15.4(i) hat α genau $[K_{j+1} : K_j]$ Fortsetzungen $\beta : K_{j+1} \to L$.

Daher hat $\mathrm{id}_K : K \to L$ genau $\prod_{j=0}^{s-1}[K_{j+1} : K_j] = [L : K]$ Fortsetzungen zu einem K-Homomorphismus $\beta : L \to L$; weil β injektiv und $[L : K]$ endlich ist, ist β bijektiv, also $\beta \in G$. Daher ist $|G| = [L : K]$.

(iii) $\Rightarrow$ (iv): Der Fixkörper $K' := \operatorname{Fix} G$ ist ein Zwischenkörper von $L|K$. Es gilt $G \leq \operatorname{Aut}(L|K')$ nach Definition von K' und $\operatorname{Aut}(L|K') \leq \operatorname{Aut}(L|K) = G$ wegen $K \subseteq K'$, also $\operatorname{Aut}(L|K') = G$. Mit 18.3 folgt $|G| \leq [L : K'] \leq [L : K]$, wegen (iii) also $[L : K'] = [L : K]$ und dann $K = K'$.

(iv) $\Rightarrow$ (v): Die Linearfaktoren von $\prod_{b \in G(a)}(x - b)$ werden von jedem Element aus G untereinander permutiert. Also liegen die Koeffizienten dieses Polynoms in $\operatorname{Fix} G$, also in K wegen (iv).

(v) $\Rightarrow$ (vi): Für jedes $a \in L$ ist $x - a$ ein Teiler des Minimalpolynoms m_a von a über K, also auch $x - g(a) \mid m_a$ für jedes $g \in G$. Diese Linearfaktoren sind irreduzibel in dem faktoriellen Ring $L[x]$, siehe 11.6, daher ist $\prod_{b \in G(a)}(x - b) \in K[x]$ ein Teiler von m_a. Weil

$\prod_{b\in G(a)}(x-b)$ die Nullstelle a hat, ist m_a auch ein Teiler dieses normierten Polynoms, also gleich diesem Polynom. [Oder: weil m_a irreduzibel ist]

(vi) $\Rightarrow$ (i): Die in (vi) angegebenen Minimalpolynome sind separabel, also ist $L|K$ separabel. Sei $L = K(a_1, a_2, \ldots, a_t)$ wie oben. Dann ist L ein Zerfällungskörper von $\prod_{j=1}^{t}\prod_{b\in G(a_j)}(x-b) \in K[x]$ über K, also ist $L|K$ auch normal.

(vii) $\Leftrightarrow$ (iii): dies folgt mit 18.3, weil $|G(a)| \le |G| \le [L:K]$.

(vii) $\Rightarrow$ (viii): Aus (vii) folgt (vi), wie schon gezeigt wurde. Wegen (vi) ist das Minimalpolynom m_a von a über K separabel und zerfällt wie in (viii) verlangt. Mit 13.6 folgt $[K[a]:K] = \mathrm{Grad}(m_a) = |G(a)| = [L:K]$, also $K[a] = L$.

(viii) $\Rightarrow$ (ii): wähle $f = m_a$. □

Die Separabilität in 18.5(ii), (vii) ist notwendig: im Beispiel 17.5 ist $\mathrm{Aut}(L|K) = \{1\}$.

18.6 Hauptsatz der Galois-Theorie. *Sei $L|K$ eine Galois-Erweiterung und $G = \mathrm{Aut}(L|K)$. Dann sind die zwei Abbildungen*

$$Z \mapsto \mathrm{Aut}(L|Z) \quad \textit{und}$$
$$H \mapsto \mathrm{Fix}\, H := \{a \in L \mid \forall h \in H : h(a) = a\}$$

zueinander inverse Bijektionen zwischen der Menge aller Zwischenkörper Z von $L|K$ und der Menge aller Untergruppen H von G (sog. Galois-Korrespondenz).

Für jeden solchen Zwischenkörper Z ist auch $L|Z$ eine Galois-Erweiterung, und es gilt $[L:Z] = |\mathrm{Aut}(L|Z)|$.

Beweis. Für jeden Zwischenkörper Z ist $L|Z$ normal (nach 17.1) und separabel (nach 17.4), also eine Galois-Erweiterung, und $[L:Z] = |\mathrm{Aut}(L|Z)|$ gilt nach 18.5(iii).

Weiter ist $H := \mathrm{Aut}(L|Z)$ eine Untergruppe von G. Nach 18.5(iv), angewandt auf $L|Z$, ist $Z = \mathrm{Fix}\, H = \mathrm{Fix}\,\mathrm{Aut}(L|Z)$.

Für jede Untergruppe H von G ist $Z := \mathrm{Fix}\, H$ ein Zwischenkörper von $L|K$ und $H \le \mathrm{Aut}(L|Z)$; wir werden diese Inklusion zur Gleichheit verschärfen. Nach 18.5(iii), (viii), angewandt auf die Galois-Erweiterung $L|Z$, gilt $|\mathrm{Aut}(L|Z)| = [L:Z]$ und $L = Z[a]$ für ein $a \in L$. Das Polynom $f = \prod_{h\in H}(x - h(a))$ gehört zu $Z[x]$, weil jedes Element von H die Linearfaktoren von f untereinander permutiert und daher die Koeffizienten von f fixiert. Also ist das Minimalpolynom m_a von a über Z ein Teiler von f. Mit 13.6 folgt $|\mathrm{Aut}(L|Z)| = [L:Z] = [Z[a]:Z] = \mathrm{Grad}(m_a) \le \mathrm{Grad}(f) = |H|$. Daher gilt $H = \mathrm{Aut}(L|Z) = \mathrm{Aut}(L|\mathrm{Fix}\, H)$.

Daher sind die angegebenen Abbildungen invers zueinander, also beide bijektiv. □

18.7 Bemerkungen. (a) Die beiden Abbildungen in 18.6 kehren Inklusionen um, d. h.

$$Z_1 \subseteq Z_2 \Leftrightarrow \mathrm{Aut}(L|Z_2) \subseteq \mathrm{Aut}(L|Z_1) \quad \text{und} \quad H_1 \subseteq H_2 \Leftrightarrow \mathrm{Fix}\, H_2 \subseteq \mathrm{Fix}\, H_1.$$

Daher ist $\mathrm{Fix}(\langle H_1, H_2\rangle) = \mathrm{Fix}\, H_1 \cap \mathrm{Fix}\, H_2$, und $\mathrm{Fix}(H_1 \cap H_2) = K(\mathrm{Fix}\, H_1 \cup \mathrm{Fix}\, H_2)$ ist der von $\mathrm{Fix}\, H_1 \cup \mathrm{Fix}\, H_2$ erzeugte Teilkörper von L.

(b) In der Situation von 18.6 sei $g \in G$. Dann gilt

$$\begin{aligned}\operatorname{Fix}(gHg^{-1}) &= \{a \in L \mid ghg^{-1}(a) = a \text{ für alle } h \in H\} \\ &= \{a \in L \mid hg^{-1}(a) = g^{-1}(a) \text{ für alle } h \in H\} \\ &= \{a \in L \mid g^{-1}(a) \in \operatorname{Fix} H\} \\ &= \{a \in L \mid a \in g(\operatorname{Fix} H)\} = g(\operatorname{Fix} H)\end{aligned}$$

sowie

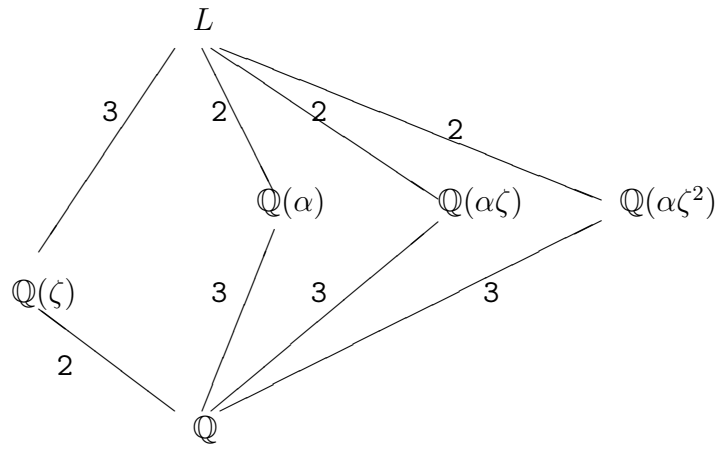
$$\begin{aligned}\operatorname{Aut}(L|g(Z)) &= \{h \in G \mid hg(z) = g(z) \text{ für alle } z \in Z\} \\ &= \{h \in G \mid g^{-1}hg \in \operatorname{Aut}(L|Z)\} = g \operatorname{Aut}(L|Z)g^{-1}.\end{aligned}$$

18.8 Beispiele. (a) Jede Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ von endlichen Körpern ist eine Galois-Erweiterung nach 18.5, denn $\mathbb{F}_{q^n}$ ist nach 16.1 (mit Beweis) ein Zerfällungskörper des separablen Polynoms $x^{q^n} - x$ über $\mathbb{F}_q$ (oder: $\mathbb{F}_q = \operatorname{Fix}\langle a \mapsto a^q\rangle$ und 18.5). Nach 16.4 ist die zugehörige Galois-Gruppe zyklisch, sie wird von $a \mapsto a^q$ erzeugt.

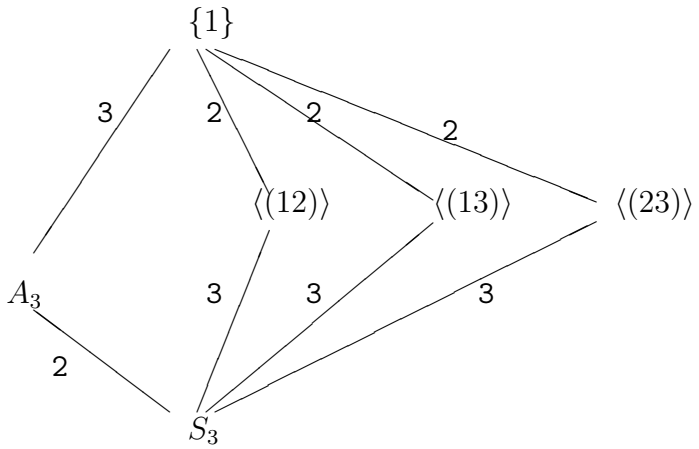
(b) Sei $a \in \mathbb{Q}$ keine dritte Potenz in $\mathbb{Q}$. Dann gilt

$$x^3 - a = (x - \alpha)(x - \alpha\zeta)(x - \alpha\zeta^2)$$

mit $\alpha = \sqrt[3]{a} \in \mathbb{R} \setminus \mathbb{Q}$ und $\zeta = e^{2\pi i/3} \in \mathbb{C}$. Der Körper $L := \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2) = \mathbb{Q}(\alpha, \zeta)$ ist ein Zerfällungskörper von $x^3 - a$ über $\mathbb{Q}$, und nach 18.5 ist $L|\mathbb{Q}$ eine Galois-Erweiterung. Es gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] = 2$ wegen $\zeta \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$ und $0 = \Phi_3(\zeta) = \zeta^2 + \zeta + 1$. Also ist $[L : \mathbb{Q}] = 6$. Wir kennen die folgenden Zwischenkörper:



Die zugehörige Galois-Gruppe $G = \operatorname{Aut}(L|\mathbb{Q})$ hat nach 18.5 die Ordnung 6 und enthält nach 18.6 mindestens drei Untergruppen der Ordnung 2 (nämlich $\operatorname{Aut}(L|\mathbb{Q}(\alpha\zeta^k))$ mit $k = 0, 1, 2$). Also ist $G \cong S_3 \cong D_6$. Das Diagramm



enthält alle Untergruppen von S_3 (mit umgekehrter Inklusion). Nach 18.6 enthält das vorige Diagramm alle Zwischenkörper von $L|\mathbb{Q}$, also alle Teilkörper von L.

18.9 Satz (Zusatz über Normalität zum Hauptsatz)**.** *Sei Z ein Zwischenkörper einer Galois-Erweiterung $L|K$. Genau dann ist $Z|K$ eine Galois-Erweiterung, wenn $N := \mathrm{Aut}(L|Z)$ ein Normalteiler von $G := \mathrm{Aut}(L|K)$ ist, und dann gilt $\mathrm{Aut}(Z|K) \cong G/N$.*

Beweis. Nach 18.6 ist $\mathrm{Fix}\, N = Z$, und 18.7(b) liefert $N \trianglelefteq G \Leftrightarrow g(\mathrm{Fix}\, N) = \mathrm{Fix}\, N$ für alle $g \in G \Leftrightarrow g(Z) = Z$ für alle $g \in G$.

Gilt $N \trianglelefteq G$, so ist $G|_Z := \{g_{|Z} \mid g \in G\} \leq \mathrm{Aut}(Z|K)$ und das Einschränken $G \to G|_Z : g \mapsto g|_Z$ ist ein Gruppen-Epimorphismus mit dem Kern $\mathrm{Aut}(L|Z) = N$, also $G|_Z \cong G/N$ nach 3.7. Nach 18.6 und 13.3 ist $|G|_Z| = |G||N|^{-1} = [L : K][L : Z]^{-1} = [Z : K]$. Mit 18.3 folgt $\mathrm{Aut}(Z|K) = G|_Z \cong G/N$, und $Z|K$ ist eine Galois-Erweiterung nach 18.5(iii).

Sei jetzt $Z|K$ eine Galois-Erweiterung, also normal, und $g \in G$. Ist $a \in Z$ und $m \in K[x]$ das Minimalpolynom von a über K, so gilt $m(g(a)) = g(m(a)) = g(0) = 0$, also $g(a) \in Z$ wegen 17.2. Dies impliziert $g(Z) \subseteq Z$ und dann $g(Z) = Z$, weil $[Z : K]$ endlich und g injektiv und K-linear ist. Also ist $N \trianglelefteq G$. □

Konsequenzen aus 18.5 und 18.6:

18.10 Lemma. *Sei $L|K$ eine endliche, separable Körpererweiterung. Dann existiert eine endliche Körpererweiterung $E|L$ derart, dass $E|K$ eine Galois-Erweiterung ist.*

Beweis. Es gilt $L = K(a_1, \ldots, a_t)$ mit geeigneten $a_j \in L$, und das Minimalpolynom f_j von a_j über K ist separabel. Das Produkt f der verschiedenen Polynome in der Liste $f_1, f_2, \ldots, f_t$ ist separabel (wie im Beweis zu 18.5, (i)⇒(ii)). Der Zerfällungskörper E von f über L ist auch ein Zerfällungskörper von f über K, wegen $L = K(a_1, \ldots, a_t)$. Wegen 18.5(ii) ist $E|K$ eine Galois-Erweiterung (die sog. Galois-Hülle von $L|K$). □

18.11 Satz (Sogenannter Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.*

Beweis. (E. Artin) Sei $L|\mathbb{C}$ eine endliche Körpererweiterung (wir werden $L = \mathbb{C}$ beweisen, vgl. 15.6). Dann ist auch $L|\mathbb{R}$ endlich. Nach 18.10 existiert eine Galois-Erweiterung $E|\mathbb{R}$ mit $L \subseteq E$. Sei S eine 2-Sylowgruppe von $G = \mathrm{Aut}(E|\mathbb{R})$. Dann ist

$$[\mathrm{Fix}\, S : \mathbb{R}] = \frac{[E : \mathbb{R}]}{[E : \mathrm{Fix}\, S]} = \frac{|G|}{|S|} \text{ ungerade, siehe 13.3 und 18.6.}$$

Also hat jedes $a \in \mathrm{Fix}\, S$ nach 13.6 und 13.3 ein Minimalpolynom m_a über $\mathbb{R}$ von ungeradem Grad. Nach dem Zwischenwertsatz aus der Analysis hat m_a eine reelle Nullstelle. Weil m_a reell irreduzibel ist, folgt $m_a = x - a$ und $a \in \mathbb{R}$. Demnach ist $\mathrm{Fix}\, S = \mathbb{R}$, und deshalb ist $G = S$ eine 2-Gruppe.

Daher ist auch $H := \mathrm{Aut}(E|\mathbb{C}) \leq G$ eine 2-Gruppe. Ist $H = \{1\}$, so folgt $E = \mathbb{C}$ wegen 18.6 und daher $L = \mathbb{C}$, wie gewünscht. Sei jetzt $H \neq \{1\}$. Nach 4.2 hat H eine Untergruppe U vom Index 2, und nach 18.6 ist $\mathrm{Fix}\, U|\mathbb{C}$ eine quadratische Körpererweiterung. Nach ÜA 27(a) ist $\mathrm{Fix}\, U = \mathbb{C}(a)$ mit $a^2 \in \mathbb{C}$ und $a \notin \mathbb{C}$. Schreibe $a^2 = re^{it}$ mit $r, t \in \mathbb{R}, r \geq 0$ (Polarkoordinaten) und setze $b := \sqrt{r}e^{it/2} \in \mathbb{C}$. Dann gilt $b^2 = re^{it} = a^2$, also $0 = a^2 - b^2 = (a + b)(a - b)$ und daher $a = \pm b \in \mathbb{C}$, ein Widerspruch. □

18.12 Satz (vom primitiven Element)**.** *Sei $L|K$ eine endliche separable Körpererweiterung (etwa eine endliche Erweiterung mit Charakteristik 0). Dann hat $L|K$ nur endlich viele Zwischenkörper, und es existiert ein („primitives“) Element $c \in L$ mit $L = K(c)$.*

Beweis. Eine Galois-Erweiterung $E|K$ wie in 18.10 hat nur endlich viele Zwischenkörper nach 18.6, also hat auch $L|K$ nur endlich viele Zwischenkörper.

Ist K endlich, so auch L, und $L^* = \langle c \rangle$ für ein $c \in L$ nach 8.5; also gilt $L = K(c)$. Sei jetzt K unendlich. Nach 18.1 ist die Vereinigung aller Zwischenkörper Z von $L|K$ mit $Z \neq L$ eine echte Teilmenge von L. Für jedes $c \in L$, das nicht in dieser Teilmenge liegt, gilt $K(c) = L$. □

[Ist $L = K(a_1, \ldots, a_t)$, so kann man c als K-Linearkombination der a_j wählen (ohne Beweis). Nach Steinitz 1910 hat eine endliche Körpererweiterung genau dann ein primitives Element, wenn sie nur endlich viele Zwischenkörper hat.

Die Separabilität in 18.12 ist nicht entbehrlich, wie die folgenden Beispiele zeigen. Sei p eine Primzahl und $L = \mathbb{F}_p(x, y)$ und $K = \mathbb{F}_p(x^p, y^p)$. Dann gilt $[L : K] = p^2$ und $c^p \in K$ für jedes $c \in L$, also auch $[K(c) : K] \leq p$. Deshalb gibt es kein primitives Element für $L|K$. Es gibt unendlich viele Zwischenkörper, etwa $K(x+ky)$ mit $k \in K$, oder $K(x^n+y)$ mit $n \in \mathbb{N} \setminus p\mathbb{N}$.]

18.13 Satz (E. Artin)**.** *Eine Körpererweiterung $L|K$ ist genau dann eine Galois-Erweiterung, wenn $K = \mathrm{Fix}\, H$ für eine endliche Gruppe $H \leq \mathrm{Aut}\, L$ gilt.*

Beweis. Ist $L|K$ eine Galois-Erweiterung, so gilt die Behauptung nach 18.5(iii, iv) mit $H = \mathrm{Aut}(L|K)$.

Sei jetzt $K = \mathrm{Fix}\, H$ mit einer endlichen Gruppe $H \leq \mathrm{Aut}\, L$. Dann ist $\mathrm{Aut}(L|K) = \mathrm{Aut}(L|\,\mathrm{Fix}\, H) = H$, wie im Beweis zu 18.5, (iii)⇒(iv). Wegen 18.5(iv) genügt es zu zeigen, dass $L|K$ endlich ist.

Jedes $a \in L$ ist eine Nullstelle des separablen Polynoms $\prod_{b\in H(a)}(x-b) \in K[x]$, denn die Linearfaktoren werden von H permutiert, daher liegen die Koeffizienten des Polynoms in $\operatorname{Fix} H = K$; also ist das Minimalpolynom von a über K separabel.

Für jedes $l \in L$ ist demnach $K(l)|K$ endlich und separabel und $[K(l) : K] \leq |H|$. Wegen dieser Gradbeschränkung können wir ein $a \in L$ so wählen, dass $[K(a) : K]$ möglichst groß ist. Für jedes $l \in L$ ist dann $K(a, l)|K$ endlich (nach der Gradformel 13.3) und separabel, also existiert nach 18.12 ein $c \in L$ mit $K(a, l) = K(c)$; wegen $[K(a) : K] \leq [K(a, l) : K] = [K(c) : K]$ und der Wahl von a folgt $K(a) = K(a, l)$, also $l \in K(a)$. Dies zeigt $L = K(a)$, also ist $L|K$ endlich. □

19. Galois-Gruppen

19.1 Galois-Gruppen als Permutationsgruppen. Sei K ein Körper, $0 \neq f \in K[x]$ und L ein Zerfällungskörper von f über K. Dann ist die Nullstellenmenge $M := \{a \in L \mid f(a) = 0\}$ endlich. Wir setzen $G := \operatorname{Aut}(f|K) := \operatorname{Aut}(L|K)$. Aus $\gamma \in G$ und $a \in M$ folgt $\gamma(a) \in M$, wegen $f(\gamma(a)) = \gamma(f(a)) = \gamma(0) = 0$; also ist $\gamma(M) \subseteq M$, sogar $\gamma(M) = M$, weil γ injektiv und M endlich ist. Das Einschränken

$$G \to \operatorname{Sym} M : \gamma \mapsto \gamma|_M$$

ist eine treue Wirkung von G auf M, denn aus $\gamma(a) = a$ für alle $a \in M$ folgt $\gamma = \mathrm{id}_L$ wegen $L = K(M)$. Daher ist G isomorph zu $G_M := \{\gamma|_M \mid \gamma \in G\} \leq \operatorname{Sym} M$.

Wir können G mit $G_M \leq \operatorname{Sym} M$ identifizieren, d.h. wir können G als Permutationsgruppe auf der Menge M der Nullstellen von f betrachten (wie Galois). Ist f separabel und $n := \operatorname{Grad}(f)$, so ist $|M| = n$ und $G \cong G_M \leq \operatorname{Sym} M \cong S_n$ (dann ist $L|K$ nach 18.5 eine Galois-Erweiterung, und man schreibt auch $\operatorname{Gal}(f|K)$ für G).

Jede Galois-Gruppe hat die Form $\operatorname{Aut}(f|K)$ mit einem Polynom $f \in K[x]$, denn nach 18.5(ii) hat jede Galois-Erweiterung die Form $L|K$, wobei L ein Zerfällungskörper eines Polynoms f über K ist.

19.2 Beispiel. $f = x^4 - 2$ ist nach Eisenstein (12.4) irreduzibel in $\mathbb{Q}[x]$ und hat in $\mathbb{C}$ die Nullstellen $a = \sqrt[4]{2}, -a, ia, -ia$. Der Zerfällungskörper $L = \mathbb{Q}(\pm a, \pm ia) = \mathbb{Q}(a, i)$ hat Grad 8 über $\mathbb{Q}$, wegen $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ nach 13.6 und $i \notin \mathbb{Q}(a) \subseteq \mathbb{R}$. Also ist $G = \operatorname{Aut}(f|\mathbb{Q}) = \operatorname{Aut}(L|\mathbb{Q})$ eine Gruppe der Ordnung 8, die man nach 19.1 als eine Untergruppe von S_4 betrachten kann. Wegen $|S_4| = 24 = 8 \cdot 3$ ist G eine 2-Sylowgruppe von S_4, also isomorph zur Diedergruppe D_8, vgl. ÜA 3c.

19.3 Satz. *Sei K ein Körper und $f \in K[x]$ irreduzibel. Dann wirkt* $\operatorname{Aut}(f|K)$ *transitiv auf der Menge aller Nullstellen von f (in einem Zerfällungskörper L von f über K).*

Beweis. Seien $a, a' \in L$ mit $f(a) = 0 = f(a')$. Nach 15.4(i), angewandt auf $\alpha = \mathrm{id} : K \to K(a')$, existiert ein K-Homomorphismus $\beta : K(a) \to K(a')$ mit $\beta(a) = a'$. Weil L auch ein Zerfällungskörper von f über $K(a)$ und $K(a')$ ist, liefert 15.4(ii) eine Fortsetzung von β zu einem K-Homomorphismus $\gamma : L \to L$. Es gilt $\gamma(a) = a'$. Ferner ist $[L : K]$ endlich und γ injektiv, also bijektiv, und daher $\gamma \in \operatorname{Aut}(L|K) = \operatorname{Aut}(f|K)$. □

Nach 19.3 führen irreduzible Polynome zu transitiven Untergruppen von S_n; die Ordnung einer solchen Untergruppe ist durch n teilbar (wegen 2.7). Die transitiven Untergruppen von S_3 sind S_3 und $A_3 \cong C_3$. Die transitiven Untergruppen von S_4 sind S_4, A_4, C_4, $C_2 \times C_2$ und D_8, bis auf Konjugation. Die transitiven Untergruppen von S_5 sind S_5, A_5, C_5, D_{10} und $C_5 \rtimes C_4 = \langle (12345), (2354) \rangle$, wieder bis auf Konjugation.

19.4 Satz (über reine Polynome)**.** *Sei K ein Körper, sei $c \in K$ eine Einheitswurzel der multiplikativen Ordnung n und sei $0 \neq a \in K$. Dann ist das „reine" Polynom $x^n - a$ separabel, und* $\mathrm{Aut}(x^n - a \mid K)$ *ist eine zyklische Gruppe; ihre Ordnung teilt n (und ist gleich n, wenn $x^n - a$ in $K[x]$ irreduzibel ist).*

Beweis. Sei b eine Nullstelle von $x^n - a$ in einem geeigneten Erweiterungskörper. Dann sind die bc^j mit $0 \leq j < n$ die sämtlichen Nullstellen von $x^n - a$. Also ist $x^n - a$ separabel, und $K(bc^j \mid 0 \leq j < n) = K(b)$ ist ein Zerfällungskörper von $x^n - a$ über K.

Sei $G = \mathrm{Aut}(K(b)|K) \cong \mathrm{Aut}(x^n - a|K)$. Für jedes $\gamma \in G$ ist $\gamma(b) = bc^j$ für ein $j \in \mathbb{N}$, also $\gamma(b)b^{-1} \in \langle c \rangle$. Die Abbildung

$$G \to \langle c \rangle : \gamma \mapsto \gamma(b)\, b^{-1}$$

ist ein Gruppenhomomorphismus, denn für $\gamma, \delta \in G$ ist $\delta(b)b^{-1} \in \langle c \rangle \subseteq K$ fest unter γ und daher

$$\frac{\gamma(b)}{b}\frac{\delta(b)}{b} = \frac{\gamma(b)}{b}\gamma\Big(\frac{\delta(b)}{b}\Big) = \frac{\gamma(b)}{b}\frac{\gamma(\delta(b))}{\gamma(b)} = \frac{(\gamma \circ \delta)(b)}{b}.$$

Dieser Gruppenhomomorphismus ist injektiv, denn aus $\gamma(b)b^{-1} = 1$ folgt $\gamma(b) = b$ und dann $\gamma = \mathrm{id}$. Also ist G isomorph zu einer Untergruppe von $\langle c \rangle \cong C_n$.

Ist $x^n - a$ irreduzibel in $K[x]$, so ist $n = [K(b) : K] = |G|$ nach 13.6 und 18.5(iii). □

(Gegen-) Beispiele: $\mathrm{Aut}(x^2 - 2 \mid \mathbb{Q}) \cong C_2$, aber $\mathrm{Aut}(x^3 - 2 \mid \mathbb{Q}) \cong S_3$ nach 18.8(b) und $\mathrm{Aut}(x^4 - 2 \mid \mathbb{Q}) \cong D_8$ nach 19.2 und $\mathrm{Aut}(x^6 + 108 \mid \mathbb{Q}) \cong S_3$, weil $\mathbb{Q}$ nicht die entsprechenden Einheitswurzeln enthält. Ferner $\mathrm{Aut}(x^4 - 4 \mid \mathbb{Q}) \cong C_2 \times C_2$.

19.5 Bemerkung (Das Umkehrproblem der Galois-Theorie)**.** Welche endlichen Gruppen kommen als Galois-Gruppen vor? Alle, denn: sei G eine endliche Gruppe und F ein beliebiger Körper. Nach Cayley (2.4) können wir G als eine Untergruppe einer symmetrischen Gruppe S_n betrachten. Sei $L = F(x_1, \ldots, x_n)$ der rationale Funktionenkörper über F in n Variablen $x_1, \ldots, x_n$. Dann wirkt G treu auf L durch Permutation dieser n Variablen (d.h. man setzt $g(x_j) = x_{g(j)}$ für $g \in G \leq S_n$) als eine Gruppe von F-Automorphismen. Nach 18.13 ist $L|\operatorname{Fix} G$ eine Galois-Erweiterung, und mit 18.6 folgt $\mathrm{Aut}(L|\operatorname{Fix} G) = G$.

Verschärfte Fragestellung: Gegeben sei ein Körper K; welche Gruppen G kommen als Galois-Gruppen von Galois-Erweiterungen $L|K$ vor?
Ist K algebraisch abgeschlossen, so kommt nur $G = \{1\}$ vor.
Für $K = \mathbb{R}$ ist $|G| \leq 2$, siehe 18.11.
Ist K endlich, so kommen genau die endlichen zyklischen Gruppen vor, siehe 16.4.
Für $K = \mathbb{C}(x)$ und für $K = \mathbb{R}(x)$ kommen alle endlichen Gruppen vor [nach dem

Riemannscher Existenzsatz aus der Überlagerungstheorie Riemannscher Flächen, siehe Malle, Matzat, Inverse Galois Theory, Springer 1999 oder Völklein, Groups as Galois groups, Cambridge Univ. Press 1996].

Für $K = \mathbb{Q}$ vermutet man [seit mehr als 100 Jahren], dass jede endliche Gruppe vorkommt. Die folgenden endlichen Gruppen wurden als Galois-Gruppen über $\mathbb{Q}$ realisiert:
— alle abelschen Gruppen (für Primzahlordnung siehe ÜA 36c)
— S_n und A_n für $n \geq 1$ (Hilbert 1892)
— alle p-Gruppen[9] [und alle auflösbaren Gruppen, wie in 20.3 definiert; siehe Neukirch, Schmidt, Wingberg, Cohomology of number fields, Springer 2000, 2013]
— viele einfache nichtabelsche Gruppen, etwa $A_5 \cong \mathrm{Aut}(x^5 + 20x + 16 \mid \mathbb{Q})$ und $\mathrm{GL}_3 \mathbb{F}_2 \cong \mathrm{Aut}(x^7 - 7x + 3 \mid \mathbb{Q})$ und das Monster M (Thompson 1984), aber derzeit noch nicht alle Gruppen $\mathrm{PSL}_2 \mathbb{F}_q$.

19.6 Bemerkung (Statistik von Galois-Gruppen)**.** Für die „meisten“ Polynome $f \in \mathbb{Z}[x]$ vom Grad n gilt $\mathrm{Aut}(f|\mathbb{Q}) \cong S_n$. Genauer gesagt: ist $n, M \in \mathbb{N}$ und $P_{n,M} = \{x^n + \sum_{j=0}^{n-1} a_j x^j \mid a_j \in \mathbb{Z} \text{ und } |a_j| \leq M\}$, also $|P_{n,M}| = (2M+1)^n$, so gilt

$$\lim_{M\to\infty} \frac{|\{f \in P_{n,M} \mid \mathrm{Aut}(f|\mathbb{Q}) \cong S_n\}|}{|P_{n,M}|} = 1 \quad \text{(nach van der Waerden 1933, 1936).}$$

Also sind die offenen Probleme in 19.5 nicht durch zufällige Wahl von Polynomen lösbar.

20. Auflösbarkeit von Gleichungen

20.1 Klassische Formeln. Eine quadratische Gleichung $x^2 + ax + b = 0$ mit $a, b \in K$ wird durch die Substitution $x = y - a/2$ zu

$$y^2 - a^2/4 + b = 0$$

mit den Lösungen $y = \pm\sqrt{a^2/4 - b}$, also $x = -a/2 \pm \sqrt{a^2/4 - b}$. Dies funktioniert für Körper K der Charakteristik $\neq 2$.

Eine kubische Gleichung $x^3 + ax^2 + bx + c = 0$ mit $a, b, c \in K$ wird durch die Substitution $x = y - a/3$ zu

$$y^3 + py + q = 0$$

mit $p, q \in K$ (nämlich $p = -a^3/3 + b$ und $q = 2a^3/27 - ab/3$). Mit der Substitution $y = z - \frac{p}{3z}$ erhält man

$$z^3 - \frac{p^3}{27z^3} + q = 0,$$

[9] Zum Beispiel ist $\mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{3})})$ eine Galois-Erweiterung von $\mathbb{Q}$ mit der Quaternionengruppe der Ordnung 8 als Galois-Gruppe (Variation von Dedekind 1886, siehe Gesammelte Werke Band II; Dean, A rational polynomial whose group is the quaternions, Amer. Math. Monthly 88 (1981) 42–45; Fujisaki, Proc. Japan Acad. 66 (1990) 80–83; Michailov, Some Groups of Orders 8 and 16 as Galois Groups over $\mathbb{Q}$, Math. Balkanica 17 (2003) 155–170).

also eine quadratische Gleichung für z^3 (man multipliziere mit z^3) mit den Lösungen $z^3 = -q/2 \pm \sqrt{q^2/4 + p^3/27}$, und $y = \sqrt[3]{z^3} - p/(3\sqrt[3]{z^3}) = \dots$ Dies funktioniert, wenn K nicht die Charakteristik 2 oder 3 hat (Tartaglia ca. 1515; Cardano, Ars magna sive de regulis algebraicis, 1545).

Eine Gleichung 4. Grades von der Form $x^4 + ax^3 + bx^2 + cx + d = 0$ wird durch die Substitution $x = y - a/4$ zu

$$y^4 + py^2 + qy + r = 0$$

mit $p, q, r \in K$. Diese Gleichungen hat Ferrari (ca. 1545) gelöst; wir suchen (nach Descartes 1637) Elemente α, β, γ in einem Erweiterungskörper von K mit

$$y^4 + py^2 + qy + r = (y^2 + \alpha y + \beta)(y^2 - \alpha y + \gamma),$$

d.h. mit $p = \beta + \gamma - \alpha^2$, $q = \alpha(\gamma - \beta)$ und $r = \beta\gamma$. (Dann sind nur noch zwei quadratische Gleichungen für y zu lösen.) Die ersten beiden Gleichungen liefern $2\gamma = \alpha^2 + p + q/\alpha$ und $2\beta = \alpha^2 + p - q/\alpha$; Einsetzen in die dritte Gleichung ergibt

$$4r = (\alpha^2 + p - q/\alpha)(\alpha^2 + p + q/\alpha) = (\alpha^2 + p)^2 - q^2/\alpha^2$$

und dann eine kubische Gleichung für α^2, die man wie oben lösen kann. Dies funktioniert, wenn K nicht die Charakteristik 2 oder 3 hat.

[Systematischer: Stroth, Algebra, de Gruyter 1998, S. 243f oder Rotman, Advanced Modern Algebra, Third edition, Part 1, Amer. Math. Soc. 2015, S. 4–8. Wir ignorieren die Mehrdeutigkeit von Wurzeln. Die Formeln für Grad 3 und 4 sind wenig brauchbar: auch ganzzahlige Nullstellen werden durch komplizierte Wurzeln ausgedrückt.]

Kann man auch Gleichungen von höherem Grad analog (d.h. durch Wurzelzeichen) auflösen? Diese Frage wurde erst viel später beantwortet, siehe 20.9.

20.2 Definition. Eine Körpererweiterung $L|K$ heisst Radikalerweiterung, falls $a_j \in L$ und $n(j) \in \mathbb{N}$ existieren mit $L = K(a_1, a_2, \dots, a_t)$ und

$$a_j^{n(j)} \in K(a_1, a_2, \dots, a_{j-1}) \quad \text{für } 1 \le j \le t.$$

Mit $n := \prod_{j=1}^{t} n(j)$ gilt dann $a_j^n \in K(a_1, a_2, \dots, a_{j-1})$ für $1 \le j \le t$. Jede Radikalerweiterung ist endlich.

Die Bedingung $a_j^n \in K(a_1, a_2, \dots, a_{j-1})$ besagt, dass a_j eine n-te Wurzel eines Elements aus $K(a_1, a_2, \dots, a_{j-1})$ ist. Nach 20.1 liegt jede Nullstelle eines Polynoms $f \in \mathbb{Q}[x]$ mit $\mathrm{Grad}(f) \le 4$ in einer Radikalerweiterung von $\mathbb{Q}$.

Nachtrag zur Gruppentheorie:

20.3 Definition. Eine Gruppe G heisst auflösbar, wenn es Untergruppen

$$\{1\} = U_1 \trianglelefteq U_2 \trianglelefteq U_3 \trianglelefteq \dots \trianglelefteq U_t = G$$

gibt mit abelschen Quotienten U_{j+1}/U_j für $1 \le j < t$.

20.4 Lemma. *Sei G eine auflösbare Gruppe. Dann ist auch jede Untergruppe H von G und jede Faktorgruppe G/N auflösbar, für $N \trianglelefteq G$.*

Beweis. Mit der Notation von 20.3 gilt $H \cap U_j \trianglelefteq H \cap U_{j+1}$, und nach [dem zweiten Isomorphiesatz] 3.9 ist $(H \cap U_{j+1})/(H \cap U_j) \cong (H \cap U_{j+1})U_j/U_j$ isomorph zu einer Untergruppe von U_{j+1}/U_j, also abelsch.

Es gilt $U_jN/N \trianglelefteq U_{j+1}N/N$; nach 3.10 und 3.9 ist die Gruppe $(U_{j+1}N/N)/(U_jN/N) \cong U_{j+1}N/U_jN = U_{j+1}U_jN/U_jN \cong U_{j+1}/(U_{j+1} \cap U_jN) \cong (U_{j+1}/U_j)/((U_{j+1} \cap U_jN)/U_j)$ ein Quotient von U_{j+1}/U_j, also abelsch. □

20.5 Beispiele. Die symmetrische Gruppe S_4 ist auflösbar: $S_4 \trianglerighteq A_4 \trianglerighteq C_2 \times C_2 \trianglerighteq \{1\}$. Auch S_1, S_2, S_3 sind auflösbar, etwa wegen 20.4. Die Gruppen S_n mit $n \geq 5$ sind nicht auflösbar, denn sonst wäre $A_5 \leq S_5$ nach 20.4 auflösbar, aber A_5 ist eine nichtabelsche einfache Gruppe nach 5.8.

Technisches Problem: eine Radikalerweiterung muss keine Galois-Erweiterung sein, auch in Charakteristik 0 nicht. Daher beweisen wir:

20.6 Satz. *Sei K ein Körper der Charakteristik 0 und $R|K$ eine Radikalerweiterung. Dann ist R ein Zwischenkörper einer Galois-Erweiterung $L|K$ mit auflösbarer Galois-Gruppe* $\mathrm{Aut}(L|K)$.

Beweis. Nach 20.2 existieren $a_j \in R$ und $n \in \mathbb{N}$ mit $R = K(a_1, a_2, \ldots, a_t)$ und $a_j^n \in K(a_1, a_2, \ldots, a_{j-1})$ für $1 \leq j \leq t$. Sei $m_j \in K[x]$ das Minimalpolynom von a_j über K, und sei L ein Zerfällungskörper von $f := (x^n - 1)\prod_{j=1}^t m_j \in K[x]$ über R; dann ist R ein Zwischenkörper von $L|K$. Ferner ist L auch ein Zerfällungskörper von f über K, wegen $R = K(a_1, a_2, \ldots, a_t)$ und $f(a_j) = 0$ für alle j. Also ist $L|K$ eine Galois-Erweiterung (weil K die Charakteristik 0 hat). Es genügt zu zeigen, dass die Gruppe $G := \mathrm{Aut}(L|K)$ auflösbar ist.

L enthält einen Zerfällungskörper von $x^n - 1$ über $\mathbb{Q}$, also eine Kopie von $\mathbb{Q}(e^{2\pi i/n})$, also eine Einheitswurzel c der multiplikativen Ordnung n. Ferner enthält L für jedes j einen Zerfällungskörper Z_j von m_j über K, und $Z_j|K$ ist eine Galois-Erweiterung (wegen Charakteristik 0). Nach 18.9 (mit Beweis) wird $\mathrm{Aut}(Z_j|K)$ von G induziert (durch Einschränken). Nach 19.3 wirkt $\mathrm{Aut}(Z_j|K)$, also auch G, transitiv auf der Menge der Nullstellen von m_j in L, für jedes j. Daher ist

$$L = K(c, \gamma(a_j) \mid 1 \leq j \leq t, \gamma \in G).$$

Sei $b_1, b_2, \ldots, b_s$ die folgende Liste: zuerst alle $\gamma(a_1)$ mit $\gamma \in G$ in irgendeiner Reihenfolge, dann alle $\gamma(a_2)$ mit $\gamma \in G$, …, zuletzt alle $\gamma(a_t)$ mit $\gamma \in G$. Wegen $\gamma(a_j)^n = \gamma(a_j^n) \in K(\gamma(a_1), \ldots, \gamma(a_{j-1}))$ für $1 \leq j \leq t$ und $\gamma \in G$ gilt

$$b_j^n \in K(b_1, b_2, \ldots, b_{j-1})$$

für $1 \leq j \leq s$. [Wegen $c^n = 1$ ist auch $L|K$ eine Radikalerweiterung.]

Wir setzen $L_0 := K(c)$ und $L_j := K(c, b_1, \ldots, b_j) = L_{j-1}(b_j)$ für $1 \leq j \leq s$ sowie

$$U_j := \mathrm{Aut}(L|L_j) \leq G \quad \text{für } 0 \leq j \leq s.$$

Für $1 \le j \le s$ ist L_j ein Zerfällungskörper von $x^n - b_j^n \in L_{j-1}[x]$ über L_{j-1}, da $x^n - b_j^n = \prod_{0 \le k < n}(x - b_j c^k)$. Also ist $L_j | L_{j-1}$ eine Galois-Erweiterung (wegen Charakteristik 0). Nach 18.9 ist $U_j = \mathrm{Aut}(L|L_j) \trianglelefteq \mathrm{Aut}(L|L_{j-1}) = U_{j-1}$, und $U_{j-1}/U_j \cong \mathrm{Aut}(L_j|L_{j-1})$ ist zyklisch nach 19.4 (wegen $c \in L_0$), insbesondere abelsch.

$L_0 = K(c)$ ist ein Zerfällungskörper von $x^n - 1$ über K, also eine Galois-Erweiterung von K. Mit 18.9 folgt $U_0 \trianglelefteq G$ und $G/U_0 \cong \mathrm{Aut}(K(c)|K)$. Diese Galois-Gruppe ist abelsch: für $\alpha, \beta \in \mathrm{Aut}(K(c)|K)$ ist $\alpha(c) = c^k$ und $\beta(c) = c^l$ mit geeigneten $k, l \in \mathbb{N}$, also $\alpha(\beta(c)) = c^{kl} = \beta(\alpha(c))$ und daher $\alpha\beta = \beta\alpha$.

Schließlich ist $L_s = K(c, b_1, \ldots, b_s) = L$ und daher $U_s = \mathrm{Aut}(L|L) = \{1\}$. Die Kette $\{1\} = U_s \trianglelefteq U_{s-1} \trianglelefteq \ldots \trianglelefteq U_1 \trianglelefteq U_0 \trianglelefteq G$ zeigt, dass G auflösbar ist. □

20.7 Korollar (Galois)**.** *Sei K ein Körper der Charakteristik 0 und sei $f \in K[x]$ irreduzibel. Liegt eine Nullstelle von f in einer Radikalerweiterung R von K, so ist die Gruppe $\mathrm{Aut}(f|K)$ auflösbar.*

Beweis. Sei L wie in 20.6. Weil $L|K$ normal ist, zerfällt f nach 17.2 in $L[x]$ in Linearfaktoren. Daher hat $L|K$ einen Zwischenkörper Z, der ein Zerfällungskörper von f über K ist. Also ist $Z|K$ normal, und 18.9 liefert $\mathrm{Aut}(f|K) = \mathrm{Aut}(Z|K) \cong \mathrm{Aut}(L|K)/\mathrm{Aut}(L|Z)$. Diese Faktorgruppe ist nach 20.4 auflösbar, weil $\mathrm{Aut}(L|K)$ auflösbar ist. □

Zu 20.6 und 20.7 gibt es partielle Umkehrungen, siehe etwa Stroth, Algebra, de Gruyter 1998, Satz 9.7 und 9.9 oder Rotman, Galois Theory, Springer 1998, Theorem 98.

20.8 Korollar. *Keine Nullstelle von $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ liegt in einer Radikalerweiterung von $\mathbb{Q}$.*

Beweis. f ist irreduzibel in $\mathbb{Q}[x]$ nach Eisenstein (12.4). Ferner hat f genau 3 reelle Nullstellen, wegen $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$, $f(2) > 0$ und weil $f' = 5x^4 - 4$ genau 2 reelle Nullstellen hat (Kurvendiskussion). Wir zeigen, dass $G := \mathrm{Aut}(f|\mathbb{Q})$ isomorph zu S_5 ist; mit 20.7 und 20.5 folgt dann die Behauptung.

Nach 19.3 ist G isomorph zu einer transitiven Untergruppe von S_5. Die komplexe Konjugation lässt die 3 reellen Nullstellen fest und vertauscht die zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$. Nummeriert man diese zwei Nullstellen mit 1,2, so gehört die Transposition (12) zu G. [Mit der Liste der transitiven Untergruppen von S_5 in § 19 folgt schon $G = S_5$.] Nach 2.7 ist 5 ein Teiler von $|G|$, also enthält G nach 4.1 einen 5-Zyklus; eine geeignete Potenz davon bildet 1 auf 2 ab, hat also die Form (12345) bei passender Nummerierung der 3 reellen Nullstellen.

Daher genügt es, die Gleichung $\langle (12), (12345) \rangle = S_5$ zu beweisen. Es gilt $(12)(12345) = (2345)$. Konjugiert man (12) mit den Potenzen dieses 4-Zyklus, so erhält man (nach 5.2) die Transpositionen $(1j)$ mit $j \in \{2, 3, 4, 5\}$, also alle Transpositionen, welche 1 bewegen. Konjugation mit Potenzen von (12345) liefert dann alle Transpositionen von S_5; diese erzeugen die Gruppe S_5 nach 5.4(a). □

[Nach Osada 1987 gilt $\mathrm{Aut}(x^n - x - 1 \mid \mathbb{Q}) = S_n$ für alle $n \in \mathbb{N}$.]

20.9 Korollar (Ruffini 1799, Abel 1824, 1826)**.** *Polynomgleichungen vom Grad ≥ 5 lassen sich im Allgemeinen nicht durch Wurzelausdrücke auflösen.*

Dieses Resultat ist ein Triumph für die Gruppentheorie: Polynomgleichungen vom Grad ≥ 5 sind deshalb nicht (mit Wurzelzeichen) auflösbar, weil die alternierende Gruppe A_5 einfach und nicht abelsch ist (siehe 5.8). Mit den Worten von Lagrange (laut Speiser): Die Gruppentheorie ist die wahre Metaphysik der Gleichungen.

Literatur: Ayoub, On the nonsolvability of the general polynomial, Amer. Math. Monthly 89 (1982) 397–401; Rosen, Niels Hendrik Abel and equations of the fifth degree, Amer. Math. Monthly 102 (1995) 495–505; Alekseev, Abel's theorem in problems and solutions, Kluwer Academic Publishers, Dordrecht 2004; Isaacs, Solution of polynomials by real radicals, Amer. Math. Monthly 92 (1985) 571–575; Dummit, Solving solvable quintics, Math. Computation 57 (1991) 387–401; Khovanskii, Galois theory, coverings and Riemann surfaces, Springer 2013.