Einführung in die Algebra

Sommersemester 2011

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

Diese Vorlesung setzt die Vorlesung „Einführung in die Zahlentheorie und algebraische Strukturen“ aus dem Wintersemester 2010/2011 fort. Dem entsprechend schließt sich auch dieses Skript unmittelbar an das Skript zur vorigen Vorlesung an. Insbesondere wird die Nummerierung der Abschnitte fortgeführt.

14. Endlich erzeugte Moduln über Hauptidealringen

Wir erinnern uns an den Satz, den wir am Ende der vorigen Vorlesung bewiesen haben (Satz und Definition 13.3):

14.1. **Satz und Definition.** *Sei R ein Hauptidealring, seien $m, n \geq 0$, und sei $A \in \mathrm{Mat}_{m\times n}(R)$. Dann gibt es $r \in \mathbb{Z}_{\geq 0}$ und Elemente $d_1, d_2, \ldots, d_r \in R$ mit $d_j \mid d_{j+1}$ für $1 \leq j < r$ und $d_r \neq 0$, so dass A zu $\mathrm{diag}_{m,n}(d_1, d_2, \ldots, d_r)$ äquivalent ist.*

Die Elemente $d_1, \ldots, d_r$ sind bis auf Assoziierte eindeutig bestimmt.

Diese Elemente $d_1, \ldots, d_r$ heißen die *Elementarteiler* der Matrix A.

Wir wollen jetzt aus diesen Satz über die Normalform von Matrizen über Hauptidealringen einen Struktur- bzw. Klassifikationssatz für „endlich erzeugte Moduln über Hauptidealringen“ ableiten. Ein wichtiger Spezialfall dieser Struktur sind abelsche Gruppen (für $R = \mathbb{Z}$, siehe unten); da der Beweis aber der selbe ist und das allgemeinere Ergebnis auch nützlich ist, wollen wir hier den allgemeineren Satz zeigen. Dazu müssen wir aber erst die relevanten Begriffe einführen. Wir werden weiterhin stillschweigend annehmen, dass alle Ringe *kommutativ* sind.

14.2. **Definition.** Sei R ein (kommutativer) Ring. Ein R-Modul ist ein Quintupel $(M, 0, +, -, \cdot)$, bestehend aus einer Menge M, einem Element $0 \in M$, einer Verknüpfung $+ : M \times M \to M$ (Addition), einer Abbildung $- : M \to M$ (Negation) und einer Verknüpfung $\cdot : R \times M \to M$ (skalare Multiplikation), so dass $(M, 0, +, -)$ eine abelsche Gruppe ist und zusätzlich gilt:

(1) $1 \cdot m = m$ für alle $m \in M$;
(2) $(r + s) \cdot m = r \cdot m + s \cdot m$ für alle $r, s \in R$, $m \in M$;
(3) $r \cdot (m + m') = r \cdot m + r \cdot m'$ für alle $r \in R$, $m, m' \in M$;
(4) $(rs) \cdot m = r \cdot (s \cdot m)$ für alle $r, s \in R$, $m \in M$.

Wenn die restlichen Daten aus dem Kontext klar sind, spricht man (wie analog in anderen Fällen) einfach vom „R-Modul M“. Statt $r \cdot m$ schreibt man meistens rm.

Der Plural von „der Modul“ im hier definierten Sinne ist „die Moduln“ (und nicht „die Module“).

Ein R-Modul ist also formal das selbe wie ein K-Vektorraum, nur dass man den Körper K durch einen beliebigen Ring R ersetzt. Sämtliche Aussagen über Vektorräume, für deren Beweis man nicht verwenden muss, dass von null verschiedene Elemente des Körpers invertierbar sind, gelten damit auch für Moduln. Zum Beispiel gelten die Regeln

$$0 \cdot m = 0 \qquad \text{und} \qquad (-r) \cdot m = r \cdot (-m)$$

für alle $r \in R$, $m \in M$.

14.3. **Bemerkung.** Man kann R-Moduln auch für nicht kommutative Ringe R definieren. Die obige Definition ergibt dann einen *R-Linksmodul*. Analog definiert man *R-Rechtsmoduln*, indem man die skalare Multiplikation von rechts operieren lässt. Ist R kommutativ, dann sind beide Strukturen isomorph.

Abelsche Gruppen kann man als Spezialfall auffassen:

14.4. **Proposition.** *Jede abelsche Gruppe $(A, 0, +, -)$ „ist“ ein $\mathbb{Z}$-Modul, d.h., es gibt eine eindeutig bestimmte skalare Multiplikation $\cdot : \mathbb{Z} \times A \to A$, so dass $(A, 0, +, -, \cdot)$ ein $\mathbb{Z}$-Modul ist.*

Beweis. Die skalare Multiplikation ist die Vervielfachungsabbildung: Es muss gelten

$$0 \cdot a = 0, \qquad 1 \cdot a = a, \qquad (-1) \cdot a = -a$$

und (für $n \in \mathbb{Z}_{\geq 0}$)

$$(n+1) \cdot a = n \cdot a + a, \qquad (-n-1) \cdot a = (-n) \cdot a - a\,.$$

Das liefert eine eindeutige induktive Definition der skalaren Multiplikation, und man überzeugt sich davon, dass sie die relevanten Eigenschaften hat. Etwas anschaulicher gilt für $n \in \mathbb{Z}_{\geq 0}$

$$n \cdot a = \underbrace{a + a + \ldots + a}_{n \text{ Summanden}}$$

und

$$(-n) \cdot a = -(n \cdot a) = n \cdot (-a) = \underbrace{(-a) + (-a) + \ldots + (-a)}_{n \text{ Summanden}}\,.$$

□

14.5. **Bemerkung.** Sind R_1 und R_2 Ringe und ist $\phi : R_1 \to R_2$ ein Ringhomomorphismus, dann lässt sich aus jedem R_2-Modul M ein R_1-Modul machen, indem man die gleiche additive Struktur verwendet und für die skalare Multiplikation $r_1 \cdot m := \phi(r_1) \cdot m$ setzt.

14.6. **Beispiele.** Sei R ein Ring. Dann ist R^n (oder allgemeiner, R^X für eine beliebige Menge X) ein R-Modul, indem man die Operationen komponentenweise definiert. Insbesondere ist R selbst in natürlicher Weise ein R-Modul.

Analog zu Vektorräumen gibt es Untermoduln.

14.7. **Definition.** Sei R ein Ring und M ein R-Modul. Ein *R-Untermodul* (oder auch nur *Untermodul*) von M ist eine Teilmenge $U \subset M$, die bezüglich der relevanten Operationen abgeschlossen ist: Es gilt $0 \in U$, und für $u, u' \in U$ und $r \in R$ gilt $u + u', -u, r \cdot u \in U$. Dabei ist die Forderung „$-u \in U$“ wegen $-u = (-1) \cdot u$ entbehrlich.

Es ist dann klar, dass $(U, 0, +|_{U \times U}, -|_U, \cdot|_{R \times U})$ wieder ein R-Modul ist.

14.8. **Beispiele.** Ist M ein R-Modul, dann sind $0 := \{0\} \subset M$ und M selbst stets (triviale) Untermoduln von M. Die Untermoduln des R-Moduls R sind genau die Ideale von R.

Wie bei Untervektorräumen und Idealen gilt:

14.9. **Lemma.** *Sei M ein R-Modul. Beliebige Durchschnitte und aufsteigende Vereinigungen von Untermoduln von M sind wieder Untermoduln von M.*

Beweis. Wie für Lemma 6.3 oder wie in der Linearen Algebra für Untervektorräume. □

Insbesondere ist folgende Definition sinnvoll (vgl. Def. 6.4):

14.10. **Definition.** Sei M ein R-Modul, $A \subset M$ eine Teilmenge. Der Untermodul

$$\langle A\rangle_R = \bigcap \{U \subset M \mid U \text{ Untermodul von } M \text{ und } A \subset U\}$$

heißt der *von A erzeugte Untermodul* von M. Ist $A = \{a_1, \ldots, a_n\}$ endlich, schreiben wir für $\langle A\rangle_R$ auch $\langle a_1, \ldots, a_n\rangle_R$.

Ist $U \subset M$ ein Untermodul und $A \subset M$ eine Teilmenge mit $U = \langle A\rangle_R$, so heißt A ein *Erzeugendensystem* von U. Hat M ein endliches Erzeugendensystem, so heißt M *endlich erzeugt*. Gilt $M = \langle a\rangle_R$ für ein $a \in M$, so heißt M ein *zyklischer R-Modul*.

Völlig analog zu Idealen und Untervektorräumen gilt dann:

14.11. **Lemma.** *Sei M ein R-Modul und $A \subset M$ eine Teilmenge. Dann gilt*

$$\langle A\rangle_R = \{r_1a_1 + \cdots + r_na_n \mid n \geq 0, r_j \in R, a_j \in A\}\,.$$

Die Elemente von $\langle A\rangle_R$ sind also gerade die endlichen *R-Linearkombinationen* von Elementen von A.

Beweis. Wie für Lemma 6.5 oder wie in der Linearen Algebra für Untervektorräume. □

14.12. **Definition.** Sei M ein R-Modul und $(a_i)_{i\in I}$ eine Familie von Elementen von M. Die Familie (a_i) heißt *Basis* von M, wenn jedes Element m von M sich eindeutig als (endliche)R-Linearkombination der a_i schreiben lässt, d.h. es gibt eine eindeutig bestimmte Familie $(r_i)_{i\in I}$ von Elementen von R mit $r_i = 0$ für alle bis auf endlich viele i, so dass $m = \sum_{i\in I} r_i \cdot a_i$ ist.

Ein R-Modul M, der eine Basis hat, heißt *frei*. Hat M eine endliche Basis, dann heißt M *endlich erzeugt frei*.

14.13. **Beispiele.** Für $n \in \mathbb{Z}_{\geq 0}$ ist R^n ein endlich erzeugter freier R-Modul mit der Basis $e_1, e_2, \ldots, e_n$, wobei e_j der übliche „Standard-Basisvektor“ ist.

Auf der anderen Seite ist $M = \mathbb{Z}/2\mathbb{Z}$ als $\mathbb{Z}$-Modul *nicht* frei, denn für jedes Element m von M und $n, k \in \mathbb{Z}$ gilt $(n + 2k) \cdot m = n \cdot m$, also ist eine Darstellung als Linearkombination niemals eindeutig. Wir sehen also, dass ein Modul im Unterschied zu einem Vektorraum keine Basis haben muss. Als $\mathbb{F}_2$-Modul (= $\mathbb{F}_2$-Vektorraum) ist M jedoch frei.

Folgende Begriffsbildung (benannt nach *Emmy Noether* (1882-1935), bedeutende deutsche Mathematikerin, Mitbegründerin der modernen Algebra) wird nützlich sein.

14.14. **Definition.** Ein R-Modul heißt *noethersch*, wenn alle eine Untermoduln endlich erzeugt sind. Ein Ring R heißt *noethersch*, wenn er als R-Modul noethersch ist, d.h. wenn alle seine Ideale endlich erzeugt sind.

Insbesondere ist ein Hauptidealring stets noethersch, denn in diesem Fall sind alle Ideale sogar von einem Element erzeugt.

Es gibt eine äquivalente Charakterisierung von „noethersch“, die häufig für Beweise nützlich ist.

14.15. **Lemma.** *Ein R-Modul M ist noethersch genau dann, wenn jede aufsteigende Kette von Untermoduln von M stationär wird. D.h., sind $U_n \subset M$ für $n \in \mathbb{Z}_{>0}$ Untermoduln mit $U_n \subset U_{n+1}$ für alle n, dann gibt es $N \in \mathbb{Z}_{>0}$, so dass $U_n = U_N$ für alle $n \geq N$.*

Für Ringe gilt das entsprechend mit „Idealen“ statt „Untermoduln“.

Beweis. Sei zunächst M noethersch und $U_1 \subset U_2 \subset \dots$ eine aufsteigende Kette von Untermoduln von M. Dann ist $U = \bigcup_{n\geq 1} U_n$ nach Lemma 14.9 wieder ein Untermodul von M, nach Voraussetzung also endlich erzeugt: $U = \langle A\rangle_R$ mit $A \subset U$ endlich. Für jedes $a \in A$ gibt es dann eine Zahl $n(a)$, so dass $a \in U_{n(a)}$. Da A endlich ist, existiert $N = \max\{n(a) \mid a \in A\}$. Da die Untermoduln U_n eine aufsteigende Kette bilden, folgt $A \subset U_N$ und damit

$$\langle A\rangle_R \subset U_N \subset U_n \subset U = \langle A\rangle_R$$

für alle $n \geq N$. Das ist die Behauptung.

Nun nehmen wir umgekehrt an, dass jede aufsteigende Kette von Untermoduln von M stationär wird. Sei U ein beliebiger Untermodul von M; wir müssen zeigen, dass U endlich erzeugt ist. Dazu nehmen wir an, das sei nicht der Fall. Dann gilt für jeden endlich erzeugten Untermodul $U' \subset U$, dass $U' \neq U$, also $U \setminus U' \neq \emptyset$ ist. Wir können dann eine aufsteigende Kette von Untermoduln von M konstruieren, die nicht stationär wird, indem wir $U_1 = 0$ und dann

$$U_{n+1} = U_n + R \cdot a_{n+1} = \langle U_n \cup \{a_{n+1}\}\rangle_R$$

setzen für ein $a_{n+1} \in U \setminus U_n$. So ein Element existiert, da $U_n = \langle a_1, a_2, \dots, a_n\rangle_R$ endlich erzeugt ist. Damit erhalten wir einen Widerspruch zur Voraussetzung, also muss die Annahme falsch sein, d.h. U muss doch endlich erzeugt sein. □

Wir werden bald sehen, dass endlich erzeugte Moduln über noetherschen Ringen stets noethersch sind. Vorher müssen wir aber noch die passenden Struktur erhaltenden Abbildungen einführen.

14.16. **Definition.** Seien M_1 und M_2 zwei R-Moduln. Ein *R-Modul-Homomorphismus* oder *R-lineare Abbildung* ist eine Abbildung $\phi : M_1 \to M_2$, so dass $\phi(m + m') = \phi(m) + \phi(m')$ und $\phi(rm) = r\phi(m)$ gilt für alle $m, m' \in M_1$ und $r \in R$.

Der *Kern* von ϕ ist das Urbild von $0 \in M_2$ unter ϕ:

$$\ker(\phi) = \phi^{-1}(0) = \{m \in M_1 \mid \phi(m) = 0\}\,.$$

Man sieht leicht, dass auch gilt $\phi(0) = 0$ und $\phi(-m) = -\phi(m)$.

Wie üblich verwenden wir die Begriffe (R-Modul-) *Monomorphismus*, *Epimorphismus*, *Isomorphismus*, *Endomorphismus*, *Automorphismus*, falls ϕ injektiv, surjektiv, bijektiv, $M_1 = M_2$, $M_1 = M_2$ und ϕ bijektiv ist.

Diese Begriffsbildung ist analog zu linearen Abbildungen zwischen Vektorräumen. Wie dort gelten folgende Aussagen:

14.17. **Lemma.**

(1) Kern und Bild einer R-linearen Abbildung sind Untermoduln (der Quelle bzw. des Ziels).
(2) Bilder und Urbilder von Untermoduln unter einer R-linearen Abbildung sind wieder Untermoduln.

Beweis. Wie in der Linearen Algebra. □

14.18. **Beispiel.** Ein endlich erzeugter freier R-Modul M mit einer n-elementigen Basis ist isomorph zu R^n. Ist $a_1, a_2, \ldots, a_n$ die Basis, dann ist ein Isomorphismus $R^n \to M$ gegeben durch

$$(r_1, r_2, \ldots, r_n) \longmapsto r_1 a_1 + r_2 a_2 + \ldots + r_n a_n \,.$$

Jetzt können wir auch Quotientenmoduln (oder Faktormoduln) definieren.

14.19. **Satz und Definition.** *Sei M ein R-Modul und U ein Untermodul von M. Dann ist die Relation*

$$m \equiv m' \bmod U \iff m - m' \in U$$

eine Äquivalenzrelation auf M, die mit Addition und skalarer Multiplikation verträglich ist:

$$m \equiv m' \bmod U \implies m + m'' \equiv m' + m'' \bmod U \quad \text{und} \quad rm \equiv rm' \bmod U \,.$$

Wir bezeichnen mit M/U die Menge der Äquivalenzklassen und mit $[m]$ oder $m+U$ die Äquivalenzklasse von $m \in M$. *Auf M/U gibt es eine eindeutig bestimmte Struktur als R-Modul, so dass die kanonische Abbildung $\phi : M \to M/U$ R-linear ist. Es gilt dann* $\ker(\phi) = U$. Dieser R-Modul M/U heißt *Quotientenmodul* oder *Faktormodul* von M modulo U; ϕ heißt *kanonischer Epimorphismus*.

Beweis. Analog zu 7.11, 7.12, 7.13. □

Wir haben auch wieder den üblichen Isomorphiesatz.

14.20. **Satz.** *Seien M_1 und M_2 zwei R-Moduln und $\phi : M_1 \to M_2$ eine R-lineare Abbildung. Dann induziert ϕ einen Isomorphismus zwischen $M_1/\ker(\phi)$ und dem Bild von ϕ.*

Beweis. Analog zu 7.14. Zur Erinnerung: Der induzierte Isomorphismus ψ ist gegeben durch

$$\psi : M_1/\ker(\phi) \longrightarrow \operatorname{im}(\phi) \,, \qquad [m] \longmapsto \phi(m) \,;$$

es ist zu zeigen, dass ψ wohldefiniert, injektiv und surjektiv ist. Letzteres ist klar; für die Injektivität zeigt man $\ker(\psi) = \{[0]\}$. □

14.21. **Bemerkung.** Analog zur Situation bei Vektorräumen hat man auch die beiden folgenden Isomorphiesätze:

Seien U und U' Untermoduln des R-Moduls M. Dann induziert die Inklusion $U \hookrightarrow U+U'$ einen Isomorphismus

$$\frac{U}{U \cap U'} \xrightarrow{\cong} \frac{U+U'}{U'}.$$

(Man wende Satz 14.20 auf die Komposition $U \to U + U' \to (U + U')/U'$ an.)

Seien $U \subset V \subset M$ Untermoduln des R-Moduls M. Dann ist V/U ein Untermodul von M/U, und man hat einen kanonischen Isomorphismus

$$\frac{M}{V} \xrightarrow{\cong} \frac{M/U}{V/U}.$$

(Man wende Satz 14.20 auf die Komposition $M \to M/U \to (M/U)/(V/U)$ an.)

14.22. **Beispiel.** Sei M ein *zyklischer* R-Modul, d.h., M wird von einem Element a erzeugt. Dann erhalten wir einen Epimorphismus $\phi : R \to M$, $r \mapsto ra$, dessen Kern ein Untermodul des R-Moduls R, also ein Ideal I von R ist. Wir sehen also: Jeder zyklische R-Modul ist isomorph zum R-Modul R/I für ein Ideal I von R.

Umgekehrt ist jeder R-Modul der Form R/I auch zyklisch, denn $[1] = 1 + I$ ist ein Erzeuger. Die zyklischen R-Moduln sind also (bis auf Isomorphie) *genau* die Moduln der Form R/I.

Insbesondere sehen wir, dass die *zyklischen abelschen Gruppen* die Form $\mathbb{Z}/n\mathbb{Z}$ haben (da jedes Ideal von $\mathbb{Z}$ ein Hauptideal ist). Es gibt dann zwei Möglichkeiten: Entweder ist $n = 0$; dann ist die Gruppe isomorph zu(r additiven Gruppe von) $\mathbb{Z}$. Oder wir können $n > 0$ wählen; dann ist die Gruppe isomorph zur additiven Gruppe von $\mathbb{Z}/n\mathbb{Z}$ und hat n Elemente

$$[0], [1], [2] = [1] + [1], [3] = [1] + [1] + [1], \ldots, [n-1] = \underbrace{[1] + \ldots + [1]}_{n-1 \text{ Summanden}}.$$

Entsprechend gilt für einen Hauptidealring R, dass die zyklischen R-Moduln isomorph sind entweder zu R selbst oder zu R/Rd mit einem Element $0 \neq d \in R$.

Nun können wir einen ersten Satz über noethersche Moduln formulieren.

14.23. **Satz.** *Sei M ein R-Modul und $U \subset M$ ein Untermodul. Dann ist M noethersch genau dann, wenn sowohl U als auch M/U noethersch sind.*

Nach Satz 14.20 ist äquivalent: *Sei $\phi : M \to M'$ eine R-lineare Abbildung. Dann ist M noethersch genau dann, wenn sowohl* $\ker(\phi)$ *als auch* $\mathrm{im}(\phi)$ *noethersch sind.*

Beweis. Wir benutzen die Charakterisierung über die aufsteigenden Ketten von Untermoduln („Kettenbedingung“). Sei zunächst M noethersch. Wir müssen zeigen, dass U und M/U beide noethersch sind. Für U ist das klar, da jede aufsteigende Kette von Untermoduln von U auch eine aufsteigende Kette von Untermoduln von M ist und deswegen stationär wird. Sei jetzt $V_1 \subset V_2 \subset \ldots$ eine aufsteigende Kette von Untermoduln von M/U, und sei $\phi : M \to M/U$ der kanonische Epimorphismus. Dann ist $\phi^{-1}(V_1) \subset \phi^{-1}(V_2) \subset \ldots$ eine aufsteigende Kette von Untermoduln von M, wird also nach Voraussetzung stationär. Wegen $V_n = \phi(\phi^{-1}(V_n))$ (hier verwenden wir, dass ϕ surjektiv ist) folgt dann, dass auch die Kette (V_n) stationär wird.

Wir setzen jetzt voraus, dass U und M/U beide noethersch sind. Sei $(U_n)_{n\geq 1}$ eine aufsteigende Kette von Untermoduln von M. Dann ist $(\phi(U_n))_{n\geq 1}$ eine aufsteigende Kette von Untermoduln von M/U, wird also stationär: $\phi(U_n) = \phi(U_{N'})$ für $n \geq N'$. Außerdem ist $(U_n \cap U)_{n\geq 1}$ eine aufsteigende Kette von Untermoduln von U und wird stationär: $U_n \cap U = U_{N''} \cap U$ für $n \geq N''$. Sei $N = \max\{N', N''\}$, dann gilt $U_n \cap U = U_N \cap U$ und $\phi(U_n) = \phi(U_N)$ für alle $n \geq N$. Dann gilt auch $U_n = U_N$: Es gilt stets $U_N \subset U_n$. Sei nun $u \in U_n$, dann ist $\phi(u) \in \phi(U_N)$, also gibt es $u' \in U_N$ mit $\phi(u) = \phi(u')$, also $u'' := u - u' \in U$. Wegen $u, u' \in U_n$ ist $u'' \in U_n \cap U = U_N \cap U \subset U_N$, also $u = u' + u'' \in U_N$. Es folgt $U_n \subset U_N$, also Gleichheit. Damit ist gezeigt, dass $(U_n)_{n\geq 1}$ stationär wird. □

Eine einfache Folgerung ist folgende Aussage.

14.24. **Proposition.** *Sei R ein noetherscher Ring und $n \in \mathbb{Z}_{\geq 0}$. Dann ist der R-Modul R^n noethersch.*

Beweis. Induktion nach n. Klar für $n = 0$ (dann ist R^0 der Nullmodul) und $n = 1$ (dann ist $R^1 = R$ noethersch nach Definition eines noetherschen Rings). Sei also $n \geq 2$. Wir betrachten die surjektive R-lineare Abbildung $\phi : R^n \to R$, $(r_1, \ldots, r_n) \mapsto r_n$. Das Bild von ϕ ist noethersch, und $\ker(\phi) = R^{n-1} \times \{0\} \cong R^{n-1}$ ist ebenfalls noethersch nach Induktionsannahme. Aus Satz 14.23 folgt dann, dass R^n ebenfalls noethersch ist. □

Nun folgt leicht das für uns wesentliche Ergebnis.

14.25. **Satz.** *Sei R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann ist M noethersch.*

Beweis. Sei $A = (a_1, \ldots, a_n)$ ein endliches Erzeugendensystem von M. Dann ist

$$\phi : R^n \longrightarrow M\,, \quad (r_1, \ldots, r_n) \longmapsto r_1 a_1 + \ldots + r_n a_n$$

eine surjektive R-lineare Abbildung. Nach Prop. 14.24 ist R^n noethersch. Nach Satz 14.23 ist dann auch $\mathrm{im}(\phi) = M$ noethersch. □

Etwas konkreter heißt das:

Jeder Untermodul eines endlich erzeugten Moduls über einem noetherschen Ring ist ebenfalls endlich erzeugt.

Ein weiterer interessanter Satz in diesem Zusammenhang ist der folgende.

14.26. **Hilbertscher Basissatz.** *Sei R ein noetherscher Ring. Dann ist der Polynomring $R[x]$ ebenfalls noethersch.*

Beweis. Wir verwenden wieder die Kettenbedingung. Sei also $(I_n)_{n\geq 1}$ eine aufsteigende Kette von Idealen von $R[x]$. Für ein Ideal I von $R[x]$ definieren wir

$$c_m(I) = \left\{ a_m \;\middle|\; f = \sum_{j=0}^{m} a_j x^j \in I \right\} \subset R\,;$$

man überzeugt sich leicht davon, dass $c_m(I)$ ein Ideal von R ist, dass gilt

$$c_0(I) \subset c_1(I) \subset c_2(I) \subset \ldots\,, \quad \text{und} \quad I \subset J \implies c_m(I) \subset c_m(J)\,.$$

Wir wollen zeigen, dass die Folge von Folgen $\big((c_m(I_n))_{m\geq 0}\big)_{n\geq 0}$ von Idealen von R stationär wird (d.h., es gibt ein N, so dass für alle $n \geq N$ gilt, dass $c_m(I_n) = c_m(I_N)$ für alle $m \geq 0$). Wenn das so ist, dann gilt auch $I_n = I_N$: Die Inklusion $I_N \subset I_n$ gilt nach

Voraussetzung. Sei $f \in I_n$; wir müssen zeigen, dass $f \in I_N$ ist. Wir beweisen das durch Induktion nach dem Grad von f; für $f = 0$ ist die Behauptung klar. Anderenfalls sei $\deg(f) = d$ und a_d der Leitkoeffizient von f. Wegen $c_d(I_n) = c_d(I_N)$ gibt es ein Polynom $g \in I_N$ vom Grad d mit Leitkoeffizient a_d. Dann ist $f - g \in I_n$ von kleinerem Grad, also (nach Induktionsannahme), $f - g \in I_N$. Es folgt $f = (f - g) + g \in I_N$. Also ist die Kette $(I_n)_{n\geq 1}$ stationär.

Es bleibt zu zeigen, dass die Idealfolgen stationär werden. Zunächst einmal gilt für jedes $n \geq 1$, dass die aufsteigende Folge $(c_m(I_n))_{m\geq 0}$ stationär werden muss (denn R ist noethersch); sei also $M(n)$ ein Index mit $c_m(I_n) = c_{M(n)}(I_n)$ für alle $m \geq M(n)$. Dann ist $(c(I_n))_{n\geq 1}$ mit

$$c(I_n) := c_{M(n)}(I_n) = \bigcup_{m\geq 0} c_m(I_n)$$

ebenfalls eine aufsteigende Kette von Idealen von R, wird also stationär: Es gibt N', so dass $c(I_n) = c(I_{N'})$ für alle $n \geq N'$. Wir setzen $M = M(N')$. Dann haben wir $c_m(I_n) = c_M(I_{N'})$ für alle $m \geq M$, $n \geq N'$. Damit werden alle Folgen $(c_m(I_n))_n$ mit $m \geq M$ beim selben Index N' stationär. Außerdem wird jede der endlich vielen solchen Folgen mit $m < M$ bei einem Index $N(m)$ stationär; die Behauptung gilt dann mit $N = \max\{N'\} \cup \{N(m) \mid 0 \leq m < M\}$. □

Insbesondere ist jeder Polynomring in endlich vielen Variablen über einem Körper noethersch. Das bedeutet:

Jedes (möglicherweise unendliche) System von Polynomgleichungen in n Variablen über einem Körper K ist äquivalent zu einem endlichen solchen System.

Denn die Menge der Gleichungen, die aus $\{f_I(x_1, \ldots, x_n) = 0 \mid i \in I\}$ folgen, besteht gerade aus allen Gleichungen $f = 0$ mit $f \in \langle\{f_i \mid i \in I\}\rangle_{K[x_1,\ldots,x_n]}$, und dieses Ideal ist endlich erzeugt.

Da man sich leicht überlegt, dass jeder Faktorring eines noetherschen Rings wieder noethersch ist, folgt auch:

Jede endlich erzeugte K-Algebra (das sind gerade die Faktorringe von Polynomringen $K[x_1, \ldots, x_n]$) *ist noethersch.*

Sei nun R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Wir wählen wie im Beweis von Satz 14.25 oben ein endliches Erzeugendensystem $(a_1, \ldots, a_n)$. Dann haben wir den Epimorphismus $\phi : R^n \to M$ wie oben. Da der Kern von ϕ ein Untermodul von R^n ist, ist $\ker(\phi)$ ebenfalls endlich erzeugt. Wir können also ein endliches Erzeugendensystem $(b_1, \ldots, b_m)$ von $\ker(\phi)$ wählen (mit $b_j \in R^n$); dann gilt nach dem Isomorphiesatz 14.20

$$M \cong R^n/\langle b_1, b_2, \ldots, b_m\rangle_R = R^n/\operatorname{im}(\psi)\,,$$

wo $\psi : R^m \to R^m$, $(r_1, \ldots, r_m) \mapsto r_1b_1 + \ldots + r_mb_m$ wieder eine R-lineare Abbildung ist. Wie in der Linearen Algebra kann eine lineare Abbildung $R^m \to R^n$ durch eine Matrix dargestellt werden, indem die (Zeilen-)Vektoren b_j in eine $m \times n$-Matrix A (mit Einträgen aus R) verpackt werden.

Wenn wir diese Matrix von links mit einer invertierbaren Matrix (aus $\mathrm{GL}_m(R)$) multiplizieren, ändern wir zwar die Zeilen von A, aber nicht den von den Zeilen erzeugten Untermodul $\operatorname{im}(\psi)$, denn wir ersetzen lediglich ψ durch $\psi \circ \alpha$ mit einem Automorphismus α von R^m. Wenn wir A von rechts mit einer invertierbaren Matrix (aus $\mathrm{GL}_n(R)$) multiplizieren, ersetzen wir die Standardbasis von R^n durch eine (beliebige) andere Basis. Äquivalent dazu ist es, dem Epimorphismus ϕ einen Automorphismus β von R^n voranzustellen, was am Bild M von ϕ aber nichts ändert. Wir sehen also, dass jede Matrix PAQ mit $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ den selben Modul M beschreibt. Dies liefert den Zusammenhang zwischen Satz 14.1

und dem Problem der Klassifikation endlich erzeugter R-Moduln. Für die Formulierung des Klassifikationssatzes brauchen wir noch den Begriff der direkten Summe von R-Moduln.

14.27. **Definition.** Sei R ein Ring, und seien $M_1, \ldots, M_n$ R-Moduln. Die *direkte Summe* $M_1 \oplus \ldots \oplus M_n = \bigoplus_{j=1}^n M_j$ ist ein R-Modul zusammen mit R-linearen Abbildungen $\iota_j : M_j \to \bigoplus_{i=1}^n M_i$ mit folgender universeller Eigenschaft:

Für jeden R-Modul M und R-lineare Abbildungen $\phi_j : M_j \to M$ $(j = 1, \ldots, n)$ gibt es genau eine R-lineare Abbildung $\phi : \bigoplus_{i=1}^n M_i \to M$, so dass $\phi \circ \iota_j = \phi_j$ gilt für alle $j = 1, \ldots, n$.

Konkret lässt sich die direkte Summe endlich vieler Moduln realisieren als das Produkt $M_1 \times \cdots \times M_n$ mit komponentenweise definierter Addition und skalarer Multiplikation; die Abbildung ι_j schickt $m_j \in M_j$ auf $(0, \ldots, 0, m_j, 0, \ldots, 0)$ mit m_j an der j-ten Stelle. Die eindeutig bestimmte Abbildung ϕ in der universellen Eigenschaft ist gegeben als $\phi(m_1, \ldots, m_n) = \phi_1(m_1) + \ldots + \phi_n(m_n)$.

Es gilt $R^n \cong R \oplus R \oplus \ldots \oplus R$ (n Summanden). Ist e_j das $j$te Standardbasis-Element von R^n, dann sieht man leicht:

$$R^n / \langle d_1 e_1, d_2 e_2, \ldots, d_n e_n \rangle_{R^n} \cong R/Rd_1 \oplus R/Rd_2 \oplus \ldots \oplus R/Rd_n$$

Man kann die direkte Summe für beliebige Familien $(M_i)_{i \in I}$ von R-Moduln definieren (mit der analogen universellen Eigenschaft). In diesem Fall kann die direkte Summe $\bigoplus_{i \in I} M_i$ aber *nicht* als das Produkt der M_i realisiert werden (warum nicht?).

14.28. **Lemma.** *Sei R ein Hauptidealring und $M = R/Rd_1 \oplus \ldots \oplus R/Rd_n$ eine direkte Summe von n zyklischen R-Moduln, wobei $d_1 \notin R^\times$ und $d_1 \mid d_2 \mid \ldots \mid d_n$ gilt ($d_j = 0$ ist erlaubt). Dann kann M von n Elementen erzeugt werden, aber nicht von $n-1$ Elementen.*

Beweis. Dass M von n Elementen erzeugt werden kann ist klar, denn M ist ein epimorphes Bild von R^n ($M \cong R^n / \langle d_1 e_1, \ldots, d_n e_n \rangle$).

Für die zweite Behauptung können wir annehmen, dass R kein Körper ist (denn sonst müssen alle $d_j = 0$ sein, und wir haben den Vektorraum R^n). Wir wählen ein Primelement von R, das d_1 teilt. Das ist möglich, da d_1 keine Einheit ist: Ist $d_1 \neq 0$, dann hat d_1 einen Primteiler; sonst wählen wir ein beliebiges Primelement (Primelemente existieren, da R kein Körper ist). Dann gibt es Epimorphismen $R/Rd_j \to R/Rp$, also auch einen Epimorphismus $M \to (R/Rp)^n$; R/Rp ist ein Körper. Ein Erzeugendensystem von $(R/Rp)^n$ als R-Modul ist auch ein Erzeugendensystem von $(R/Rp)^n$ als (R/Rp)-Vektorraum, muss also mindestens n Elemente haben. Wäre M von weniger als n Elementen erzeugbar, müsste das auch für M/pM gelten, ein Widerspruch. □

Die Teilbarkeitsbedingung ist wesentlich, wie das Beispiel des $\mathbb{Z}$-Moduls

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

zeigt, der von dem einen Element $(1 + 2\mathbb{Z}, 1 + 3\mathbb{Z})$ erzeugt wird!

14.29. **Klassifikationssatz für endlich erzeugte Moduln über Hauptidealringen.** *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{Z}_{\geq 0}$ und bis auf Assoziierte eindeutig bestimmte Elemente $d_1, \ldots, d_k \in R \setminus \{0\}$, mit $d_1 \mid \ldots \mid d_k$ und $d_1 \notin R^\times$, so dass*

$$M \cong R/Rd_1 \oplus \ldots \oplus R/Rd_k \oplus R^r \,.$$

D.h., ein endlich erzeugter R-Modul ist eine direkte Summe endlich vieler *zyklischer* R-Moduln.

Beweis. Die Existenz folgt leicht aus obiger Überlegung und Satz 14.1: Sei A eine Matrix, die M wie oben beschreibt. Dann können wir statt A jede dazu äquivalente Matrix $A' = PAQ$ verwenden; nach Satz 14.1 können wir $A' = \mathrm{diag}_{m,n}(d_1, \ldots, d_k)$ wählen. Wir erhalten einen Isomorphismus wie angegeben (mit $r = n - k$), nur dass der Anfang der Folge $d_1, \ldots, d_k$ aus Einheiten bestehen könnte. Dann gilt für die zugehörigen Summanden aber $R/Rd_i = R/R = 0$; sie können also weggelassen werden.

Zur Eindeutigkeit: $n = k + r$ ist eindeutig bestimmt als minimale Anzahl von Erzeugenden von M nach Lemma 14.28 Das Ideal Rd_j ($= 0$ für $k < j \leq n$) ist charakterisiert als

$$Rd_j = \{r \in R \mid rM \text{ kann von } \leq n - j \text{ Elementen erzeugt werden}\} \,.$$

(Beachte: $d \cdot R/Rd' = 0$ genau dann, wenn $d' \mid d$.) Daher ist auch die Folge der Ideale

$$Rd_1, Rd_2, \ldots, Rd_k, \underbrace{0, \ldots, 0}_{r\text{-mal}}$$

eindeutig bestimmt, was zur Eindeutigkeitsaussage im Satz äquivalent ist. □

Als Spezialfall erhalten wir:

14.30. **Klassifikationssatz für endlich erzeugte abelsche Gruppen.** *Sei A eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte positive ganze Zahlen $d_1, d_2, \ldots, d_k$ mit $1 \neq d_1 \mid d_2 \mid \ldots \mid d_k$ und eine Zahl $r \in \mathbb{Z}_{\geq 0}$, so dass*

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^r \,.$$

A ist genau dann endlich, wenn $r = 0$ ist; dann ist $\#A = d_1 d_2 \cdots d_k$.

Beweis. Wir wenden Satz 14.29 auf den Ring $R = \mathbb{Z}$ an. Die Endlichkeitsaussage ist klar; die Aussage über die Ordnung $\#A$ von A folgt daraus, dass die unterliegende Menge der direkten Summe das Produkt der Mengen $\mathbb{Z}/d_j\mathbb{Z}$ ist. □

Satz 14.30 gibt offenbar die Darstellung einer abelschen Gruppe als direkte Summe der *kleinstmöglichen* Anzahl zyklischer Gruppen (und analog Satz 14.29 für Moduln über Hauptidealringen). Nun kann man die zyklischen Gruppen $\mathbb{Z}/d\mathbb{Z}$ aber manchmal als Produkt von mehreren (nichttrivialen) zyklischen Gruppen schreiben: Nach dem Chinesischen Restsatz 9.9 ist, wenn $d = \prod_{i=1}^m p_i^{e_i}$ die Primfaktorzerlegung ist,

$$\mathbb{Z}/d\mathbb{Z} \cong \prod_{i=1}^m \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

als Ringe, was einen Isomorphismus

$$\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_m^{e_m}\mathbb{Z}$$

der additiven Gruppen induziert. Daraus ergibt sich die Existenzaussage im folgenden Satz. Die Eindeutigkeit folgt aus der Eindeutigkeitsaussage in Satz 14.30

14.31. **Klassifikationssatz für endliche abelsche Gruppen, 2. Version.** *Jede endliche abelsche Gruppe A ist eine direkte Summe von endlich vielen zyklischen abelschen Gruppen, deren Ordnung eine (echte) Primzahlpotenz ist. Die Ordnungen der Summanden sind bis auf die Reihenfolge eindeutig bestimmt.*

Diese Version des Klassifikationssatzes liefert die Darstellung als direkte Summe von *maximal* vielen nichttrivialen zyklischen Gruppen.

Satz 14.31 lässt sich auch für Moduln über Hauptidealringen formulieren; die Formulierung ist aber etwas umständlicher.

In diesem Zusammenhang möchte ich noch einige Begriffe und Tatsachen aufführen, die manchmal nützlich sind.

14.32. **Definition.** Sei R ein Ring und M ein R-Modul.

(1) Ein Element $0 \neq m \in M$ heißt *Torsionselement*, wenn es ein Element $0 \neq r \in R$ gibt mit $rm = 0$.
(2) M heißt *Torsionsmodul*, wenn alle $0 \neq m \in M$ Torsionselemente sind.
(3) M heißt *torsionsfrei*, wenn M keine Torsionselemente enthält.

Eine endlich erzeugte abelsche Gruppe (oder $\mathbb{Z}$-Modul) ist zum Beispiel genau dann eine Torsionsgruppe, wenn sie endlich ist. Allgemeiner gilt:

14.33. **Proposition.** *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul, und seien k und r die zu M gehörigen Zahlen aus Satz 14.29. Dann gilt:*

(1) *M ist Torsionsmodul genau dann, wenn $r = 0$.*
(2) *M ist torsionsfrei genau dann, wenn $k = 0$.*

Beweis. Übung. □

Insbesondere folgt:

14.34. **Proposition.** *Sei R ein Hauptidealring.*

(1) *Jeder endlich erzeugte torsionsfreie R-Modul ist frei.*
(2) *Jeder Untermodul von R^n ist frei.*

Beweis. Übung. □

15. Quadratische Reste und das Quadratische Reziprozitätsgesetz

Unser nächstes Ziel ist die Beantwortung der folgenden Frage:

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Wie stellt man fest, ob die Kongruenz

$$x^2 \equiv a \bmod p$$

in $\mathbb{Z}$ lösbar ist?

Die Antwort wird durch das *Quadratische Reziprozitätsgesetz* geliefert.

Zuerst müssen wir aber ein Resultat über Untergruppen der multiplikativen Gruppe eines Körpers beweisen. Der Vollständigkeit halber wiederholen wir die Definition einer Gruppe und geben die Definition, was eine Untergruppe ist.

15.1. **Definition.** Eine *Gruppe* ist ein Quadrupel $(G, e, *, i)$, bestehend aus einer Menge G, einem Element $e \in G$, einer Verknüpfung $* : G \times G \to G$ und einer Abbildung $i : G \to G$, die die folgenden Bedingungen erfüllen:

(1) $\forall g \in G : e * g = g * e = g$ (e ist neutrales Element).
(2) $\forall g_1, g_2, g_2 \in G : g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ (Assoziativität).
(3) $\forall g \in G : g * i(g) = i(g) * g = e$ (Inverses).

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

(4) $\forall g_1, g_2 \in G : g_1 * g_2 = g_2 * g_1$ (Kommutativität).

Abelsche Gruppen werden gerne in der Form $(G, 0, +, -)$ geschrieben. Häufig ist für beliebige Gruppen auch die Notation $(G, 1, \cdot, x \mapsto x^{-1})$ gebräuchlich. Sind die weiteren Daten aus dem Kontext klar, sprechen wir einfach von „der Gruppe G“.

15.2. **Definition.** Sei $(G, e, *, i)$ eine Gruppe. Eine *Untergruppe* von G ist eine Teilmenge U von G mit folgenden Eigenschaften:

(1) $e \in U$.
(2) $\forall u, u' \in U : u * u' \in U$.
(3) $\forall u \in U : i(u) \in U$.

(D.h., U enthält das neutrale Element und ist unter der Verknüpfung und unter Inversenbildung abgeschlossen.) Es ist dann klar, dass $(U, e, *|_{U\times U}, i|_U)$ wieder eine Gruppe ist.

Wir hatten früher bereits für jeden Ring R seine *Einheitengruppe* $R^\times$ definiert (das ist die Menge der multiplikativ invertierbaren Elemente von R mit der Multiplikation von R als Verknüpfung). Ist R ein Körper K, spricht man auch von der *multiplikativen Gruppe* $K^\times$ von K (dann ist $K^\times = K \setminus \{0\}$ als Menge). Da die Multiplikation in einem Körper kommutativ ist, ist $K^\times$ eine *abelsche* Gruppe. Unser erstes Resultat macht eine Aussage über endliche Untergruppen dieser multiplikativen Gruppe.

15.3. **Satz.** *Sei K ein Körper und $G \subset K^\times$ eine endliche Untergruppe. Dann ist G zyklisch (d.h., eine zyklische abelsche Gruppe im Sinn des vorigen Kapitels).*

Beweis. Als endliche abelsche Gruppe ist G nach Satz 14.30 isomorph zu einer direkten Summe $\mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_k\mathbb{Z}$ mit positiven ganzen Zahlen $d_1 \mid \ldots \mid d_k$ und $d_1 > 1$. Wir können annehmen, dass $G \neq \{1\}$ ist (anderenfalls ist die Aussage trivialerweise richtig); das bedeutet $k \geq 1$. Zu zeigen ist $k = 1$. Dazu nehmen wir das Gegenteil an: $k \geq 2$. Dann ist d_k ein *echter* Teiler der Gruppenordnung $\#G = d_1 \cdots d_k$. Das d_k-fache jedes Elements von $\mathbb{Z}/d_1\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}/d_k\mathbb{Z}$ ist null (hier brauchen wir die Teilerbedingung). Übersetzt auf die multiplikativ geschriebene Gruppe G bedeutet das $g^{d_k} = 1$ für alle $g \in G$. Damit sind alle $\#G > d_k$ Elemente von G Nullstellen des Polynoms $x^{d_k} - 1$ vom Grad d_k. Das ist ein Widerspruch zu Folgerung 11.9 (ein Polynom vom Grad n kann in einem Integritätsbereich höchstens n verschiedene Nullstellen haben). Also muss $k = 1$ sein, und $G \cong \mathbb{Z}/d_1\mathbb{Z}$ ist zyklisch. □

Das bedeutet, dass jede solche Gruppe G die Gruppe der n-ten Einheitswurzeln in K sein muss, für $n = \#G$. Zum Beispiel sieht man, dass die größte endliche Untergruppe von $\mathbb{R}^\times$ die Gruppe $\{\pm 1\}$ ist, und dass die endlichen Untergruppen von $\mathbb{C}^\times$ alle die Form $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ haben.

15.4. **Bemerkung.** Für einen Schiefkörper ist die Aussage von Satz 15.3 falsch, wie die Untergruppe $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ der multiplikativen Gruppe des Quaternionenschiefkörpers zeigt: Q ist nicht einmal kommutativ! Der Grund dafür ist, dass Folgerung 11.9 für einen Schiefkörper nicht gilt (alle acht Elemente von Q sind Nullstellen von $x^4 - 1$).

15.5. **Folgerung.** *Ist F ein endlicher Körper, dann ist seine multiplikative Gruppe $F^\times$ zyklisch.*

Beweis. In diesem Fall ist die ganze Gruppe $F^\times$ endlich, so dass Satz 15.3 auf sie angewendet werden kann. □

Wir kennen bereits endliche Körper: Ist p eine Primzahl, dann ist der Faktorring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper; $\mathbb{F}_p$ hat p Elemente, also hat die (zyklische) Gruppe $\mathbb{F}_p^\times$ genau $p - 1$ Elemente.

15.6. **Definition.** Sei p eine Primzahl. Eine ganze Zahl a heißt *Primitivwurzel mod p*, wenn die Restklasse $[a] \in \mathbb{F}_p$ die multiplikative Gruppe $\mathbb{F}_p^\times$ erzeugt.

Nach Folgerung 15.5 gibt es für jede Primzahl p Primitivwurzeln mod p. Die Anzahl der Restklassen mod p, die aus Primitivwurzeln mod p bestehen, ist gegeben durch $\phi(p-1)$ (Eulersche ϕ-Funktion). Für die ersten paar Primzahlen finden wir folgende Primitivwurzeln zwischen 1 und $p - 1$:

p	2	3	5	7	11
Primitivwurzeln mod p	1	2	2, 3	3, 5	2, 6, 7, 8

Zum Beispiel ist 3 eine Primitivwurzel mod 7, weil alle Elemente von $\mathbb{F}_7^\times$ als Potenzen von [3] geschrieben werden können:

$$[3]^0 = [1],\ [3]^1 = [3],\ [3]^2 = [9] = [2],\ [3]^3 = [6],\ [3]^4 = [18] = [4],\ [3]^5 = [12] = [5]$$

Dagegen ist 2 keine Primitivwurzel mod 7, denn man erhält nur drei Elemente als Potenzen von [2]:

$$[2]^0 = [1], \quad [2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [8] = [1]\,.$$

In diesem Zusammenhang gibt es die

15.7. **Vermutung von Artin (1927).** *Ist $a \in \mathbb{Z}$ mit $a \neq -1$ und a kein Quadrat, dann gibt es unendlich viele Primzahlen p, so dass a eine Primitivwurzel mod p ist.*

(Warum muss man -1 und die Quadrate ausschließen?)

Diese Vermutung ist immer noch offen. Die besten Ergebnisse sind von der folgenden Art:

Es gibt höchstens zwei Primzahlen a, für die die Artin-Vermutung nicht gilt.[1]

Auf der anderen Seite ist die Vermutung aber noch für keine einzige konkrete Zahl a bewiesen!

Ist a eine Primitivwurzel mod p, dann gibt es für jede nicht durch p teilbare ganze Zahl x einen Exponenten k mit $x \equiv a^k \bmod p$. Da $[a] \in \mathbb{F}_p^\times$ eine (multiplikative) Gruppe mit $p - 1$ Elementen erzeugt, gilt $a^{p-1} \equiv 1 \bmod p$ („kleiner Satz von Fermat“). Das bedeutet, dass k nur mod $p - 1$ eindeutig bestimmt ist.

[1] D.R. Heath-Brown, *Artin's conjecture for primitive roots,* Quart. J. Math. Oxford Ser. **37** (1), 27–38 (1986).

15.8. **Definition.** Jedes $k \in \mathbb{Z}$ (oder auch die Restklasse von k in $\mathbb{Z}/(p-1)\mathbb{Z}$) wie oben heißt *diskreter Logarithmus* mod p von x zur Basis a. Wir schreiben

$$\log_a x = k \qquad \text{oder} \qquad \log_{[a]}[x] = k\,;$$

es muss dabei aus dem Kontext klar sein, modulo welcher Primzahl p man rechnet.

15.9. **Definition.** Sei p eine ungerade Primzahl (also $p > 2$) und a eine nicht durch p teilbare ganze Zahl. Ist die Kongruenz $x^2 \equiv a \bmod p$ in $\mathbb{Z}$ lösbar, dann heißt a ein *quadratischer Rest* (QR) mod p. Andernfalls heißt a ein *quadratischer Nichtrest* (QNR) mod p.

Für beliebiges $a \in \mathbb{Z}$ definieren wir das *Legendre-Symbol* wir folgt:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p \mid a \\ 1 & \text{falls } a \text{ quadratischer Rest mod } p \\ -1 & \text{falls } a \text{ quadratischer Nichtrest mod } p \end{cases}$$

Aus der Definition folgt unmittelbar:

$$a \equiv b \bmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Hier ist eine kleine Tabelle mit den quadratischen Resten bzw. Nichtresten zwischen 1 und $p-1$:

p	3	5	7	11	13	17
QR	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12	1, 2, 4, 8, 9, 13, 15, 16
QNR	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11	3, 5, 6, 7, 10, 11, 12, 14

Es fällt auf, dass es stets genau so viele quadratische Reste wie Nichtreste gibt. Das ist kein Zufall, wie das folgende Ergebnis zeigt.

15.10. **Satz.** *Sei p eine ungerade Primzahl und g eine Primitivwurzel mod p.*

(1) *Ist $a \in \mathbb{Z}$, $p \nmid a$, dann ist a quadratischer Rest mod p genau dann, wenn $\log_g a$ gerade ist. Insbesondere gibt es genau $\frac{p-1}{2}$ Restklassen mod p, die aus quadratischen Resten bestehen, und genau $\frac{p-1}{2}$ Restklassen mod p, die aus quadratischen Nichtresten bestehen.*

(2) *Für $a, b \in \mathbb{Z}$ gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(3) *(**Euler-Kriterium**) Für $a \in \mathbb{Z}$ gilt*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p\,.$$

Beweis.

(1) Ist a QR mod p, dann gibt es $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod p$. Außerdem ist $x \equiv g^m \bmod p$ mit $m = \log_g x$, also $a \equiv x^{2m} \bmod p$, d.h., $\log_g a = 2m$ ist gerade. (Beachte, dass die Aussage „$\log_g a$ ist gerade“ sinnvoll ist, obwohl der diskrete Logarithmus nur modulo $p-1$ definiert ist, denn $p-1$ ist gerade.)

Ist umgekehrt $\log_g a = 2m$ gerade, dann folgt analog mit $x = g^m$, dass $x^2 \equiv a \bmod p$ ist; damit ist a QR mod p.

(2) Die Aussage ist klar wenn p ein Teiler von a oder b ist (dann sind beide Seiten null). Wir können also $p \nmid ab$ annehmen. In diesem Fall lässt sich die Aussage aus Teil (1) schreiben als

$$\left(\frac{a}{p}\right) = (-1)^{\log_g a}.$$

Es folgt

$$\left(\frac{ab}{p}\right) = (-1)^{\log_g(ab)} = (-1)^{\log_g a + \log_g b} = (-1)^{\log_g a}(-1)^{\log_g b} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(3) Die Aussage ist klar für $p \mid a$ (beide Seiten sind null mod p). Sei also $p \nmid a$ und $k = \log_g a$. Wegen $g^{p-1} \equiv 1 \bmod p$ gilt $g^{(p-1)/2} \equiv \pm 1 \bmod p$ (denn $\mathbb{F}_p$ ist ein Körper; die Gleichung $x^2 = [1]$ hat also nur die beiden (wegen $p \neq 2$ verschiedenen) Lösungen $[1]$ und $[-1]$). Es kann nicht $g^{(p-1)/2} \equiv 1 \bmod p$ gelten, denn dann könnte $[g]$ keine Gruppe mit $p-1$ Elementen erzeugen. Also gilt $g^{(p-1)/2} \equiv -1 \bmod p$. Es folgt

$$\left(\frac{a}{p}\right) = (-1)^k \equiv g^{\frac{p-1}{2}k} = (g^k)^{(p-1)/2} \equiv a^{(p-1)/2} \bmod p.$$

□

Daraus können wir schon einmal ableiten, wann -1 ein quadratischer Rest mod p ist und wann nicht.

15.11. **Folgerung.** *Sei p eine ungerade Primzahl. Dann gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4, \\ -1 & \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

Beweis. Nach Satz 15.10, Teil (3), gilt

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p.$$

Da beide Seiten den Wert ± 1 haben und $p > 2$ ist, folgt Gleichheit. □

Also ist -1 quadratischer Rest mod p genau dann, wenn $p \equiv 1 \bmod 4$ ist. Die Aussage von Folgerung 15.11 wird auch als *Erstes Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz* bezeichnet. Der Grund dafür wird später klar werden.

Wie sieht es damit aus, wann 2 quadratischer Rest mod p ist? Hier ist eine Tabelle mit Einträgen $+$ für „ja“ und $-$ für „nein“:

	$3:-$	$5:-$	$7:+$
	$11:-$	$13:-$	
$17:+$	$19:-$		$23:+$
		$29:-$	$31:+$
		$37:-$	
$41:+$	$43:-$		$47:+$

Es drängt sich folgende Vermutung auf:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \text{ oder } 7 \bmod 8, \\ -1 & \text{falls } p \equiv 3 \text{ oder } 5 \bmod 8. \end{cases}$$

Wir werden bald einen Beweis dafür geben. Erst brauchen wir aber noch einige Vorbereitungen.

15.12. **Definition.** Sei R' ein Ring, $R \subset R'$ ein Unterring und $A \subset R'$ eine Teilmenge. Dann bezeichnen wir mit $R[A]$ (im Fall $A = \{a_1, \ldots, a_n\}$ auch $R[a_1, \ldots, a_n]$ geschrieben) den *von A über R erzeugten Unterring* von R', also

$$R[A] = \bigcap \{S \mid S \text{ Unterring von } R' \text{ mit } R \subset S \text{ und } A \subset S\}\,.$$

15.13. **Lemma.** *Sei R' ein Ring, $R \subset R'$ ein Unterring, und $a \in R'$. Dann gilt*

$$R[a] = \{f(a) \mid f \in R[x]\}$$

(wobei $R[x]$ der Polynomring ist).

Beweis. Die rechte Seite ist das Bild des Einsetzungshomomorphismus $R[x] \to R'$, der x auf a abbildet; diese Menge ist also ein Unterring von R'. Auf der anderen Seite ist klar, dass jeder R und a enthaltende Unterring von R' auch alle $f(a)$ mit Polynomen $f \in R[x]$ enthalten muss. Die Menge rechts ist also der kleinste Unterring von R', der $R \cup \{a\}$ enthält, also definitionsgemäß gleich $R[a]$. □

Wir haben diese Schreibweise schon früher verwendet, zum Beispiel $\mathbb{Z}[i]$ für die ganzen gaußschen Zahlen oder $\mathbb{Z}[\sqrt{2}]$. Diese Ringe sind Spezialfälle (für $R' = \mathbb{C}$, $R = \mathbb{Z}$ und $f = x^2 + 1$ bzw. $f = x^2 - 2$) des folgenden Sachverhalts.

15.14. **Lemma.** *Sei R' ein Integritätsbereich, $R \subset R'$ ein Unterring, und $a \in R'$ eine Nullstelle des normierten Polynoms $f \in R[x]$ vom Grad n. Wir nehmen an, dass f in $K[x]$ irreduzibel ist, wobei K der Quotientenkörper von R ist. Dann lassen sich die Elemente von $R[a]$ eindeutig in der Form*

$$r_0 + r_1 a + r_2 a^2 + \ldots + r_{n-1} a^{n-1}$$

schreiben, wobei $r_0, r_1, \ldots, r_{n-1} \in R$. Insbesondere gilt $(R[a])^\times \cap R = R^\times$.

Beweis. Nach Lemma 15.13 haben alle Elemente von $R[a]$ die Form $h(a)$ mit einem Polynom $h \in R[x]$. Nach Satz 11.8 (Division mit Rest für Polynome) gibt es Polynome $q, r \in R[x]$ mit $h = qf + r$ und $\deg(r) \leq n - 1$, also

$$r = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}\,.$$

Anwenden des Einsetzungshomomorphismus $x \mapsto a$ liefert

$$h(a) = q(a)f(a) + r(a) = r(a) = r_0 + r_1 a + \ldots + r_{n-1} a^{n-1}\,.$$

Damit ist gezeigt, dass sich jedes Element in der angegebenen Weise schreiben lässt. Es bleibt die Eindeutigkeit zu zeigen, d.h. die Injektivität der R-linearen Abbildung

$$\phi : R^n \longrightarrow R[a]\,, \quad (r_0, r_1, \ldots, r_{n-1}) \longmapsto r_0 + r_1 a + \ldots + r_{n-1} a^{n-1}\,.$$

Wir betrachten den Kern von ϕ: Sei $(r_0, \ldots, r_{n-1}) \in R^n$ mit $\phi(r_0, \ldots, r_{n-1}) = 0$. Das bedeutet für das Polynom $r = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} \in R[x]$, dass $r(a) = 0$ ist. Wir nehmen jetzt an, dass $r \neq 0$ ist und wollen daraus einen Widerspruch ableiten. Sei K der Quotientenkörper von R, dann ist $K[x]$ ein Hauptidealring, und wir können r und f auch als Elemente von $K[x]$ auffassen. Da f in $K[x]$ irreduzibel ist und $0 \leq \deg(r) < \deg(f)$, sind r und f in $K[x]$ teilerfremd, also gibt es Polynome $u_1, v_1 \in K[x]$ mit $u_1 r + v_1 f = 1$. Durch Multiplikation mit

einem gemeinsamen Nenner $d \in R \setminus \{0\}$ erhalten wir $u = du_1, v = dv_1 \in R[x]$ und $ur + vf = d$. Einsetzen von a liefert den Widerspruch

$$0 = u(a)r(a) + v(a)f(a) = d\,.$$

Also muss $r = 0$, sein; damit ist ϕ injektiv.

Für den Beweis des Zusatzes sei $u \in (R[a])^\times \cap R$. Dann gibt es $v = r_0 + r_1 a + \ldots + r_{n-1}a$ mit $uv = 1$. Wir erhalten die Relation

$$1 = uv = (ur_0) + (ur_1)a + \ldots + (ur_{n-1})a^{n-1}\,.$$

Da die Darstellung als R-Linearkombination von $1, a, \ldots, a^{n-1}$ eindeutig ist, folgt $ur_0 = 1$, also $u \in R^\times$. Die umgekehrte Inklusion ist trivial. □

15.15. **Lemma.** *Sei R ein Ring, der $\mathbb{Z}$ enthält, und sei p eine Primzahl. Dann gilt in R:*

$$(r_1 + r_2 + \ldots + r_n)^p \equiv r_1^p + r_2^p + \ldots + r_n^p \bmod Rp\,.$$

Beweis. Es genügt der Fall $n = 2$ ($n < 2$ ist trivial, der allgemeine Fall folgt dann durch Induktion). Es gilt

$$(r_1 + r_2)^p = \sum_{j=0}^{p} \binom{p}{j} r_1^{p-j} r_2^j = r_1^p + \binom{p}{1} r_1^{p-1} r_2 + \ldots + \binom{p}{p-1} r_1 r_2^{p-1} + r_2^p\,,$$

wobei alle Terme außer dem ersten und letzten durch p teilbar sind, denn die entsprechenden Binomialkoeffizienten sind durch p teilbar (in $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ teilt p den Zähler, aber nicht den Nenner). Die Behauptung folgt. □

15.16. **Bemerkung.** Äquivalent kann man Lemma 15.15 auch so formulieren:

Sei R ein Ring und p eine Primzahl, so dass in R gilt $p \cdot 1 = 0$. Dann gilt für $r_1, \ldots, r_n$ in R stets $(r_1 + \ldots + r_n)^p = r_1^p + \ldots + r_n^p$.

Diese Aussage ist (vor allem in den USA) auch als „Freshman's Dream" bekannt (Freshman = Studienanfänger), weil sich damit Potenzen von Summen so schön vereinfachen lassen. Die Implikation 15.16 $\Longrightarrow$ 15.15 bekommt man durch Betrachtung von R/Rp.

Jetzt können wir unsere Vermutung beweisen.

15.17. **Satz.** *Ist p eine ungerade Primzahl, dann gilt*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{falls } p \equiv 1 \text{ oder } 7 \bmod 8, \\ -1 & \text{falls } p \equiv 3 \text{ oder } 5 \bmod 8. \end{cases}$$

Beweis. Sei $\tau \in \mathbb{C}$ eine Zahl mit $\tau^4 = -1$, und sei $R = \mathbb{Z}[\tau]$. Dann gilt

$$(\tau + \tau^{-1})^2 = \tau^2 + 2 + \tau^{-2} = 2 + \tau^{-2}(\tau^4 - 1) = 2$$

und, für n ungerade,

$$\tau^n + \tau^{-n} = (-1)^{(n^2-1)/8}(\tau + \tau^{-1})\,.$$

(Denn $\tau^3 = -\tau^{-1}$, $\tau^5 = -\tau$, etc.) Wir haben dann folgende Kongruenzen mod Rp:

$$(\tau + \tau^{-1})^p \equiv \tau^p + \tau^{-p} = (-1)^{(p^2-1)/8}(\tau + \tau^{-1})$$

und

$$(\tau+\tau^{-1})^p = \big((\tau+\tau^{-1})^2\big)^{(p-1)/2}(\tau+\tau^{-1}) = 2^{(p-1)/2}(\tau+\tau^{-1}) \equiv \left(\frac{2}{p}\right)(\tau+\tau^{-1})\,.$$

Durch Multiplikation mit $(\tau+\tau^{-1})$ ergibt sich

$$2(-1)^{(p^2-1)/8} \equiv 2\left(\frac{2}{p}\right) \bmod Rp\,,$$

und weil 2 mod p invertierbar ist (p ist ungerade), folgt

$$(-1)^{(p^2-1)/8} \equiv \left(\frac{2}{p}\right) \bmod Rp\,.$$

Nach Lemma 15.14 (beachte, dass $x^4+1 \in \mathbb{Z}[x]$ irreduzibel ist), ist p keine Einheit in $\mathbb{Z}[\tau]$. Wegen p ungerade gilt dann auch $2 \notin Rp$. Daher können wir aus der Kongruenz mod Rp oben auf Gleichheit schließen. □

Obige Aussage heißt auch das *Zweite Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz*. Nachdem wir nun zwei „Ergänzungsgesetze“ kennen, stellt sich natürlich die Frage, was das *Quadratische Reziprozitätsgesetz* selbst aussagt. Wir bemerken dafür zunächst, dass ein Teil der Aussage der Ergänzungsgesetze sich auch wie folgt formulieren lässt:

- Ob -1 quadratischer Rest oder Nichtrest mod p ist, hängt nur von p mod 4 ab.
- Ob 2 quadratischer Rest oder Nichtrest mod p ist, hängt nur von p mod 8 ab.

Die Frage, die sich dann stellt, ist, ob sich das verallgemeinern lässt:

- Ob a quadratischer Rest oder Nichtrest mod p ist, hängt nur von p mod $N(a)$ ab.

Dabei wäre noch ein geeigneter Wert für $N(a)$ zu bestimmen. Wegen der Multiplikativität des Legendre-Symbols, genügt es, Primzahlen a zu betrachten. Wenn man sich ähnliche Tabellen macht wie oben für $a=2$, findet man folgende wahrscheinliche Werte für $N(a)$:

a	3	5	7	11	13	17	19	23
$N(a)$	12	5	28	44	13	17	76	92

Man könnte also folgende Vermutung formulieren: Für eine ungerade Primzahl q gilt

$$N(q) = \begin{cases} q & \text{falls } q \equiv 1 \bmod 4, \\ 4q & \text{falls } q \equiv 3 \bmod 4. \end{cases}$$

Das Quadratische Reziprozitätsgesetz zeigt, dass diese Vermutung richtig ist, und sagt auch noch, wie man $\left(\frac{q}{p}\right)$ bestimmen kann. Zuerst noch eine Definition.

15.18. **Definition.** Sei p eine ungerade Primzahl. Dann sei

$$p^* = (-1)^{(p-1)/2}p = \begin{cases} p & \text{falls } p \equiv 1 \bmod 4, \\ -p & \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

Es gilt dann stets $p^* \equiv 1 \bmod 4$.

15.19. **Satz (Quadratisches Reziprozitätsgesetz).** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Das bedeutet: Für $p \equiv 1 \bmod 4$ oder $q \equiv 1 \bmod 4$ gilt $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Im anderen Fall $p \equiv q \equiv 3 \bmod 4$ gilt dagegen $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Bevor wir uns über einen Beweis Gedanken machen, überlegen wir uns, dass daraus wirklich unsere Vermutung über $N(q)$ folgt:

- Ist $q \equiv 1 \bmod 4$, dann gilt stets $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, und das Symbol $\left(\frac{p}{q}\right)$ hängt nur von $p \bmod q$ ab.
- Ist $q \equiv 3 \bmod 4$, dann gilt $\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$. Der erste Faktor hängt nur von $p \bmod 4$ ab, der zweite nur von $p \bmod q$. Das Produkt hängt also nur von $p \bmod 4q$ ab.

Wir werden das Quadratische Reziprozitätsgesetz als „QRG“ abkürzen. Mit Hilfe des QRG und seiner Ergänzungsgesetze kann man nun Legendre-Symbole, die größere Zahlen enthalten, recht bequem auswerten. Zum Beispiel:

$$\begin{aligned}\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{42}{67}\right) &= \left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{7}{67}\right) \\ &= (-1)(-\left(\frac{67}{3}\right))(-\left(\frac{67}{7}\right)) = -\left(\frac{1}{3}\right)\left(\frac{4}{7}\right) = -1\,.\end{aligned}$$

Oder alternativ:

$$\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{-25}{67}\right) = \left(\frac{-1}{67}\right)\left(\frac{5}{67}\right)^2 = -1\,.$$

Wir wollen das QRG auf ähnliche Weise beweisen wie das Zweite Ergänzungsgesetz. Dazu überlegen wir noch einmal, was wir dafür gebraucht haben:

- Einen geeigneten Ring R, in dem p keine Einheit ist;
- Ein Element $\gamma \in R$ mit $\gamma^2 = 2$ und $\gamma^p \equiv (-1)^{(p^2-1)/8}\gamma \bmod Rp$.

Wir wollen hier die 2 durch eine Primzahl p (und p durch q) ersetzen. Wir brauchen dann ein $\gamma \in R$ mit

- $\gamma^2 = p^*$ und
- $\gamma^q \equiv \left(\frac{q}{p}\right)\gamma \bmod Rq$.

Gauß (der das QRG als Erster vollständig bewies und in seinem Leben sieben verschiedene Beweise dafür fand) hat diese Elemente γ gefunden, deswegen werden sie heute nach ihm benannt.

15.20. **Definition.** Sei p eine ungerade Primzahl. Wir setzen $\zeta = e^{2\pi i/p} \in \mathbb{C}$ und $R = \mathbb{Z}[\zeta]$. Für $a \in \mathbb{Z}$ heißt

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)\zeta^{aj} \in R$$

eine *Gaußsche Summe* (zur Primzahl p). Für g_1 schreiben wir auch einfach g (die Primzahl p muss aus dem Kontext klar sein) und nennen es *die* Gaußsche Summe.

15.21. **Lemma.** *Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$, und ζ wie oben.*

(1) *Es gilt* $\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0$.
(2) *Es gilt* $\sum_{j=0}^{p-1} \zeta^{aj} = 0$, *falls* $p \nmid a$; *im anderen Fall ist der Wert* p.
(3) $g_a = \left(\frac{a}{p}\right) g$.
(4) $g^2 = p^*$.

Beweis.

(1) Das ist lediglich eine andere Formulierung der Aussage, dass es genauso viele quadratische Reste wie Nichtreste mod p gibt.
(2) Die Aussage für $p \mid a$ ist klar (dann gilt $\zeta^a = 1$). Es gelte also $p \nmid a$ und damit $\zeta^a \neq 1$. Es folgt
$$\sum_{j=0}^{p-1} \zeta^{aj} = \sum_{j=1}^{p} \zeta^{aj} = \zeta^a \sum_{j=0}^{p-1} \zeta^{aj} \,,$$
also $(1-\zeta^a)\sum_{j=0}^{p-1} \zeta^{aj} = 0$. Wegen $\zeta^a \neq 1$ folgt die Behauptung.
(3) Für $p \mid a$ folgt die Behauptung aus Teil (1). Es gelte also $p \nmid a$, dann gibt es $a' \in \mathbb{Z}$ mit $aa' \equiv 1 \bmod p$. Aus der Multiplikativität des Legendre-Symbols folgt $\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right)$. Mit j durchläuft auch $a'j$ alle Restklassen mod p, also erhalten wir
$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj} = \sum_{j=0}^{p-1} \left(\frac{a'j}{p}\right) \zeta^{j} = \left(\frac{a'}{p}\right) \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{j} = \left(\frac{a}{p}\right) g \,.$$
(4) Wir haben
$$\begin{aligned}(p-1)g^2 = \sum_{a=0}^{p-1} g_a^2 &= \sum_{a=0}^{p-1} \sum_{j,k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \zeta^{aj+ak} \\ &= \sum_{j,k=0}^{p-1} \left(\frac{jk}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(j+k)} = \sum_{j,k=0}^{p-1} \left(\frac{jk}{p}\right) \begin{cases} 0 & \text{falls } p \nmid j+k \\ p & \text{falls } p \mid j+k \end{cases} \\ &= \sum_{j=0}^{p-1} \left(\frac{-j^2}{p}\right) p = \left(\frac{-1}{p}\right) p(p-1)\end{aligned}$$
(unter Verwendung von (3) und (2)), also $g^2 = \left(\frac{-1}{p}\right) p = p^*$.

□

Wir bemerken noch, dass gilt $\zeta^p = 1$, aber $\zeta \neq 1$, also ist ζ eine Nullstelle des Polynoms
$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \,.$$
Diese Polynom ist irreduzibel in $\mathbb{Q}[x]$ (sei f das Polynom, dann ist auf $f(x+1) = ((x+1)^p - 1)/x = x^p + px^{p-1} + \ldots + p$ das Eisenstein-Kriterium anwendbar). Nach Lemma 15.14 ist also keine Primzahl q eine Einheit in $R = \mathbb{Z}[\zeta]$

Der Beweis ist nun analog wie für das Zweite Ergänzungsgesetz.

Beweis von Satz 15.19. Sei $\zeta = e^{2\pi i/p}$ und $R = \mathbb{Z}[\zeta]$ wie oben. Sei $g \in R$ die Gaußsche Summe für p. Dann gilt modulo Rq:

$$g^q = (g^2)^{(q-1)/2} \cdot g = (p^*)^{(q-1)/2} g \equiv \left(\frac{p^*}{q}\right) g$$

und

$$g^q \equiv \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)^q \zeta^{qj} = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{qj} = g_q = \left(\frac{q}{p}\right) g\,.$$

Es folgt $\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \bmod Rq$; nach Multiplikation mit g haben wir dann $\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \bmod Rq$. Da $p^* \bmod q$ invertierbar ist, folgt $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \bmod Rq$. Da q in R keine Einheit und außerdem ungerade ist, folgt daraus die Gleichheit der Symbole. □

15.22. **Bemerkung.** Ein Nachteil bei der oben angedeuteten Methode, ein Legendre-Symbol mit Hilfe des QRG und seiner Ergänzungsgesetze zu berechnen, besteht darin, dass man die obere Zahl, die in den während der Rechnung angetroffenen Symbolen auftritt, faktorisieren muss. Das ist aber nicht wirklich nötig. Dazu erweitert man die Definition des Legendre-Symbols: Ist $n > 0$ ungerade mit Primfaktorzerlegung $n = \prod_i p_i^{e_i}$, dann definiert man für $a \in \mathbb{Z}$

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i}\,;$$

man nennt das Symbol dann *Jacobi-Symbol*. Es ist in beiden Argumenten multiplikativ. Das QRG und die Ergänzungsgesetze gelten dann auch für das Jacobi-Symbol:

Seien m und n zwei positive ungerade Zahlen. Dann gilt:

(1) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$;

(2) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;

(3) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Der Beweis ist eine Übungsaufgabe.

Damit lässt sich die Faktorisierung (abgesehen vom Abspalten des Vorzeichens und einer Potenz von 2) bei der Berechnung vermeiden:

$$\begin{aligned}\left(\frac{887}{1009}\right) = \left(\frac{1009}{887}\right) = \left(\frac{122}{887}\right) = \left(\frac{2}{887}\right)\left(\frac{61}{887}\right) = \left(\frac{887}{61}\right)\\ = \left(\frac{33}{61}\right) = \left(\frac{61}{33}\right) = \left(\frac{28}{33}\right) = \left(\frac{7}{33}\right)\\ = \left(\frac{33}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1\end{aligned}$$

Was jedoch im allgemeinen **nicht mehr** stimmt, ist die Implikation

$$\left(\frac{a}{n}\right) = 1 \implies a \text{ QR mod } n\,.$$

Zum Beispiel gilt $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, aber 2 ist *kein* Quadrat mod 15 (da kein Quadrat mod 3 und mod 5).

16. Gruppen und Gruppenhomomorphismen

Wir beginnen nun mit einem neuen Thema: der Gruppentheorie. Was eine *Gruppe* ist, wissen wir bereits, und auch den Begriff der *Untergruppe* haben wir bereits kennen gelernt. Bevor wir uns weiteren relevanten Begriffen zuwenden, wollen wir uns erst einmal einige Beispiele von Gruppen ansehen. Eine reichhaltige Quelle von Gruppen (und einer der Gründe dafür, dass Gruppen in der Mathematik so wichtig sind) sind *Symmetrie-* oder *Automorphismengruppen*.

Allgemein ist ein *Automorphismus* eines Objekts X eine Struktur erhaltende Abbildung $\phi : X \to X$, die invertierbar ist (und so dass die inverse Abbildung ebenfalls Struktur erhaltend ist). Wir kennen das zum Beispiel von Ringen, Vektorräumen oder R-Moduln. Ist X einfach eine Menge ohne zusätzliche Struktur, dann ist ein Automorphismus von X nichts anderes als eine *Permutation* von X, also eine bijektive Abbildung $X \to X$. Ist X ein topologischer Raum oder eine differenzierbare Mannigfaltigkeit, dann geht es um *Homöomorphismen* oder *Diffeomorphismen* $X \to X$. In jedem Fall gilt:

16.1. **Proposition.** *Die Menge der Automorphismen von X bildet mit der Komposition von Abbildungen als Verknüpfung eine Gruppe.*

Diese Gruppe heißt dann die *Automorphismengruppe* von X, geschrieben $\mathrm{Aut}(X)$.

Beweis. „Morphismen“ haben immer die Eigenschaft, dass die Komposition von zwei Morphismen wieder ein Morphismus ist. Die Assoziativität der Verknüpfung ist klar (denn sie gilt allgemein für die Komposition von Abbildungen). Die Identität id_X ist das neutrale Element, der inverse Morphismus (der jeweils existiert, weil wir Automorphismen betrachten) ist das inverse Element. □

16.2. **Beispiele.**

(1) Die Permutationen einer Menge X bilden eine Gruppe, die *symmetrische Gruppe* $S(X)$. Ist $X = \{1, 2, \ldots, n\}$, dann schreiben wir auch S_n für $S(X)$.
(2) Ist V ein Vektorraum über einem Körper K, dann heißt die Automorphismengruppe von V (die aus allen invertierbaren K-linearen Abbildungen $V \to V$ besteht) die *allgemeine lineare Gruppe* von V, geschrieben $\mathrm{GL}(V)$ (general linear group). Im Spezialfall $V = K^n$ schreiben wir auch $\mathrm{GL}_n(K)$; das ist die Gruppe der invertierbaren $n \times n$-Matrizen mit der Matrizenmultiplikation als Verknüpfung.
(3) Ist V ein *euklidischer* Vektorraum, dann erhalten wir als Automorphismengruppe von V die Gruppe $\mathrm{O}(V)$ der *orthogonalen Abbildungen*. Ist $V = \mathbb{R}^n$ mit dem Standard-Skalarprodukt, dann schreibt man auch $\mathrm{O}(n)$ für $\mathrm{O}(V)$.
(4) Die Untergruppe von $\mathrm{O}(2)$, die die Menge der Ecken eines regulären n-Ecks mit Zentrum im Ursprung auf sich abbildet, heißt *(n-te) Diedergruppe* und wird mit D_n bezeichnet. Sie besteht aus den Drehungen um Vielfache von $2\pi/n$ und den Spiegelungen an Ursprungsgeraden durch die Ecken oder Kantenmittelpunkte des n-Ecks. Man spricht hier auch von der *Symmetriegruppe* des regulären n-Ecks.
(5) Ist R ein Ring, dann können wir die Automorphismengruppe $\mathrm{Aut}(R)$ betrachten. Wir hatten zum Beispiel gesehen, dass $\mathrm{Aut}(\mathbb{Z}[i])$ aus genau zwei Elementen besteht.
(6) Auf einer einelementigen Menge gibt es genau eine Struktur als Gruppe. Eine solche Gruppe heißt *trivial*. Zum Beispiel sind S_0 und S_1 triviale Gruppen.

(7) Wir definieren die Gruppe $\mathbb{Z}_n$ für $n \in \mathbb{Z}_{>0}$ als die Menge $\{0, 1, 2, \ldots, n-1\}$ mit der Addition „modulo n“ als Verknüpfung: das Ergebnis ist der Rest der Summe bei Division durch n. Wir schreiben die Verknüpfung als Addition.

Wir werden die Gruppenverknüpfung meistens als Multiplikation schreiben, also $g \cdot h$ oder gh für $g * h$; das neutrale Element wird 1 geschrieben. Die *Potenzen* von g sind dann wie üblich definiert durch

$$g^0 = 1\,, \qquad g^{n+1} = g^n \cdot g\,, \qquad g^{-n} = (g^{-1})^n\,.$$

Dann gelten die Rechenregeln

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

wie man leicht durch Induktion beweist. Man beachte: Die Regel $(gh)^n = g^n \cdot h^n$ gilt im allgemeinen **nicht**, sondern nur, wenn zusätzlich $gh = hg$ gilt. (Übung: $(gh)^2 = g^2h^2 \iff gh = hg$)

Analog zur Situation bei Ringen oder R-Moduln gilt:

16.3. **Lemma.** *Sei G eine Gruppe. Beliebige Durchschnitte (über nicht-leere Familien) und aufsteigende Vereinigungen von Untergruppen von G sind wieder Untergruppen von G.*

Beweis. Analog zum Beweis von Lemma 14.9. □

Es ist also wieder folgende Definition sinnvoll.

16.4. **Definition.** Sei G eine Gruppe und $A \subset G$ eine Teilmenge. Die kleinste Untergruppe von G, die A enthält,

$$\langle A\rangle = \bigcap \{U \mid U \subset G \text{ Untergruppe mit } A \subset U\}\,,$$

heißt die *von A erzeugte Untergruppe* von G. Gilt $\langle A\rangle = G$, dann heißt A ein *Erzeugendensystem* von G. Wie üblich schreiben wir $\langle a_1, \ldots, a_n\rangle$, wenn $A = \{a_1, \ldots, a_n\}$ endlich ist. In diesem Fall heißt G *endlich erzeugt*. Gilt $G = \langle g\rangle$ für ein $g \in G$, dann heißt G *zyklisch*.

Man kann sich leicht davon überzeugen, dass $\langle A\rangle$ aus allen Produkten (beliebiger Länge) von Elementen von A und ihren Inversen besteht. Insbesondere gilt

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

Zum Beispiel ist $\mathbb{Z}_n$ zyklisch, denn die Gruppe wird von 1 erzeugt. Ebenso ist (die additive Gruppe von) $\mathbb{Z}$ zyklisch. Aus den Potenzrechenregeln folgt, dass eine zyklische Gruppe abelsch ist; die Begriffe „zyklische Gruppe“ und „zyklische abelsche Gruppe“ (wie früher schon definiert) fallen also zusammen. Damit ist auch klar, dass die Gruppen $\mathbb{Z}$ und $\mathbb{Z}_n$ (bis auf Isomorphie) die einzigen zyklischen Gruppen sind.

Beispiel. Die Diedergruppen D_n sind nicht zyklisch (für $n > 1$); sie sind für $n > 2$ nicht einmal abelsch, da zwei Spiegelungen an Achsen, die nicht aufeinander senkrecht stehen, nicht miteinander kommutieren. D_n ist aber von zwei Elementen erzeugt: $D_n = \langle \sigma, \tau\rangle$, wobei σ die Drehung um $2\pi/n$ und τ eine Spiegelung ist. Die n Drehungen in D_n sind dann σ^k mit $k = 0, 1, \ldots, n-1$; die n Spiegelungen sind $\sigma^k\tau$ mit $k = 0, 1, \ldots, n-1$. Es gelten die Relationen $\sigma^n = 1$, $\tau^2 = 1$ und $\tau\sigma = \sigma^{-1}\tau$.

16.5. **Definition.** Sei G eine Gruppe. Die Kardinalität $\#G$ von G heißt die *Ordnung* von G. Für ein Element $g \in G$ heißt $\#\langle g\rangle$ die *Ordnung* $\operatorname{ord}(g)$ von g. (In beiden Fällen sprechen wir einfach von „unendlicher Ordnung“, wenn die Mengen nicht endlich sind.)

16.6. **Lemma.** *Sei G eine Gruppe und $g \in G$ ein Element. Dann ist*

$$\operatorname{ord} g = \min\{n \in \mathbb{Z}_{>0} \mid g^n = 1\}\,,$$

falls die Menge nicht leer ist, anderenfalls hat g unendliche Ordnung.

Beweis. Es ist $\operatorname{ord}(g) = \#\langle g\rangle = \#\{g^n \mid n \in \mathbb{Z}\}$. Außerdem gilt

$$g^k = g^l \iff g^{k-l} = 1 \iff g^{|k-l|} = 1\,.$$

Ist $g^n \neq 1$ für alle $n \geq 1$, dann sind demnach alle Potenzen g^n für $n \in \mathbb{Z}$ paarweise verschieden; damit ist $\langle g\rangle$ unendlich. Anderenfalls sei m das minimale $n \geq 1$ mit $g^n = 1$. Dann gilt $g^n = 1 \iff m \mid n$. (Sei $n = qm + r$ mit $0 \leq r < m$, dann ist $g^n = (g^m)^q \cdot g^r = g^r$, und nach Wahl von m ist $g^r = 1$ genau dann, wenn $r = 0$ ist.) Es folgt $g^k = g^l \iff k \equiv l \bmod m$. Also hat $\langle g\rangle$ genau die m verschiedenen Elemente $g^0 = 1, g, g^2, \ldots, g^{m-1}$, d.h., $\operatorname{ord}(g) = m$. □

16.7. **Beispiele.**

(1) Die Ordnung der symmetrischen Gruppe S_n ist $n!$.
(2) Die Ordnung der Diedergruppe D_n ist $2n$. Diese Gruppe enthält (z.B.) Elemente der Ordnung n und der Ordnung 2.
(3) Ist G eine endliche Gruppe, und $g \in G$ ein Element mit $\operatorname{ord}(g) = \#G$, dann ist $G = \langle g\rangle$ zyklisch.
(4) Ist F ein endlicher Körper mit $\#F = q$, dann gilt (Übung)

$$\#\operatorname{GL}_2(F) = (q^2 - 1)(q^2 - q)\,.$$

16.8. **Definition.** Sei G eine Gruppe mit zwei Teilmengen $A, B \subset G$. Wir schreiben

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

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

Eine Untergruppe einer Gruppe G führt zu einer Aufteilung von G in Teilmengen. Wir schreiben im Folgenden häufig „$U \leq G$“ für „U ist eine Untergruppe von G“.

16.9. **Definition.** Sei G eine Gruppe und $U \leq G$. Für $g \in G$ heißt gU die *Linksnebenklasse von g bezüglich U* und Ug die *Rechtsnebenklasse von g bezüglich U*. Wir schreiben $G/U = \{gU \mid g \in G\}$ für die Menge der Linksnebenklassen bzgl. U und $U\backslash G = \{Ug \mid g \in G\}$ für die Menge der Rechtsnebenklassen bzgl. U.

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

(1) $h^{-1}g \in U$,
(2) $g \in hU$,
(3) $gU \subset hU$,
(4) $gU = hU$,
(5) $gU \cap hU \neq \emptyset$.

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

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

Beweis. Wir zeigen zuerst die Äquivalenz der ersten drei Aussagen:

$$\begin{aligned} h^{-1}g \in U &\iff \exists u \in U : h^{-1}g = u \\ &\iff \exists u \in U : g = hu \\ &\iff g \in hU \\ &\implies gU \subset (hU)U = h(UU) \subset hU\,; \end{aligned}$$

die Implikation „$gU \subset hU \implies g \in hU$“ folgt aus $g \in gU$.

Aus (4) folgt (5), und aus (5) folgt $gu_1 = hu_2$ mit geeigneten $u_1, u_2 \in U$, also $h^{-1}g = u_1^{-1}u_2 \in U$ (und damit (1)) und $g^{-1}h = u_2^{-1}u_1 \in U$. Nach dem zuerst Bewiesenen gilt dann auch $gU \subset hU$ und $hU \subset gU$, also $gU = hU$.

Die Äquivalenz von (4) und (5) besagt, dass die Nebenklassen eine Partition von G bilden; das ist gleichbedeutend damit, dass das Enthaltensein in der selben Nebenklasse eine Äquivalenzrelation definiert. □

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

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

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

Beweis. Übung. □

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

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

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

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

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

Beweis. Es gilt $\#G = \sum_{gU \in G/U} \#gU$. Da nach Lemma 16.13 alle Nebenklassen gU die selbe Kardinalität $\#gU = \#U$ haben, folgt die Behauptung. □

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

Beweis. Wir wenden Folgerung 16.14 auf $U = \langle g \rangle$ an. Es gilt dann also $\#G = m \operatorname{ord}(g)$ mit $m \in \mathbb{Z}$. Es folgt $g^{\#G} = (g^{\operatorname{ord}(g)})^m = 1^m = 1$. □

16.16. **Bemerkung.** Eine Anwendung ist der *kleine Satz von Fermat:*

Ist p eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$, dann gilt $a^{p-1} \equiv 1 \bmod p$.

Dafür wenden wir Folgerung 16.15 auf die multiplikative Gruppe $\mathbb{F}_p^\times$ an. Das lässt sich verallgemeinern: Anwendung auf die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ der Ordnung $\phi(n)$ (Eulersche ϕ-Funktion) liefert:

Ist $n \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ teilerfremd zu n, dann gilt $a^{\phi(n)} \equiv 1 \bmod n$.

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

16.17. **Satz (Cauchy).** *Sei G eine endliche Gruppe und p ein Primteiler von $\#G$. Dann gibt es in G Elemente der Ordnung p.*

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

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

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

Auf der anderen Seite können wir M aufteilen in eine Menge

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

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

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

Diese Elemente sind alle verschieden, denn die Periode der Folge

$$g_1, g_2, \ldots, g_p, g_1, g_2, \ldots, g_p, g_1, \ldots$$

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

Als nächstes betrachten wir die Struktur erhaltenden Abbildungen von Gruppen.

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

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

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

16.19. **Bemerkung.** Aus $\phi(1) = \phi(1^2) = \phi(1)^2$ folgt $\phi(1) = 1$, und aus $\phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ folgt $\phi(g^{-1}) = \phi(g)^{-1}$; ein Homomorphismus erhält also wirklich die komplette Gruppenstruktur. Man sieht auch leicht, dass für einen Isomorphismus ϕ die Umkehrabbildung ϕ^{-1} ebenfalls ein Isomorphismus ist, und dass die Komposition zweier Gruppenhomomorphismen wieder ein Gruppenhomomorphismus ist.

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

(1) *Ist $U \leq G$, dann ist $\phi(U) \leq G'$. Insbesondere ist das Bild von ϕ eine Untergruppe von G'.*
(2) *Ist $U' \leq G'$, dann ist $\phi^{-1}(U') \leq G$. Insbesondere ist der Kern von ϕ eine Untergruppe von G.*
(3) *ϕ ist genau dann injektiv, wenn* $\ker(\phi)$ *trivial ist.*

Beweis.

(1) $1 = \phi(1) \in \phi(U)$; mit $u_1' = \phi(u_1)$ und $u_2' = \phi(u_2)$ sind auch $u_1'u_2' = \phi(u_1u_2)$ und $(u_1')^{-1} = \phi(u_1^{-1})$ in $\phi(U)$.
(2) $\phi(1) = 1$, also ist $1 \in \phi^{-1}(U')$. Seien $u_1, u_2 \in \phi^{-1}(U')$, also $\phi(u_1), \phi(u_2) \in U'$, dann gilt auch $\phi(u_1u_2) = \phi(u_1)\phi(u_2) \in U'$ und $\phi(u_1^{-1}) = \phi(u_1)^{-1} \in U'$ und damit $u_1u_2, u_1^{-1} \in \phi^{-1}(U')$.
(3) „$\Rightarrow$“ ist trivial. Für die Gegenrichtung sei $\ker(\phi) = \{1\}$. Dann gilt für $g_1, g_2 \in G$:

$$\begin{aligned}\phi(g_1) = \phi(g_2) &\implies \phi(g_1g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = 1\\ &\implies g_1g_2^{-1} \in \ker(\phi) = \{1\}\\ &\implies g_1g_2^{-1} = 1 \implies g_1 = g_2\,.\end{aligned}$$

□

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

16.21. **Beispiele.**

(1) Für beliebige Gruppen G und G' gibt es immer den *trivialen Homomorphismus* $G \to G'$, $g \mapsto 1$.
(2) Die Determinante ist multiplikativ. Das bedeutet, dass für jeden Körper K und jede Zahl $n \in \mathbb{Z}_{\geq 0}$ die Abbildung $\det : \mathrm{GL}_n(K) \to K^\times$ ein Gruppenhomomorphismus ist. Der Kern wird $\mathrm{SL}_n(K)$ geschrieben und heißt *spezielle lineare Gruppe*. Für $n \geq 1$ ist det ein Epimorphismus.

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

(4) Für eine Permutation $\sigma \in S_n$ sei $P(\sigma) \in \mathrm{GL}_n(\mathbb{R})$ die zugehörige Permutationsmatrix (d.h., der Eintrag in Zeile $\sigma(i)$ und Spalte i ist 1, für $i = 1, \dots, n$; alle anderen Einträge sind 0), so dass gilt $P(\sigma)e_i = e_{\sigma(i)}$, wobei $e_1, \dots, e_n$ die Standardbasis von $\mathbb{R}^n$ ist. Dann ist $P : S_n \to \mathrm{GL}_n(\mathbb{R})$ ein Gruppenhomomorphismus. Das Bild von P liegt in der orthogonalen Gruppe $\mathrm{O}(n)$, denn $P(\sigma)^\top = P(\sigma^{-1})$, also gilt $P(\sigma)P(\sigma)^\top = I_n$.

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

(6) Das Legendre-Symbol definiert einen Homomorphismus $\mathbb{F}_p^\times \to \{\pm 1\}$.

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

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

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

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

von G ist. Zum Beispiel hat eine abelsche Gruppe keine inneren Automorphismen außer der Identität.

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

(9) $\exp : (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$ ist ein Monomorphismus mit Bild $\mathbb{R}_+^\times = \{x \in \mathbb{R} \mid x > 0\}$.

(10) $\exp : (\mathbb{C}, +) \to (\mathbb{C}^\times, \cdot)$ ist ein Epimorphismus mit Kern $2\pi i\mathbb{Z}$.

17. Normalteiler und Faktorgruppen

Wie in anderen Situationen auch, würden wir gerne auf der Menge G/U eine Gruppenstruktur definieren, so dass die kanonische Abbildung $G \to G/U$ ein Homomorphismus wird. Dazu müssten wir definieren $gU \cdot g'U = (gg')U$. Hier ergibt sich aber ein Problem: Diese Verknüpfung ist nicht immer wohldefiniert. Wenn wir $g = 1$ nehmen, dann ist jedes $u \in U$ ein anderer Repräsentant von $gU = U$, also sollte $ug' \in g'U$ sein für alle $u \in U$. Das bedeutet $Ug' = g'U$, also dass Links- und Rechtsnebenklassen übereinstimmen. Dies ist jedoch nicht immer der Fall (man finde ein Beispiel für $G = S_3$). Daher führt man einen neuen Begriff ein.

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

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

17.2. **Beispiele.**

(1) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.
(2) Ist G eine Gruppe und $U \leq G$ mit $(G : U) = 2$, dann ist U ein Normalteiler. (Denn für gU bzw. Ug gibt es nur die beiden Möglichkeiten U und $G \setminus U$; aus $gU \cap Ug \neq \emptyset$ folgt also $gU = Ug$.) Zum Beispiel ist A_n ein Normalteiler von S_n.
(3) Sei $g \in G$ mit $\mathrm{ord}(g) = 2$. Dann ist $\langle g \rangle = \{1, g\}$ genau dann ein Normalteiler von G, wenn $g \in Z(G)$ ist. Zum Beispiel sind die Untergruppen der Ordnung 2 von S_3 keine Normalteiler.
(4) In jeder Gruppe sind die trivialen Untergruppe $\{1\}$ und G Normalteiler.

17.3. **Lemma.** *Sei $\phi : G \to G'$ ein Gruppenhomomorphismus.*

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

Beweis.

(1) Wir wissen bereits, dass $\phi^{-1}(N')$ eine Untergruppe von G ist. Außerdem gilt für $g \in G$:
$$g\phi^{-1}(N')g^{-1} \subset \phi^{-1}(\phi(g)N'\phi(g)^{-1}) \subset \phi^{-1}(N') .$$
(2) Wir wissen bereits, dass $\phi(N)$ eine Untergruppe von G' ist. Da ϕ surjektiv ist, lässt sich jedes $g' \in G$ schreiben als $\phi(g)$ mit $g \in G$. Damit gilt dann
$$g'\phi(N)(g')^{-1} = \phi(g)\phi(N)\phi(g^{-1}) = \phi(gNg^{-1}) = \phi(N) .$$

□

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

17.4. **Satz und Definition.** *Sei G eine Gruppe und N ein Normalteiler von G. Dann definiert $gN \cdot hN = (gN)(hN) = (gh)N$ eine Gruppenstruktur auf G/N, so dass die kanonische Abbildung $\phi : G \to G/N$, $g \mapsto gN$, ein Homomorphismus ist.*

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

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

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

Wir haben den üblichen Homomorphiesatz.

17.5. **Homomorphiesatz für Gruppen.** *Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus*

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

Insbesondere gilt $(G : \ker(\phi)) = \#\operatorname{im}(\phi)$. Für jeden Normalteiler $N \lhd G$ mit $N \subset \ker(\phi)$ erhalten wie einen induzierten Homomorphismus $G/N \to G'$ mit Bild $\operatorname{im}(\phi)$.

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

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

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

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

also besteht der Kern von $\tilde{\phi}$ nur aus dem Element K. □

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

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

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

$$\#SL_2(\mathbb{F}_p) = \frac{\#GL_2(\mathbb{F}_p)}{\#\mathbb{F}_p^\times} = \frac{(p^2-1)(p^2-p)}{p-1} = (p^2-1)p = (p-1)p(p+1)\,,$$

denn $\mathrm{SL}_2(\mathbb{F}_p) = \ker(\det : \mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times)$, und det ist in diesem Fall surjektiv.

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

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

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

In gewisser Weise spielen einfache Gruppen für die Gruppentheorie eine ähnliche Rolle wie Primzahlen für die multiplikative Theorie der ganzen Zahlen. Wenn G etwa eine nichttriviale endliche Gruppe ist, dann ist G entweder einfach, oder G hat einen nichttrivialen Normalteiler N. In diesem Fall kann man G aus N und G/N „zusammensetzen“ (allerdings gibt es bei gegebenen Gruppen N und G/N im allgemeinen mehrere Möglichkeiten, wie man daraus eine Gruppe zusammenbauen

kann, insofern ist die Situation deutlich komplizierter als bei den ganzen Zahlen); N und G/N lassen sich weiter zerlegen, bis man bei einfachen Gruppen ankommt. Man kann zeigen, dass die einfachen Gruppen, die man bekommt, bis auf Isomorphie eindeutig bestimmt sind, unabhängig davon, wie man diesen Prozess durchführt — das ist das Analogon zum Satz über die eindeutige Primfaktorzerlegung.

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

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

Beweis. Sei A eine einfache endliche abelsche Gruppe. Dann ist A nicht trivial, also hat $\#A$ einen Primteiler p. Nach dem Satz von Cauchy 16.17 hat A ein Element a der Ordnung p und damit eine Untergruppe $\langle a\rangle$ der Ordnung p. In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler; da A einfach ist, muss $\langle a\rangle = A$ sein, und es gilt $\#A = p$.

Ist umgekehrt p eine Primzahl und A eine abelsche Gruppe mit $\#A = p$, dann gilt für jeden Normalteiler (= Untergruppe) N von A, dass $\#N$ ein Teiler von p ist (Satz von Lagrange 16.14), also ist $\#N = 1$ und damit $N = \{1\}$ oder $\#N = p$ und damit $N = A$. □

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

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

Eine weitere Familie von einfachen Gruppen sind die alternierenden Gruppen:

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

Auch die A_3 ist einfach, da sie abelsch ist und Ordnung 3 hat. Dagegen hat die A_4 einen nichttrivialen Normalteiler der Ordnung 4 (Übung).

Beweis. Der Beweis ist an sich nicht schwer, aber leider haben wir dafür keine Zeit. Siehe zum Beispiel [KM, § 9.3.2].

Ganz kurze Skizze: Man zeigt zuerst, dass alle Dreierzyklen in A_n zueinander konjugiert sind (d.h., sind $\sigma_1, \sigma_2 \in A_n$ Dreierzyklen, dann gibt es $\tau \in A_n$ mit $\tau\sigma_1\tau^{-1} = \sigma_2$). Dann zeigt man, dass ein Normalteiler $N \neq \{1\}$ von A_n einen Dreierzykel enthalten muss. Es folgt, dass N *alle* Dreierzyklen enthält. Da man auch leicht zeigen kann, dass die Dreierzyklen die A_n erzeugen, folgt $N = A_n$. □

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

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

Zu jeder Primzahlpotenz $q = p^e$ gibt es einen (bis auf Isomorphie eindeutigen) Körper $\mathbb{F}_q$ mit q Elementen. Wir können dann die Gruppe $\mathrm{SL}_n(\mathbb{F}_q)$ betrachten. Ihr Zentrum besteht aus den skalaren Matrizen λI_n mit $\lambda^n = 1$ und ist ein Normalteiler. Der Quotient $\mathrm{PSL}_n(\mathbb{F}_q) := \mathrm{SL}_n(\mathbb{F}_q)/Z(\mathrm{SL}_n(\mathbb{F}_q))$ ist einfach, außer für sehr kleine Werte von n und q. Zum Beispiel ist die $\mathrm{PSL}_2(\mathbb{F}_7)$ der Ordnung 168 die zweitkleinste nicht-abelsche einfache Gruppe.

18. Operationen von Gruppen auf Mengen

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

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

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

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

Analog kann man Operationen *von rechts* als Abbildungen $X \times G \to X$ definieren.

Eine Operation m von G auf X ist das selbe wie ein Gruppenhomomorphismus $\mu : G \to S(X)$ von G in die symmetrische Gruppe von X, in dem Sinne, dass $m \longmapsto \big(g \mapsto (x \mapsto m(g, x))\big)$ und $\mu \longmapsto \big((g, x) \mapsto (\mu(g))(x)\big)$ zueinander inverse Abbildungen sind (Übung). Ist X eine Menge mit Struktur (zum Beispiel ein Vektorraum, ein Ring, eine Gruppe, ein topologischer Raum ...) und ist das Bild von μ enthalten in der entsprechenden Automorphismengruppe, dann sagt man, G operiere auf dem Vektorraum, Ring, der Gruppe, dem topologischen Raum X, oder G operiere auf X durch lineare Abbildungen, Ringautomorphismen, Gruppenautomorphismen, Homöomorphismen.

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

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

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

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

Die Untergruppe (!)

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

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

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

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

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

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

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

18.4. **Beispiel.** Sei G eine Gruppe und $U \leq G$ eine Untergruppe. Dann operiert G auf G/U via $g \cdot g'U = (gg')U$. Wir erhalten also einen Gruppenhomomorphismus $G \to S(G/U)$. Ist U eine Untergruppe von endlichem Index n, dann kann man $S(G/U)$ mit der symmetrischen Gruppe S_n identifizieren.

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

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

Man kann diese Art der Operation auch ausnutzen, um das Folgende zu zeigen. Dies ist eine Verallgemeinerung der Aussage, dass eine Untergruppe vom Index 2 immer ein Normalteiler ist.

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

Beweis. Die Operation von G auf G/U liefert einen Homomorphismus $G \to S_p$. Sein Kern ist ein echter Normalteiler von G (denn G permutiert ja die Nebenklassen wirklich), dessen Index ein Teiler von $\#S_p = p!$ sein muss (nach dem Homomorphiesatz 17.5). Da p der *kleinste* Primteiler von $\#G$ ist, gilt $\mathrm{ggT}(\#G, p!) = p$, also ist der Index p. Der Kern ist außerdem in U enthalten, da U der Stabilisator von $U \in G/U$ ist (der Kern ist der Durchschnitt aller Stabilisatoren). Es bleibt nur die Möglichkeit, dass der Kern gleich U ist, also ist U (als Kern eines Homomorphismus) ein Normalteiler. □

18.6. **Beispiel.** Sei G eine Gruppe, dann operiert G auf sich selbst durch Gruppenautomorphismen via $g \mapsto c_g$, also $g \cdot x = gxg^{-1}$. (Operation „durch Konjugation“.) Die Bahnen dieser Operation heißen die *Konjugationsklassen* von G. Der Kern des Homomorphismus $G \to \mathrm{Aut}(G)$, $g \mapsto c_g$, ist gerade das Zentrum $Z(G)$, wie wir schon früher gesehen haben. Der Stabilisator von $x \in G$ unter dieser Operation heißt der *Zentralisator* $C_G(x)$ von x in G.

Auf analoge Weise operiert G auf der Menge aller Untergruppen von G (von fester Ordnung oder festem Index) via $g \cdot U = gUg^{-1}$. Die Bahnen heißen wieder *Konjugationsklassen* (von Untergruppen). Eine Untergruppe U ist genau dann ein Fixpunkt dieser Operation, wenn U ein Normalteiler ist. Der Stabilisator von U

unter dieser Operation heißt der *Normalisator* $N_G(U)$ von U in G. U ist ein Normalteiler in $N_G(U)$, und $N_G(U)$ ist die größte Untergruppe von G mit dieser Eigenschaft (Übung).

Dieses Beispiel wird uns noch beschäftigen.

Zuerst aber beweisen wir eine einfache, aber grundlegende Tatsache.

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

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

(wohldefiniert und) eine Bijektion. Insbesondere gelten die Relationen

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

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

Die Abbildung ist offensichtlich surjektiv. Seien jetzt $gG_x, g'G_x \in G/G_x$ mit $g \cdot x = g' \cdot x$. Dann folgt $x = 1 \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x$, also ist $g^{-1}g' \in G_x$ und damit $gG_x = g'G_x$; die Abbildung ist also auch injektiv.

Die angegebenen Relationen erhält man durch Vergleich der Kardinalitäten und mit dem Satz von Lagrange. □

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

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

Beweis. Für $h \in G$ gilt

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

18.9. **Folgerung (Bahnengleichung).** *Die endliche Gruppe G operiere auf der endlichen Menge X. Dann gilt*

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

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

Man kann das so interpretieren, dass in der Summe x über ein *Repräsentantensystem* der Bahnen in $X \setminus X^G$ läuft. Nach Lemma 18.8 hängt der Index $(G : G_x)$ nicht vom gewählten Repräsentanten der Bahn $G \cdot x$ ab.

Beweis. Wir schreiben $\#X$ als Summe aller Kardinalitäten $\#(G \cdot x)$ der Bahnen. Die Bahnen der Länge 1 ergeben gerade die Fixpunkte X^G; für die übrigen verwenden wir die Relation $\#(G \cdot x) = (G : G_x)$ aus Lemma 18.7. □

Diese harmlos erscheinende Relation hat interessante Anwendungen.

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

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

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

Beweis. Ist $U \leq G$ eine Untergruppe mit $U \neq G$, dann muss der Index $(G : U)$ ein Vielfaches von p sein. Aus der Relation in Folgerung 18.9 ergibt sich also die Kongruenz $\#X \equiv \#X^G \bmod p$. Daraus folgen sofort die beiden Behauptungen. □

18.12. **Beispiel.** Wir betrachten noch einmal den Beweis des Satzes 16.17 von Cauchy. Dort war p eine Primzahl und G eine endliche Gruppe mit $p \mid \#G$. Die zyklische Gruppe $\mathbb{Z}_p$ operiert auf G^p durch „Rotation“: Der Erzeuger bewirkt die Permutation

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

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

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

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

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

Beweis. Wir betrachten die Operation von G durch Konjugation auf sich selbst. Dann ist $\#X = \#G$ durch p teilbar, und 1 ist ein Fixpunkt, also hat die Menge der Fixpunkte mindestens p Elemente. Die Fixpunktmenge ist aber gerade das Zentrum $Z(G)$. Da $Z(G) \triangleleft G$, gilt $Z(G) = G$, wenn G einfach ist. Dann ist G aber abelsch, muss also Ordnung p haben, siehe Prop. 17.7. □

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

Beweis. Sei G eine Gruppe mit $\#G = p^2$. Nach Folgerung 18.14 ist $Z(G)$ nicht trivial, also gilt $\#Z(G) = p$ oder $\#Z(G) = p^2$. Im zweiten Fall ist $Z(G) = G$, also G abelsch. Im ersten Fall sei $a \in G \setminus Z(G)$. Dann ist die von a und $Z(G)$ erzeugte Untergruppe von G abelsch (denn a kommutiert mit den Elementen von $Z(G)$) und echt größer als $Z(G)$, muss also ganz G sein. Damit ist G wieder als abelsch nachgewiesen (was in diesem Fall ein Widerspruch ist, da wir $Z(G) \neq G$ angenommen hatten). □

19. Die Sätze von Sylow

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

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

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

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

(1) *M ist disjunkte Vereinigung von Rechtsnebenklassen bzgl. G_M.*
(2) *$\#G_M \mid p^e$.*
(3) *M ist eine Rechtsnebenklasse bzgl. einer Untergruppe von G genau dann, wenn G_M Ordnung p^e hat. In diesem Fall sind alle Mengen gM in der Bahn von M Rechtsnebenklassen einer Untergruppe.*
(4) *Jede Bahn, deren Elemente Rechtsnebenklassen sind, enthält genau eine Untergruppe von G.*

Beweis.

(1) Der Stabilisator G_M operiert auf M durch Translation von links; M zerfällt also in Bahnen bezüglich dieser Operation, und das sind gerade die Rechtsnebenklassen von G_M.
(2) Da die Rechtsnebenklassen von G_M alle die selbe Mächtigkeit $\#G_M$ haben, folgt aus Teil (1), dass $\#G_M$ ein Teiler von $\#M = p^e$ sein muss.
(3) Gilt $\#G_M = p^e$, dann ist M eine Rechtsnebenklasse bzgl. G_M nach Teil (1), denn die Anzahl der Rechtsnebenklassen bzgl G_M ist gegeben durch $\frac{p^e}{\#G_M}$. Gilt umgekehrt $M = Ug$ mit einer Untergruppe $U \leq G$, dann ist $U \subset G_M$, und es folgt mit Teil (2) $p^e = \#M = \#U \mid \#G_M \mid p^e$, also $\#G_M = p^e$.
Hat der Stabilisator G_M von M Ordnung p^e, dann gilt das auch für den Stabilisator $G_{gM} = gG_Mg^{-1}$ jeder anderen Menge gM in der Bahn von M.
(4) Die Bahn enthalte die Rechtsnebenklasse Ug bzgl. der Untergruppe U; Dann enthält die Bahn die Untergruppe $U' = g^{-1}Ug \leq G$. Die Bahn besteht dann genau aus den Linksnebenklassen von U'; U' selbst ist die einzige Linksnebenklasse, die eine Untergruppe ist. □

Wir schreiben $\#G = kp^e$. Wir wenden die Bahnengleichung 18.9 auf die Operation von G auf $\mathcal{T}$ an:

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

wobei $(M_j)_{j \in J}$ ein Repräsentantensystem der Bahnen ist. Die Indizes $(G : G_{M_j})$ sind alle von der Form kp^f (mit $f \leq e$), und es folgt (unter Verwendung von

Lemma 19.1)

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

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

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

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

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

Wir haben also folgenden Satz bewiesen, der den Satz von Cauchy verallgemeinert.

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

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

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

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

Beweis. Diesmal lassen wir G (und damit U) auf der Menge $G/S = \{gS \mid g \in G\}$ der Linksnebenklassen von S durch Linkstranslation operieren: $h \cdot gS = (hg)S$. Weil S eine p-Sylowgruppe von G ist, ist $\#(G/S) = \#G/\#S$ nicht durch p teilbar. Es muss also mindestens eine Bahn unter der Operation von U geben, deren Länge nicht durch p teilbar ist. Sei gS ein Element einer solchen Bahn. Der Stabilisator von gS in G ist gSg^{-1}, der Stabilisator in U also $U' = U \cap gSg^{-1}$. Die Länge der Bahn stimmt mit dem Index $(U : U')$ überein. Da die Länge der Bahn nicht durch p teilbar ist, der Index aber eine Potenz von p sein muss, folgt $(U : U') = 1$ und damit $U' = U$, also $U \subset gSg^{-1}$.

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

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

19.5. **Satz (Sylow).** *Sei G eine endliche Gruppe, p ein Primteiler von $\#G$. Sei $\#G = kp^e$ mit $p \nmid k$. Dann gilt für die Anzahl s_p der p-Sylowgruppen von G:*

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

Beweis. Die erste Aussage $s_p \equiv 1 \bmod p$ ist ein Spezialfall des Satzes von Frobenius 19.2. Für die zweite Aussage betrachten wir die Operation von G durch Konjugation auf der Menge der p-Sylowgruppen von G: $g \cdot S = gSg^{-1}$. Nach Satz 19.4 ist die Operation transitiv. Die Anzahl s_p ist also gleich der Länge der (einzigen) Bahn und muss demnach ein Teiler von $\#G$ sein. Da nach der ersten Aussage p kein Teiler von s_p ist, folgt $s_p \mid k$. □

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

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

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

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

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

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

Wir erinnern uns an die Definition des *direkten Produkts* von Gruppen (Definition 9.11): Sind $G_1, G_2, \ldots, G_n$ Gruppen, dann wird das cartesische Produkt $G_1 \times G_2 \times \cdots \times G_n$ eine Gruppe, wenn man die Verknüpfung komponentenweise definiert. Sind die Gruppen abelsch, dann ist das direkte Produkt isomorph zur direkten Summe (vgl. Definition 14.27).

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

Beweis. Nach Satz 19.4 sind S_p und S_q Normalteiler von G. Da die Ordnungen von S_p und S_q teilerfremd sind, muss $S_p \cap S_q = \{1\}$ gelten. Nach Lemma 19.6 gilt also $ss' = s's$ für alle $s \in S_p$ und $s' \in S_q$. Daraus folgt, dass ϕ ein Gruppenhomomorphismus ist, denn für $s_1, s_2 \in S_p$, $s_1', s_2' \in S_q$ gilt

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

Der Kern von ϕ ist trivial, denn aus $ss' = 1$ folgt $s = s'^{-1} \in S_p \cap S_q = \{1\}$, also $(s, s') = (1, 1)$. Es folgt, dass ϕ injektiv ist. Da beide Seiten die selbe Mächtigkeit haben, muss ϕ auch surjektiv sein. □

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

Es folgt das versprochene Anwendungsbeispiel für die Sätze von Sylow.

19.8. **Proposition.** *Seien $p < q$ Primzahlen, so dass $p \nmid q - 1$. Dann ist jede Gruppe G mit $\#G = pq$ zyklisch.*

Beweis. Seien s_p und s_q die Anzahlen der p- und q-Sylowgruppen von G. Nach Satz 19.5 gilt dann $s_p \mid q$ und $s_p \equiv 1 \bmod p$. Da $q \not\equiv 1 \bmod p$, ist $s_p = 1$ die einzige Möglichkeit. Ebenso gilt $s_q \mid p$ und $s_q \equiv 1 \bmod q$; wegen $q > p$ muss $s_q = 1$ sein. Nach Proposition 19.7 ist G isomorph zum Produkt seiner p- und seiner q-Sylowgruppe. Diese Gruppen sind zyklisch (da von Primzahlordnung), also insbesondere abelsch, ihr Produkt stimmt also mit ihrer direkten Summe überein; nach dem Chinesischen Restsatz ist die direkte Summe isomorph zur zyklischen Gruppe $\mathbb{Z}_{pq}$. □

Man kann die Gruppen der Ordnung pq ganz allgemein klassifizieren. Dazu braucht man aber die Konstruktion des *semidirekten Produkts*. Wir werden uns das evtl. in der „Vertiefung der Algebra“ noch genauer ansehen. Hier betrachten wir einen einfachen Spezialfall.

19.9. **Proposition.** *Sei p eine ungerade Primzahl und G eine Gruppe der Ordnung $2p$. Dann ist G entweder zyklisch oder isomorph zur Diedergruppe D_p.*

Beweis. G hat eine p-Sylowgruppe N, die ein Normalteiler ist (denn sie hat Index 2 in G; alternativ kann man auch Satz 19.5 verwenden: $s_p \mid 2$ und $s_p \equiv 1 \bmod p$ implizieren $s_p = 1$). Die Anzahl der 2-Sylowgruppen ist nach Satz 19.5 entweder 1 oder p. Im ersten Fall ist G zyklisch, das sieht man wie im Beweis von Proposition 19.8. Im anderen Fall sei $n \in N$ ein Erzeuger von N (N ist zyklisch der Ordnung p) und $g \in G$ ein Element der Ordnung 2. Dann muss $gn \neq ng$ gelten, denn sonst wäre die 2-Sylowgruppe $\langle g \rangle$ von G ein Normalteiler. Es ist also $gng = gng^{-1} = n^k$ mit $k \not\equiv 1 \bmod p$. Andererseits gilt

$$n = (g^2)n(g^2)^{-1} = g(gng^{-1})g^{-1} = gn^k g^{-1} = (gng^{-1})^k = (n^k)^k = n^{k^2}$$

und damit $k^2 \equiv 1 \bmod p$. Da $\mathbb{F}_p$ ein Körper ist, muss $k \equiv \pm 1 \bmod p$ sein. Der Fall $k \equiv 1$ ist ausgeschlossen, also folgt

$$gng = gng^{-1} = n^{-1}\,.$$

Wir erhalten einen Isomorphismus $G \to D_p$, indem wir g auf eine der Spiegelungen und n auf die Drehung um $2\pi/p$ abbilden. □

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

- Für $\#G = 1$ gibt es nur die triviale Gruppe.
- Für $\#G = p$ prim (also $\#G \in \{2, 3, 5, 7, 11, 13\}$) gibt es nur die zyklische Gruppe $\mathbb{Z}_p$.
- Für $\#G = p^2$ mit $p \in \{2, 3\}$ muss G abelsch sein (siehe Folgerung 18.15), also ist entweder $G \cong \mathbb{Z}_{p^2}$ zyklisch, oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Die für $p = 2$ auftretende Gruppe $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$ heißt die *Kleinsche Vierergruppe*.

- Für $\#G = 2p$ mit $p \in \{3, 5, 7\}$ gilt nach Proposition 19.9, dass entweder $G \cong \mathbb{Z}_{2p}$ zyklisch ist, oder $G \cong D_p$ ist isomorph zur Diedergruppe D_p. Im Fall $p = 3$ gilt $D_3 \cong S_3$; somit ist die symmetrische Gruppe S_3 die kleinste nicht-abelsche Gruppe.
- Für $\#G = 15$ gilt nach Proposition 19.8, dass G zyklisch ist.

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

$$G \cong \mathbb{Z}_8\,, \qquad G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \quad \text{und} \quad G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

(vergleiche den Klassifikationssatz 14.30).

Ist G nicht abelsch, dann wissen wir, dass das Zentrum $Z(G)$ nicht trivial ist (Folgerung 18.14) und dass $Z(G) \neq G$ gilt. Wäre $\#Z(G) = 4$, dann würde wie im Beweis von Proposition 19.9 folgen, dass G doch abelsch wäre; dieser Fall kann also nicht eintreten. Es folgt $Z(G) = \{1, z\}$ mit einem $1 \neq z \in G$.

G muss Elemente der Ordnung 4 enthalten (denn eine Gruppe, deren nichttriviale Elemente alle Ordnung 2 haben, ist abelsch — Übung). Sei $g \in G$ ein solches Element. Dann muss gelten $Z(G) \subset \langle g \rangle$, also $g^2 = z$, denn sonst wäre nach Lemma 19.6 G abelsch. Jetzt gibt es zwei Möglichkeiten. Die erste ist, dass ein Element von $G \setminus \langle g \rangle$ Ordnung 2 hat. Sei h ein solches Element. Da $\langle g \rangle$ ein Normalteiler ist, gilt $hgh = hgh^{-1} = g^{\pm 1}$. Es kann nicht $hgh^{-1} = g$ sein, da dann G abelsch wäre. Also ist $hgh^{-1} = g^{-1}$, und G ist isomorph zur Diedergruppe D_4. In diesem Fall haben dann *alle* Elemente von $G \setminus \langle g \rangle$ die Ordnung 2.

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

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

ist.

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

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

Man kann die Sätze von Sylow auch benutzen, um zum Beispiel die Gruppen der Ordnung 12 zu klassifizieren (siehe etwa [Fi, S. 127]). Neben den beiden Typen $\mathbb{Z}_{12}$ und $\mathbb{Z}_2 \times \mathbb{Z}_6$ von abelschen Gruppen gibt es drei Typen von nicht-abelschen Gruppen, nämlich die Diedergruppe D_6, die alternierende Gruppe A_4 und eine weitere Gruppe $G = \langle a, b \rangle$ mit $\mathrm{ord}(a) = 3$, $\mathrm{ord}(b) = 4$, $bab^{-1} = a^{-1}$.

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

20. Körpererweiterungen

Im letzten Abschnitt dieser Vorlesung werden wir Körpererweiterungen studieren.

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

Ist L ein weiterer Teilkörper von K mit $k \subset L \subset K$, dann heißt L ein *Zwischenkörper* (engl. *intermediate field*) der Körpererweiterung $k \subset K$.

Zum Beispiel sind $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}(i) \subset \mathbb{C}$ Körpererweiterungen. $\mathbb{Q}(i)$ und $\mathbb{R}$ sind Zwischenkörper von $\mathbb{Q} \subset \mathbb{C}$.

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

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

20.3. **Definition.** Sei $k \subset K$ eine Körpererweiterung und $A \subset K$ eine Teilmenge. Wir schreiben

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

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

Sind $k_1, k_2 \subset K$ zwei Teilkörper, dann schreibt man auch $k_1 k_2$ für den Teilkörper $k_1(k_2) = k_2(k_1)$ und nennt ihn das *Kompositum* von k_1 und k_2.

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

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

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

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

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

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

Beweis. Wir müssen den Fall ausschließen, dass $n = \operatorname{char}(R) > 0$ eine zusammengesetzte Zahl ist. Sei in diesem Fall $n = n_1 n_2$ eine nichttriviale Faktorisierung. Dann gilt $\phi_R(n_1), \phi_R(n_2) \neq 0$, aber $\phi_R(n_1)\phi_R(n_2) = \phi_R(n_1 n_2) = \phi_R(n) = 0$, also hat R Nullteiler; ein Widerspruch. □

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

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

Beweis. Sei P der Primkörper von K. Da jeder Teilkörper von K die 1 von K enthält, muss $\operatorname{im}(\phi_K) \subset P$ gelten. Im Fall $\operatorname{char}(K) = 0$ ist ϕ_K injektiv, also ist $\operatorname{im}(\phi_K) \cong \mathbb{Z}$. Nach der Definition des Quotientenkörpers (Satz 10.1) gibt es eine Fortsetzung von ϕ_K zu einem Homomorphismus $\tilde{\phi}_K : \mathbb{Q} \to P \subset K$. Als Homomorphismus zwischen Körpern ist $\tilde{\phi}_K$ injektiv, und sein Bild ist ein in P enthaltener Teilkörper von K; es folgt $P = \operatorname{im}(\tilde{\phi}_K) \cong \mathbb{Q}$.

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

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

Sei $k \subset K$ eine Körpererweiterung. Indem wir die Multiplikation von K auf $k \times K$ einschränken, erhalten wir eine skalare Multiplikation von k auf K. Aus den Körperaxiomen folgt dann sofort, dass K ein *k-Vektorraum* ist. Zum Beispiel ist $\mathbb{C}$ ein zweidimensionaler $\mathbb{R}$-Vektorraum, oder $\mathbb{R}$ ist ein unendlichdimensionaler $\mathbb{Q}$-Vektorraum (denn jeder endlichdimensionale $\mathbb{Q}$-Vektorraum ist abzählbar). Das ermöglicht die folgende Definition.

20.8. **Definition.** Sei $k \subset K$ eine Körpererweiterung. Dann heißt die Dimension von K als k-Vektorraum,

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

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

20.9. **Beispiele.** Es ist $[\mathbb{C} : \mathbb{R}] = 2$ und $[\mathbb{R} : \mathbb{Q}] = \infty$. Ist F ein endlicher Körper, dann ist $\operatorname{char}(F) = p$ eine Primzahl (nach Lemma 20.7), und $\#F = p^n$ mit einem $n \geq 1$, denn F ist ein n-dimensionaler Vektorraum über $\mathbb{F}_p$. Wir werden später untersuchen, ob es zu jeder Primzahlpotenz p^n auch einen Körper mit p^n Elementen gibt.

20.10. **Lemma.** *Sei $k \subset L \subset K$ ein Zwischenkörper. Dann gilt*

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

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

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

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

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

Beweis. Die erste Aussage folgt unmittelbar aus Lemma 20.10. Die zweite ergibt sich aus $L = k \iff [L : k] = 1 \iff [K : L] = [K : k]$. □

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

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

Die Umkehrung in Teil (2) gilt nicht.

Beweis. Sei $[L_2 : k] = n < \infty$ und $b_1 = 1, b_2, \ldots, b_n$ eine k-Basis von L_2. Sei $M = \langle b_1, \ldots, b_n \rangle_{L_1} \subset K$. Es ist klar, dass M in $L_1 L_2$ enthalten ist und sowohl L_1 als auch L_2 enthält. Wir zeigen, dass M ein Körper ist, dann folgt $M = L_1 L_2$. Zunächst ist klar, dass M unter Addition und Subtraktion abgeschlossen ist und 0 und 1 enthält. Da alle Produkte $b_i b_j \in L_2$ wieder als (k-)Linearkombinationen der b_i geschrieben werden können, ist M auch unter der Multiplikation abgeschlossen, also jedenfalls ein Unterring von K. Sei $0 \neq a \in M$. Dann ist die Abbildung $m_a : M \to M$, $x \mapsto ax$, L_1-linear und injektiv. Da M ein endlichdimensionaler L_1-Vektorraum ist, muss m_a auch surjektiv sein, also gibt es $x \in M$ mit $ax = 1$; damit ist $a^{-1} \in M$.

Der Rest des Beweises ist eine Übungsaufgabe. □

21. Algebraische Elemente und Erweiterungen

Wir kommen nun zu einer wichtigen Begriffsbildung in der Körpertheorie.

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

(1) Ein Element $a \in K$ heißt *algebraisch über* k, wenn es ein normiertes Polynom $f \in k[X]$ gibt mit $f(a) = 0$. Ist a nicht algebraisch über k, dann heißt a *transzendent über* k. Im Fall $k = \mathbb{Q}$ und $K = \mathbb{R}$ oder $\mathbb{C}$ spricht man von *algebraischen* bzw. *transzendenten Zahlen*.
(2) Die Körpererweiterung $k \subset K$ heißt *algebraisch* und K heißt *algebraisch über* k, wenn alle Elemente von K über k algebraisch sind. Anderenfalls heißt die Körpererweiterung *transzendent*.
(3) k heißt *algebraisch abgeschlossen in* K, wenn jedes Element von K, das über k algebraisch ist, bereits in k liegt. In diesem Fall heißt die Körpererweiterung $k \subset K$ auch *rein transzendent*.
(4) Ein Körper k heißt *algebraisch abgeschlossen*, wenn jedes nicht konstante Polynom $f \in k[X]$ eine Nullstelle in k hat.

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

21.2. **Beispiele.**

(1) Die Zahlen $\sqrt{2}$, i, $\sqrt[3]{2}$ sind algebraisch als Nullstellen von $X^2 - 2$, $X^2 + 1$, $X^3 - 2$. Ebenso sind alle Zahlen der Form $\zeta = e^{2\pi i q}$ mit $q \in \mathbb{Q}$ algebraisch, denn ist $q = a/b$ mit $a, b \in \mathbb{Z}$, dann ist ζ Nullstelle von $X^b - 1$.
(2) Die Zahlen e und π sind transzendent (Hermite 1873, Lindemann 1882). Demgegenüber ist unbekannt, ob $e + \pi$ und $e \cdot \pi$ beide transzendent sind. (Sie können jedenfalls nicht beide algebraisch sein — warum?)
(3) $\mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn jede (echt) komplexe Zahl $z = a + bi$ ist Nullstelle des reellen Polynoms $X^2 - 2aX + a^2 + b^2$. Insbesondere ist $\mathbb{R}$ nicht algebraisch abgeschlossen.
(4) Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen. Da $\mathbb{R}$ und $\mathbb{C}$ unter anderem durch topologische Eigenschaften definiert sind, kann es dafür keinen rein algebraischen Beweis geben. Der einfachste Beweis kann mit Hilfsmitteln der Funktionentheorie geführt werden (Satz von Liouville).

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

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

vergleiche Satz 11.2 (universelle Eigenschaft des Polynomrings). Es ist dies der Einsetzungshomomorphismus $f \mapsto f(a)$, und es gilt $k[a] = \mathrm{im}(\phi_a)$, siehe Lemma 15.13. Wir haben dann folgende Charakterisierung.

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

(1) *a ist algebraisch über k.*
(2) *ϕ_a ist nicht injektiv.*
(3) *$k[a] = k(a)$.*
(4) *$k \subset k(a)$ ist eine endliche Körpererweiterung.*

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

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

„(2)⇒(3)“: Ist ϕ_a nicht injektiv, dann ist der Kern $\ker(\phi_a)$ ein von null verschiedenes Ideal von $k[X]$. Da $k[X]$ ein Hauptidealring ist (vgl. 11.10), ist $\ker(\phi_a) = \langle f\rangle_{k[X]}$ mit einem Polynom $f \neq 0$, das bis auf Multiplikation mit einem Element aus $k^\times$ eindeutig bestimmt ist. Fordern wir zusätzlich, dass f normiert ist, dann ist f eindeutig bestimmt. Nach dem Homomorphiesatz für Ringe 7.14 ist $k[a] = \mathrm{im}(\phi_a) \cong k[X]/\langle f\rangle_{k[X]}$. Da $k[a] \subset K$ ein Integritätsbereich ist, ist f ein Primelement und damit irreduzibel. Damit ist das von f erzeugte Ideal maximal, also ist $k[a]$ sogar ein Körper und damit gleich $k(a)$ (vgl. 7.21).

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

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

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

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

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

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

$$h = X^n + h_{n-1}X^{n-1} + \ldots + h_2X^2 + h_1X + h_0 \in k[X]\,,$$

also ist a algebraisch über k. □

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

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

Das in Satz 21.3 auftretende Polynom f hat einen Namen:

21.4. **Definition.** Sei $k \subset K$ eine Körpererweiterung und $a \in K$ algebraisch über k. Dann heißt das Polynom f in Satz 21.3 das *Minimalpolynom* von a über k, und der Grad $[k(a) : k] = \deg(f)$ heißt der *Grad* von a über k.

Es gilt dann für Polynome $h \in k[X]$, dass $h(a) = 0$ ist genau dann, wenn h ein Vielfaches von f ist.

Satz 21.3 hat einige wichtige Konsequenzen.

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

Beweis. Da a Nullstelle eines normierten Polynoms mit Koeffizienten in k ist, ist a algebraisch über k. Sei $m \in k[X]$ das Minimalpolynom von a über k. Aus $f(a) = 0$ folgt $m \mid f$, und da f irreduzibel und normiert ist, muss $f = m$ gelten. Die Aussage über den Grad von a über k war Teil von Satz 21.3. □

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

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

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

Beweis. Sind a und b algebraisch über k, dann gilt $[k(a) : k], [k(b) : k] < \infty$ nach Satz 21.3. Aus Lemma 20.12 ergibt sich, dass dann $k(a, b)$ ebenfalls eine endliche Erweiterung von k ist. Da $a \pm b$, ab und a/b Elemente von $k(a, b)$ sind, müssen die von ihnen erzeugten Körpererweiterungen von k ebenfalls endlich sein. Wiederum nach Satz 21.3 müssen diese Elemente algebraisch über k sein. □

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

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

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

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

Beweis. Ist $a \in K$, dann ist $k(a) \subset K$ endlich über k, also ist a nach Satz 21.3 algebraisch über k. □

21.9. **Beispiel.** Die Umkehrung von Folgerung 21.8 gilt nicht: Sei $\mathbb{A}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Dann ist $\mathbb{A}$ eine algebraische Erweiterung von $\mathbb{Q}$ von unendlichem Grad. Das kann man zum Beispiel so sehen: Für jedes $n \geq 1$ ist das Polynom $X^n - 2 \in \mathbb{Q}[X]$ irreduzibel (Eisenstein-Kriterium 12.10). Es gilt $\mathbb{Q}(\sqrt[n]{2}) \subset \mathbb{A} \cap \mathbb{R} \subset \mathbb{A}$, also auch $n = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \leq [\mathbb{A} \cap \mathbb{R} : \mathbb{Q}] \leq [\mathbb{A} : \mathbb{Q}]$. Der Körper $\mathbb{A}$ besteht aus allen algebraischen komplexen Zahlen. Dass er selbst algebraisch abgeschlossen ist, folgt aus dem folgenden Ergebnis.

21.10. **Satz (Transitivität der Algebraizität).** *Seien $k \subset L \subset K$ Körpererweiterungen. Dann ist K algebraisch über k genau dann, wenn sowohl L algebraisch über k als auch K algebraisch über L ist.*

Beweis. Wir nehmen zunächst an, dass $k \subset K$ algebraisch ist. Dann ist jedes Element $a \in K$ algebraisch über k, also ist nach Satz 21.3 $[k(a) : k] < \infty$. Es folgt $[L(a) : L] \leq [k(a) : k] < \infty$, also ist $L \subset K$ algebraisch. Wählt man $a \in L$, folgt auch, dass $k \subset L$ algebraisch ist.

Seien jetzt $k \subset L$ und $L \subset K$ algebraisch, und sei $a \in K$. Da a nach Annahme algebraisch ist über L, gibt es ein normiertes irreduzibles Polynom $h \in L[X]$ mit $h(a) = 0$ und $[L(a) : L] = \deg(h) =: n$. Seien $h_0, h_1, \ldots, h_{n-1} \in L$ die Koeffizienten von h (ohne $h_n = 1$). Da $k \subset L$ algebraisch ist, gilt mit Satz 21.3 und wiederholter Anwendung von Lemma 20.12, dass $L' = k(h_0, h_1, \ldots, h_{n-1})$ über k endlich ist. Wegen $h \in L'[X]$ gilt immer noch $[L'(a) : L'] = n < \infty$. Es folgt

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

also ist a algebraisch über k. □

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

Beweis. Wir müssen zeigen, dass jedes nicht konstante Polynom $f \in \bar{k}[X]$ eine Nullstelle in $\bar{k}$ hat. Da K algebraisch abgeschlossen ist, hat f jedenfalls eine Nullstelle $a \in K$. Als Nullstelle eines Polynoms in $\bar{k}[X]$ ist a algebraisch über $\bar{k}$. Nach Satz 21.10 ist a dann auch algebraisch über k, also liegt a in $\bar{k}$. □

21.12. **Bemerkung.** Ist k ein Körper und $k \subset K$ eine algebraische Körpererweiterung, so dass K algebraisch abgeschlossen ist, dann heißt K ein *algebraischer Abschluss* von k. Man kann zeigen, dass es für jeden Körper einen algebraischen Abschluss gibt, und dass dieser bis auf Isomorphismus „über k“ eindeutig bestimmt ist, siehe zum Beispiel [Fi, § III.2.5] oder [KM, § 23].

Wir sehen jedenfalls, dass der in Beispiel 21.9 eingeführte Körper $\mathbb{A}$ der algebraischen Zahlen ein algebraischer Abschluss von $\mathbb{Q}$ ist.

22. Zerfällungskörper

Bisher haben wir stets „bereits vorhandene“ Körpererweiterungen $k \subset K$ betrachtet und (zum Beispiel) Elemente von K studiert. Man kann sich jedoch auch fragen, ob es zu gegebenem Körper k eine Körpererweiterung mit bestimmten gewünschten Eigenschaften gibt (etwa eine, die Nullstellen gewisser Polynome enthält) und wie man eine solche gegebenenfalls konstruiert. Der Beweis von Satz 21.3 weist dazu den Weg.

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

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

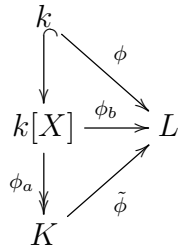
Beweis. Wir definieren $K = k[X]/\langle f \rangle_{k[X]}$ wie angegeben. Weil f irreduzibel ist, ist $\langle f \rangle_{k[X]}$ ein maximales Ideal im Hauptidealring $k[X]$; deshalb ist K ein Körper. Die Aussage $[K : k] = \deg(f)$ folgt wie im Beweis von Satz 21.3. Wir schreiben den kanonischen Epimorphismus $k[X] \to K$ als $h \mapsto [h]$. Sei $a = [X]$ das Bild von X in K, dann gilt $f(a) = f([X]) = [f] = [0]$, also hat f in K eine Nullstelle. □

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

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

22.2. **Satz.** *Sei k ein Körper, und sei $f \in k[X]$ normiert und irreduzibel. Sei $k \subset K$ eine Körpererweiterung und $a \in K$ mit $f(a) = 0$ und $K = k(a)$ (zum Beispiel wie in Satz 22.1 mit $a = [X]$). Weiterhin sei L ein weiterer Körper, $\phi : k \to L$ ein Homomorphismus und $b \in L$ eine Nullstelle von $\tilde{f}$, wobei $\tilde{f} \in L[X]$ durch Anwendung von ϕ auf die Koeffizienten von f entsteht. Dann gibt es einen eindeutig bestimmten Homomorphismus $\tilde{\phi} : K \to L$ mit $\tilde{\phi}|_k = \phi$ und $\tilde{\phi}(a) = b$.*

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



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

Als Beispiel sei erwähnt, dass man mit diesem Ergebnis leicht sehen kann, dass $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}(\omega\sqrt[3]{2})$ mit $\omega = e^{2\pi i/3}$ isomorph sind (obwohl der erste Körper in $\mathbb{R}$ enthalten ist und der zweite nicht). Dazu wenden wir Satz 22.2 an mit $k = \mathbb{Q}$, $f = X^3 - 2$, $K = \mathbb{Q}(\sqrt[3]{2})$, $a = \sqrt[3]{2}$, $L = \mathbb{Q}(\omega\sqrt[3]{2})$, $b = \omega\sqrt[3]{2}$ und $\phi : \mathbb{Q} \hookrightarrow \mathbb{Q}(\omega\sqrt[3]{2})$. Da ϕ auf $\mathbb{Q}$ die Identität ist, ist hier $\tilde{f} = f$. Wir erhalten einen Homomorphismus $\tilde{\phi} : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\omega\sqrt[3]{2})$. Da $\tilde{\phi}$ eine injektive $\mathbb{Q}$-lineare Abbildung zwischen $\mathbb{Q}$-Vektorräumen gleicher endlicher Dimension (hier 3) ist, muss $\tilde{\phi}$ auch bijektiv und damit ein Isomorphismus sein.

22.3. **Zusatz.** *In der Situation von Satz 22.2 gibt es genau* $\#\{b \in L \mid \tilde{f}(b) = 0\}$ *Homomorphismen* $\tilde{\phi} : K \to L$ *mit* $\tilde{\phi}|_k = \phi$.

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

Durch Iteration der Konstruktion von Satz 22.1 können wir erreichen, dass ein gegebenes Polynom in Linearfaktoren zerfällt.

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

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

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

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

Beweis. Der Existenzbeweis geht durch Induktion über den Grad n von f (jeweils gleichzeitig für alle Körper k). Im Fall $n = 0$ ist nichts zu zeigen, denn $K = k$ ist der einzige Zerfällungskörper. Sei also $n > 0$. Wir schreiben $f = gh$ mit einem normierten irreduziblen Polynom $g \in k[X]$. Nach Satz 22.1 gibt es eine Körpererweiterung $k \subset k' = k(a)$, so dass wir in $k'[X]$ die Zerlegung $g = (X - a)g_1$ haben. Das Polynom $f_1 = g_1 h \in k'[X]$ hat Grad $n - 1$. Nach Induktionsannahme gibt es einen Zerfällungskörper K von f_1 über k'. Dann ist K auch ein Zerfällungskörper von f über k, denn die Nullstellen von f, nämlich a und die Nullstellen von f_1, liegen alle in K, und K wird über $k' = k(a)$ von den Nullstellen von f_1 erzeugt, also wird K über k von den Nullstellen von f erzeugt. Ebenso haben wir $[K : k'] \leq (n-1)!$, also $[K : k] = [K : k'] \cdot [k' : k] \leq (n-1)! \cdot n = n!$.

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

Der Homomorphismus ψ wird schrittweise konstruiert. Sei ψ schon auf dem Zwischenkörper L von $k \subset K$ definiert (zu Beginn ist $L = k$); wir haben also $\psi_L : L \to K'$ mit $\psi_L|_k = \mathrm{id}_k$. Wir faktorisieren f in $L[X]$ in normierte irreduzible Faktoren. Sind diese alle linear, dann muss $L = K$ sein, und wir sind fertig. Anderenfalls sei h ein irreduzibler Faktor vom Grad ≥ 2. Sei $\tilde{h} \in K'[X]$ das Polynom, das durch Anwendung von ϕ_L auf die Koeffizienten von h entsteht. Sei a eine Nullstelle von h in K und b eine Nullstelle von $\tilde{h}$ in K', und sei $L' = L(a)$. Dann gibt es nach Satz 22.2 eine (eindeutig bestimmte) Fortsetzung $\psi_{L'} : L' \to K'$ von ψ_L mit $\psi_{L'}(a) = b$. Da $L' \neq L$, gilt $[L' : k] > [L : k]$. Weil $[K : k]$ endlich ist, müssen wir nach endlich vielen Schritten $L = K$ erreichen. □

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

22.6. **Bemerkung.** Aus dem Zusatz 22.3 folgt im Fall, dass f keine mehrfachen Nullstellen (in K') hat, dass es genau $[K : k] = [K' : k]$ Isomorphismen $\psi : K \to K'$ mit $\psi|_k = \mathrm{id}_k$ gibt. (Im Beweis oben gibt es beim Schritt von L zu L' genau $[L' : L]$ Möglichkeiten, den Homomorphismus fortzusetzen; die Behauptung folgt durch Induktion.) Man kann das auf $K' = K$ anwenden und erhält die Aussage, dass die Körpererweiterung $k \subset K$ genau $[K : k]$ Automorphismen hat (das sind Körperautomorphismen von K, die auf k die Identität induzieren). Das ist die maximal mögliche Anzahl. Körpererweiterungen mit der Eigenschaft, dass sie diese Maximalzahl an Automorphismen haben, heißen *Galois-Erweiterungen*; wir werden sie in der „Vertiefung der Algebra“ genauer studieren.

23. Endliche Körper

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

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

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

(1) *Für jede Primzahl p ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen.*
(2) $\mathrm{char}(F) = p$ *ist eine Primzahl, und F enthält (eine Kopie von) $\mathbb{F}_p$.*
(3) $\#F = p^e$ *mit $e \geq 1$.*
(4) *In F gilt $(x + y)^p = x^p + y^p$ (und $(xy)^p = x^p y^p$).*
(5) *Die multiplikative Gruppe $F^\times$ von F ist zyklisch.*

Die vorletzte Aussage legt folgende Definition nahe:

23.2. **Definition.** Sei F ein Körper der Charakteristik $p > 0$. Dann ist $\phi_F : F \to F$, $x \mapsto x^p$, ein Endomorphismus von F; ϕ_F heißt der *Frobenius-Endomorphismus* von F. Ist F endlich, dann ist ϕ_F ein Automorphismus von F und heißt dem entsprechend der *Frobenius-Automorphismus* von F.

(Dass ϕ_F ein Ringhomomorphismus ist, folgt aus $(x + y)^p = x^p + y^p$ („Freshman's Dream“). Als Homomorphismus zwischen Körpern ist ϕ_F injektiv. Ist F endlich, muss $\phi_F : F \to F$ dann sogar bijektiv sein.)

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

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

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

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

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

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

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

Wir haben uns jetzt zwar schon einmal einen Überblick über die Teilkörper eines endlichen Körpers verschafft, aber wir wissen immer noch nicht, ob es auch zu jeder Primzahlpotenz p^e einen endlichen Körper mit p^e Elementen gibt. (Aus dem eben bewiesenen Lemma folgt nur, dass mit dem Exponenten e auch jeder Teiler von e vorkommen muss.) Um diese Frage zu beantworten, verwenden wir die Existenz von Zerfällungskörpern und lassen uns von der Beschreibung der Teilkörper in Lemma 23.3 inspirieren.

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

Beweis. Die zweite Aussage sagt uns, wie wir einen geeigneten Körper F' finden können: Sei F' ein Zerfällungskörper von $f = X^{q^n} - X$ über F, der nach Satz 22.5 existiert. Dann ist F' von endlichem Grad über F, also ebenfalls endlich. Die Menge der Fixpunkte von ϕ_F^{en} bildet nach dem Beweis von Lemma 23.3 einen Teilkörper F'' von F'. Diese Fixpunkte sind gerade die Nullstellen von f in F' (beachte: $q^n = p^{en}$). Da F' Zerfällungskörper von f ist, zerfällt f in $F'[X]$ in Linearfaktoren. Da $f' = p^{en} X^{p^{en}-1} - 1 = -1$ niemals verschwindet, hat f in F' $q^n = p^{en}$ verschiedene Nullstellen. Es folgt $\#F' = q^n$. Da alle Nullstellen von f schon in F' liegen, muss $F'' = F'$ sein (denn F' ist von diesen Nullstellen erzeugt). □

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

Beweis. Wir wenden Satz 23.4 auf $F = \mathbb{F}_p$ an. □

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

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

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

Aus Satz 23.4 und Lemma 23.6 können wir nun Schlüsse über die Existenz von irreduziblen Polynomen vorgegebenen Grades über einem endlichen Körper ziehen.

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

Beweis. Sei $q = \#F = p^e$. Nach Satz 23.4 gibt es eine Körpererweiterung F' von F vom Grad n, nach Lemma 23.3 hat F' einen Teilkörper mit q Elementen, und wieder nach Satz 23.4 ist dieser Teilkörper zu F isomorph. Wir können also F' als Erweiterung von F vom Grad n betrachten. Nach Lemma 23.6 ist F' eine einfache Erweiterung von F. Sei $\alpha \in F'$ ein primitives Element (also $F' = F(\alpha)$), und sei $f \in F[X]$ das Minimalpolynom von α. Dann gilt $\deg(f) = [F(\alpha) : F] = [F' : F] = n$, und f ist irreduzibel und normiert. □

Man kann diese Aussage noch verfeinern, indem man die Anzahl der normierten irreduziblen Polynome vom Grad n betrachtet. Dazu beweisen wir erst noch zwei vorbereitende Aussagen.

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

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

Insbesondere ist F' ein Zerfällungskörper von f über F.

Beweis. Nach Satz 22.1 gibt es eine Körpererweiterung F'' von F vom Grad n, in der f eine Nullstelle hat. Nach Satz 23.4 sind also F' und F'' isomorph als Körpererweiterungen von F. Es folgt, dass f in F' eine Nullstelle α hat. Sei jetzt $\beta \in F'$ irgend eine Nullstelle von f. Dann gilt

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

denn $\phi^e_{F'}$ ist nach Lemma 23.3 auf F, also auf den Koeffizienten von f, die Identität. Also ist auch β^q eine Nullstelle von f. Induktiv erhalten wir also, dass alle α^{q^k} für $k = 0, 1, 2, \ldots$ Nullstellen von f sind.

Da die Abbildung $\phi^e_{F'} : x \mapsto x^q$ bijektiv und F' endlich ist, muss die Folge $(\alpha, \alpha^q, \alpha^{q^2}, \ldots)$ von Beginn an periodisch sein. Da $\phi^{en}_{F'}$ nach Lemma 23.3 die Identität auf F' ist, ist die Periodenlänge ein Teiler von n. Wäre sie ein echter Teiler m von n, dann wäre α in der Fixpunktmenge von $\phi^{em}_{F'}$ enthalten, also in einer Körpererweiterung vom Grad m von F. Das wäre aber ein Widerspruch dazu, dass das Minimalpolynom von α Grad n hat, vergleiche Folgerung 21.5. Also ist die Periodenlänge n, und damit sind die ersten n Glieder der Folge paarweise verschieden. Da diese n Elemente allesamt Nullstellen von f sind, müssen es alle Nullstellen von f sein, und die behauptete Faktorisierung folgt. □

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

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

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

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

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

Sei $\alpha \in F'$. Dann ist $[F(\alpha) : F]$ ein Teiler von n, also ist der Grad des Minimalpolynoms f von α ein Teiler von n. Damit ist f ein Faktor im Produkt auf der rechten Seite. Dieses Argument zeigt, dass jede Nullstelle von h auch Nullstelle des Produkts ist, also teilt h das Produkt. Sei jetzt umgekehrt $f \in F[X]$ ein normiertes irreduzibles Polynom mit $m = \deg(f) \mid n$. Es gibt einen Zwischenkörper $F \subset K \subset F'$ mit $[K : F] = m$. Nach Lemma 23.8 ist K ein Zerfällungskörper von f über F, also zerfällt f auch über F' in Linearfaktoren. Das zeigt, dass f ein Teiler von h ist. Da verschiedene normierte irreduzible Polynome teilerfremd sind, folgt, dass das Produkt auf der rechten Seite ein Teiler von h ist. Da beide Seiten normiert sind und sich gegenseitig teilen, müssen sie gleich sein. □

Aus dieser Faktorisierung können wir nun leicht folgende Rekursion herleiten.

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

$$\sum_{k \mid n} k a_k(q) = q^n\,.$$

Beweis. Die linke Seite ergibt den Grad des Produkts auf der rechten Seite der Formel in Lemma 23.9, die rechte Seite ist der Grad des Polynoms $X^{q^n} - X$ auf der linken Seite. □

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

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

Für $q = 2$ haben wir also $a_1(2) = 2$, $a_2(2) = 1$, $a_3(2) = 2$, $a_4(2) = 3$, vergleiche die Tabelle von irreduziblen Polynomen über $\mathbb{F}_2$ in 12.8.

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

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

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

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

23.13. **Lemma.** *Sei R ein Ring, und seien $(a_n)_{n\geq 1}$ und $(b_n)_{n\geq 1}$ zwei Folgen von Elementen von R. Dann gilt*

$$\forall n \geq 1 : \sum_{k|n} a_k = b_n \iff \forall n \geq 1 : \sum_{k|n} \mu\big(\frac{n}{k}\big) b_k = a_n \,.$$

Beweis. Wir zeigen zunächst

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

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

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

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

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

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

23.14. **Folgerung.** *Es gilt*

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

Beweis. Anwendung von Lemma 23.13 auf $a_n := n a_n(q)$ und $b_n := q^n$. □

Zum Beispiel gilt

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

Es gibt also $a_6(2) = 9$ verschiedene irreduzible Polynome vom Grad 6 über $\mathbb{F}_2$.

24. Konstruktionen mit Zirkel und Lineal

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

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

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

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

Wir überlegen jetzt, wie sich die Konstruktion von Punkten algebraisch niederschlägt. Eine erste Beobachtung ist, dass sich ein Punkt (x,y) genau dann ausgehend von S konstruieren lässt, wenn das für die Punkte $(x,0)$ und $(y,0)$ gilt. Wir können also ohne Einschränkung annehmen, dass $S = S' \times \{0\}$ ist mit einer Teilmenge $S' \subset \mathbb{R}$ (bestehend aus den x- und y-Koordinaten der Punkte aus S). Wir nennen dann eine reelle Zahl α *konstruierbar aus* S', wenn sich $(\alpha,0)$ ausgehend von $S = S' \times \{0\}$ konstruieren lässt. Im Folgenden schreiben wir der Einfachheit halber S für die Menge S'. Wir sagen, α sei *konstruierbar*, wenn α aus $\{0,1\}$ konstruierbar ist.

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

Formaler ausgedrückt: Es gibt einen Körperturm

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

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

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

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

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

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

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

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

Es hat die Form

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

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

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

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

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

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

Den resultierenden Fall (eine lineare und eine quadratische Gleichung) haben wir aber bereits behandelt.

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

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

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

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

Damit können wir bereits die Unlösbarkeit mehrerer klassischer Probleme zeigen.

24.2. **Folgerung (Würfelverdopplung).** *Die Zahl $\sqrt[3]{2}$ ist nicht konstruierbar.*

Beweis. $X^3-2 \in \mathbb{Q}[X]$ ist irreduzibel nach Eisenstein, also ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und damit keine Zweierpotenz. Nach Proposition 24.1 ist $\sqrt[3]{2}$ also nicht konstruierbar. □

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

Wir sagen, ein Winkel φ ist *konstruierbar*, wenn sein Cosinus (oder sein Sinus, beides ist äquivalent) konstruierbar ist. Durch Errichten des Lots auf die x-Achse im Punkt $(\cos\varphi, 0)$ und Schneiden mit dem Einheitskreis kann man leicht eine Gerade durch den Ursprung konstruieren, die mit der x-Achse den Winkel φ einschließt.

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

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

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

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

Das Polynom $f = X^3-3X+1$ ist irreduzibel, denn es hat keine rationale Nullstelle (nur ±1 kämen in Frage). Es folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$. Nach Proposition 24.1 ist also α (und damit natürlich auch $\alpha/2 = \cos\frac{2\pi}{9}$) nicht konstruierbar. □

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

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

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

Beweis. Wegen $\cos\frac{2\pi}{3} = -\frac{1}{2}$ müsste $\cos\frac{2\pi}{9}$ (aus $\{0,1\}$) konstruierbar sein, was aber nach Folgerung 24.3 nicht der Fall ist. □

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

Beweis. Die p-te Einheitswurzel $\zeta = e^{2\pi i/p}$ ist Nullstelle von $f = X^{p-1} + X^{p-2} + \ldots + X + 1$, und f ist irreduzibel (Eisenstein für $f(X+1)$, siehe 12.11). Es gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos\frac{2\pi}{p})] = 2$ (Beispiel nach Folgerung 21.6). Wenn das reguläre p-Eck konstruierbar ist, dann muss $[\mathbb{Q}(\cos\frac{2\pi}{p}) : \mathbb{Q}]$ eine Zweierpotenz sein, und damit ist auch

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

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

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

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

Zum Beispiel kann man keine regulären 7-, 11- oder 13-Ecke konstruieren. Umgekehrt kann man zeigen, dass reguläre p-Ecke für Fermatsche Primzahlen p tatsächlich konstruierbar sind (Gauß 1796). Für $p = 3$ und $p = 5$ ist das seit der Antike bekannt. Gauß fand 1796 eine Konstruktion für das reguläre 17-Eck (mit neunzehn Jahren!) — daran erinnert ein siebzehnzackiger Stern an seinem Denkmal in Braunschweig. Richelot gab 1832 eine Konstruktion des regulären 257-Ecks an. „Im Jahr 1894 fand Johann Gustav Hermes nach mehr als zehnjähriger Anstrengung eine Konstruktionsvorschrift für das regelmäßige 65537-Eck und beschrieb diese in einem Manuskript von mehr als 200 Seiten, welches sich heute in einem speziell dafür angefertigten Koffer in der Mathematischen Bibliothek der Universität Göttingen befindet.“ (Wikipedia zum 65537-Eck)

Weitere Fermatsche Primzahlen sind nicht bekannt. (Fermat hatte einmal behauptet, alle Zahlen $2^{2^m}+1$ seien prim. Schon Euler zeigte, dass $2^{32}+1$ durch 641 teilbar ist.)

Die Unmöglichkeit eines anderen klassischen Problems zeigt die nächste Folgerung.

24.6. **Folgerung (Quadratur des Kreises).** *Die Zahl $\sqrt{\pi}$ ist nicht konstruierbar.*

Beweis. Wäre $\sqrt{\pi}$ konstruierbar, dann wäre $\sqrt{\pi}$ und damit auch π nach Proposition 24.1 algebraisch. π ist aber transzendent. □

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

Wenn man zeigen will, dass gewisse Konstruktionen *möglich* sind, dann braucht man eine Umkehrung von Proposition 24.1. Tatsächlich ist es so, dass die vier Grundrechenarten und das Ziehen von Quadratwurzel durch Konstruktionen mit Zirkel und Lineal ausgeführt werden können. Für Addition und Subtraktion ist das klar. Für Multiplikation und Division verwendet man den Strahlensatz. Für Quadratwurzeln konstruiert man einen Kreis mit Durchmesser $1 + x$ und trägt 1 auf dem Durchmesser ab. Das Lot in diesem Punkt trifft den Kreis im Abstand $\sqrt{x}$, wie man mit dem Satz des Pythagoras, angewandt auf die drei entstehenden rechtwinkligen Dreiecke, leicht nachrechnet. Daraus ergibt sich:

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

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

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

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

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

für $16 \cos \frac{2\pi}{17}$.

Im nächsten Semester werden wir eine Charakterisierung konstruierbarer Zahlen mit Hilfe der *Galoistheorie* kennen lernen. Daraus ergibt sich dann zum Beispiel die Aussage, dass das reguläre n-Eck genau dann konstruierbar ist, wenn $\phi(n)$ (Eulersche ϕ-Funktion) eine Zweierpotenz ist. Das bedeutet, dass $n = 2^k p_1 \cdots p_m$ ist, wo $p_1, \ldots, p_m$ verschiedene Fermatsche Primzahlen sind.

Literatur

[Fi] Gerd Fischer: *Lehrbuch der Algebra,* Vieweg, 2008. Signatur 80/SK 200 F529 L5. Online-Zugriff unter http://dx.doi.org/10.1007/978-3-8348-9455-7

[KM] Christian Karpfinger und Kurt Meyberg: *Algebra. Gruppen - Ringe - Körper,* Spektrum Akademischer Verlag, 2010. Online-Zugriff unter http://dx.doi.org/10.1007/978-3-8274-2601-7.