Ralf Gerkmann

Mathematisches Institut
Ludwig-Maximilians-Universität München

Vorlesungsskript

Algebra und Zahlentheorie

Zusammenfassung

Algebraische Strukturen wie Gruppen, Ringe und Körper bilden die unverzichtbare Grundlage für jedes Teilgebiet der Mathematik, angefangen beim Lösen elementarer zahlentheoretischer Probleme oder algebraischer Gleichungen, über die Klassifikation diskreter geometrischer Strukturen und topologischer Räume bis hin zu fortgeschrittenen Bereichen wie der Algebraischen Geometrie oder der Harmonischen Analysis. Auch in vielen Anwendungsgebieten, in der Informatik beispielsweise in der Kryptographie und in der Theorie der Programmiersprachen, innerhalb der Physik etwa in der Klassischen Mechanik, der Quantenmechanik und der Elementarteilchenphysik, spielen sie eine wichtige Rolle.

Jeder der drei oben genannten algebraischen Strukturen ist ein eigener Vorlesungsteil gewidmet, wobei wir allerdings den theoretischen Konzepten, die in allen drei Gebieten auftreten (zum Beispiel Faktorstrukturen und Homomorphiesätze), besondere Beachtung schenken. Beim Aufbau der Gruppentheorie orientieren uns unter anderem am sog. *Klassifikationsproblem*, bei dem wir vor allem durch die zuletzt behandelten Sylowsätze noch entscheidende Fortschritte erzielen. Bei der Ringtheorie stehen als Motivation vor allem Probleme der klassischen Zahlentheorie im Vordergrund. Im letzten Teil der Vorlesung befassen wir uns mit der Theorie der algebraischen Körpererweiterungen. Den krönenden Abschluss der Algebra wird die (im Sommersemester behandelte) Galoistheorie bilden, bei der die Gruppen- und die Körpertheorie miteinander verbunden werden. Im Einzelnen werden in der zweisemestrigen Vorlesung folgende Themen behandelt.

- Definition der algebraischen Grundstrukturen: Gruppen, Ringe und Körper
- Homomorphismen, Unter- und Faktorstrukturen, Konstruktion von Erweiterungen
- zyklische und abelsche Gruppen
- semidirekte Produkte und Auflösbarkeit
- Gruppenoperationen und Sylowsätze
- Kongruenzrechnung
- Teilbarkeit und eindeutige Primfaktorzerlegung
- endliche und algebraische Körpererweiterungen
- Fortsetzung von Körperhomomorphismen
- normale Körperweiterungen
- Theorie der endlichen Körper
- Galoistheorie und Anwendungen

Inhaltsverzeichnis

§ 1. *Definition der Gruppen, Beispiele*

Zusammenfassung. Das Ziel dieses Kapitels besteht darin, mit dem Gruppenbegriff, den wir schon aus der Linearen Algebra kennen, besser vertraut zu werden. Zunächst betrachten wir eine große Anzahl konkreter Beispiele von Gruppen: Gruppen als Bestandteile algebraischer Strukturen, Permutationsgruppen, lineare Gruppen und Symmetriegruppen. Anschließend sehen wir uns an, wie der Begriff der Gruppe auf einfacheren Konzepte, denen der Halbgruppe und des Monoids, aufgebaut ist. Mit Hilfe von direkten Produkten können gegebene Gruppen zu komplexeren Gruppen zusammengesetzt werden. Zum Schluss erläutern wir noch ein großes fernes Ziel der Gruppentheorie, die *Klassifikation* der Gruppen.

Wichtige Grundbegriffe

- Halbgruppen, Monoide und Gruppen
- Permutationsgruppe, symmetrische Gruppe
- Bewegung, Symmetriegruppe
- Abgeschlossenheit einer Teilmenge unter einer Verknüpfung
- direktes Produkt zweier Gruppen

Im gesamten ersten Teil der Vorlesung dreht sich alles um die folgende Definition, die bereits aus der Linearen Algebra bekannt ist.

Definition 1.1 Eine ***Gruppe*** ist ein Paar $(G, *)$ bestehend aus einer nichtleeren Menge G und einer Verknüpfung $*$ auf G (also einer Abbildung $G \times G \to G$), so dass die folgenden Bedingungen erfüllt sind.

(i) Die Verknüpfung ist assoziativ, d.h. es gilt $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.

(ii) Es gibt ein ausgezeichnetes Element $e \in G$, genannt das ***Neutralelement*** der Gruppe, mit der Eigenschaft, dass $e * a = a * e = a$ für alle $a \in G$ gilt.

(iii) Für jedes Element $a \in G$ gibt es ein Element $a^{-1} \in G$, genannt das zu a ***inverse Element***, mit $a * a^{-1} = a^{-1} * a = e$.

Gilt darüber hinaus $a * b = b * a$ für alle $a, b \in G$, dann spricht man von einer ***abelschen*** oder auch einer ***kommutativen*** Gruppe.

Bevor wir uns mit dieser Definition genauer auseinandersetzen, sollten wir uns zunächst klarmachen, dass uns viele konkrete Beispiele von Gruppen bereits bekannt sind.

(1) Gruppen kommen als Bestandteile anderer, uns bereits bekannter algebraischer Strukturen, vor. Ist etwa $(R, +, \cdot)$ ein Ring, ist $(R, +)$ eine abelsche Gruppe, mit dem Neutralelement 0_R. Zum Beispiel ist $(\mathbb{Z}, +)$ eine abelsche Gruppe.

(2) Wichtige Beispiele für abelsche Gruppen erhält man durch die bereits bekannten Restklassenringe $\mathbb{Z}/n\mathbb{Z}$. Für jedes $n \in \mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe bestehend aus n Elementen. Hier ist $\bar{0} = 0+n\mathbb{Z}$, die Restklasse der Null, das Neutralelement.

(3) Ist $(K, + \cdot)$ ein Körper, dann ist $(K^\times, \cdot)$ eine Gruppe. Dabei bezeichnet $K^\times$ die Menge $K \setminus \{0_K\}$, also die Gesamtheit aller Körperelemente ungleich dem Nullelement 0_K. Beispielsweise ist $(\mathbb{C}^\times, \cdot)$ eine abelsche Gruppe, und für jede Primzahl p ist $(\mathbb{F}_p^\times, \cdot)$ ist eine abelsche Gruppe mit $p-1$ Elementen. (Wir erinnern daran, dass für jede Primzahl p der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, den wir dann auch mit $\mathbb{F}_p$ bezeichnet hatten.)

(4) Ist K ein Körper und $(V, +, \cdot)$ ein K-Vektorraum, dann ist $(V, +)$ eine abelsche Gruppe. Beispielsweise ist $(\mathbb{R}^2, +)$ eine abelsche Gruppe, wobei $+$ die Vektoraddition durch $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ bezeichnet.

Mit den symmetrischen Gruppen sind uns aus der Linearen Algebra auch schon Beispiele für nicht-abelsche Gruppen bekannt. Im Hinblick auf spätere Anwendungen führen wir hier einen etwas allgemeineren Begriff ein. Für jede Menge X sei $\mathrm{Abb}(X)$ die Menge der Abbildungen $X \to X$.

Definition 1.2 Sei X eine Menge. Dann ist das Paar $(\mathrm{Per}(X), \circ)$ bestehend aus der Teilmenge $\mathrm{Per}(X) \subseteq \mathrm{Abb}(X)$ der *bijektiven* Abbildungen $X \to X$ und der Komposition $\circ$ von Abbildungen eine Gruppe, die man als ***Permutationsgruppe*** der Menge X bezeichnet. Die Elemente von $\mathrm{Per}(X)$ nennt man auch ***Permutationen*** von X.

Ist $n \in \mathbb{N}$ und $M_n = \{1, ..., n\}$, dann ist $S_n = \mathrm{Per}(M_n)$ die bereits aus der Lineare Algebra bekannte ***symmetrische Gruppe***. Wir haben in der Linearen Algebra die Gruppeneigenschaft nur für S_n nachgewiesen, aber der Beweis ist für eine beliebige Permutationsgruppe $\mathrm{Per}(X)$ derselbe: Zunächst erinnern wir daran, dass die Komposition $\sigma \circ \tau$ zweier bijektiver Abbildungen $\sigma, \tau : X \to X$ wiederum eine bijektive Abbildung ergibt, so dass es sich bei $\circ$ tatsächlich um eine Verknüpfung auf $\mathrm{Per}(X)$ handelt. Auch wissen wir bereits, dass sich die Komposition von Abbildungen assoziativ verhält, also $(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)$ für alle $\rho, \sigma, \tau \in \mathrm{Per}(X)$ gilt. Der Grund dafür war, dass die Anwendung der beiden Abbildungen links und rechts auf ein beliebiges Element $x \in X$ jeweils übereinstimmend das Element $\rho(\sigma(\tau(x)))$ ergibt.

Für jedes $\sigma \in \mathrm{Per}(X)$ gilt jeweils $\sigma \circ \mathrm{id}_X = \sigma$ und $\mathrm{id}_X \circ \sigma = \sigma$. Auch dies überprüft man durch, dass man $\sigma \circ \mathrm{id}_X$ und $\mathrm{id}_X \circ \sigma$ auf ein beliebiges $x \in X$ anwendet; das Ergebnis ist in beiden Fällen $\sigma(x)$. Also ist id_X das Neutralelement der Gruppe $(\mathrm{Per}(X), \circ)$. Schließlich gilt noch $\sigma \circ \sigma^{-1} = \mathrm{id}_X$ und $\sigma^{-1} \circ \sigma = \mathrm{id}_X$ für jedes $\sigma \in \mathrm{Per}(X)$, wobei σ^{-1} jeweils die Umkehrabbildung bezeichnet. Dies folgt direkt aus der Definition der Umkehrabbildung. Die Gleichungen zeigen, dass σ^{-1} jeweils das zu σ inverse Element ist.

Wir geben einige Eigenschaften der symmetrischen Gruppe S_n an, die zum Teil in der Lineare Algebra hergeleitet wurden, und die wir von nun an als bekannt voraussetzen.

(i) Die Gruppe S_n besteht aus $n!$ Elementen.

(ii) Die Elemente der Gruppe S_n können in der sog. ***Tabellenschreibweise*** dargestellt werden: Sind $a_1, ..., a_n \in M_n$ vorgegeben, dann verwenden wir den Ausdruck

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

zur Darstellung der Abbildung $\sigma : M_n \to M_n$ gegeben durch $\sigma(k) = a_k$ für $1 \leq k \leq n$. Offenbar ist σ genau dann in S_n enthalten, wenn jede Zahl aus M_n unter den Werten $a_1, ..., a_n$ genau einmal vorkommt.

(iii) Sei $n \in \mathbb{N}$ und $k \in \{2, ..., n\}$. Ein ***k-Zykel*** in S_n ist ein Element $\sigma \in S_n$ mit der folgenden Eigenschaft: Es gibt eine k-elementige Teilmenge $\{m_1, ..., m_k\} \subseteq M_n$, so dass

$$\sigma(x) \quad = \quad \begin{cases} m_{i+1} & \text{falls } x = m_i \ , \ 1 \leq i < k \\ m_1 & \text{falls } x = m_k \\ x & \text{sonst} \end{cases}$$

für alle $x \in M_n$ erfüllt ist. Für ein solches Element wird die Notation $\sigma = (m_1 \ ... \ m_k)$ verwendet. Die 2-Zykel in S_n bezeichnet man auch als ***Transpositionen***.

(iv) Die ***Signumsfunktion*** ist eine Abbildung $\text{sgn} : S_n \to \{\pm 1\}$, die die Gleichung $\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$ für alle $\sigma, \tau \in S_n$ erfüllt. Ist σ ein k-Zykel, dann gilt $\text{sgn}(\sigma) = (-1)^{k-1}$.

(v) Die Teilmenge $A_n \subseteq S_n$ gegeben durch $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = +1\}$ wird als ***alternierende Gruppe*** bezeichet.

Sind $\sigma, \tau \in A_n$, dann gilt dasselbe für das Produkt $\sigma \circ \tau$, denn es gilt $\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = (+1)(+1) = +1$. Die Gleichungskette

$$\text{sgn}(\sigma^{-1}) \quad = \quad (+1)\text{sgn}(\sigma^{-1}) \quad = \quad \text{sgn}(\sigma)\text{sgn}(\sigma^{-1}) \quad = \quad \text{sgn}(\sigma \circ \sigma^{-1}) \quad = \quad \text{sgn}(\text{id}_{\mathbb{R}^n}) \quad = \quad +1$$

zeigt, dass auch σ^{-1} in A_n enthalten ist. Es lässt sich nun leicht zeigen, dass A_n mit der Komposition $\circ$ als Verknüpfung tatsächlich ebenfalls eine Gruppe bildet.

Wir werden später mit Hilfsmitteln der Gruppentheorie beweisen, dass jedes Element aus S_n auf im wesentlichen eindeutige Weise als Produkt disjunkter Zyklen dargestellt werden kann. Eine solche Darstellung bezeichnet man als ***Zykelschreibweise***. Die Zykelschreibweise ermöglicht es, die Elemente von S_n in Klassen einzuteilen und auf diese Weise eine bessere Übersicht herzustellen.

Definition 1.3 Ist $r \in \mathbb{N}$ und sind $k_1, ..., k_r \in \mathbb{N}$ mit $k_1 \geq ... \geq k_r \geq 2$, dann bezeichnet man das Tupel $(k_1, ..., k_r)$ als ***Zerlegungstyp*** eines Elements $\sigma \in S_n$, wenn σ als Produkt disjunkter Zyklen der Längen $(k_1, ..., k_r)$ dargestellt werden kann.

Beispielsweise ist $\sigma = (1\ 2\ 3)(4\ 5)(6\ 7) \in S_7$ ein Element vom Zerlegungstyp $(3, 2, 2)$. Der Identität id wird per Konvention das leere Tupel () als Zerlegungstyp zugeordnet.

Beispielsweise sind die Elemente der Gruppe S_3 durch die folgenden Tabellen gegeben.

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

In Zykelschreibweise ermöglicht eine übersichtlichere Aufzählung der Elemente, wenn man diese nach Zerlegungstyp ordnet; es ist

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

Auch die Elemente der Gruppe S_4 lassen sich noch leicht in Zykelschreibweise angeben. Schreiben wir nacheinander alle Elemente der Zerlegungstypen (), (2), (3), (4) und (2, 2) hin, so erhalten wir die Aufzählung

$$\begin{aligned} S_4 \quad = \quad & \{\ \mathrm{id}\ ,\ (1\ 2)\ ,\ (1\ 3)\ ,\ (1\ 4)\ ,\ (2\ 3)\ ,\ (2\ 4)\ ,\ (3\ 4)\ , \\ & (1\ 2\ 3)\ ,\ (1\ 3\ 2)\ ,\ (1\ 2\ 4)\ ,\ (1\ 4\ 2)\ ,\ (1\ 3\ 4)\ ,\ (1\ 4\ 3)\ ,\ (2\ 3\ 4)\ ,\ (2\ 4\ 3)\ , \\ & (1\ 2\ 3\ 4)\ ,\ (1\ 3\ 2\ 4)\ ,\ (1\ 4\ 3\ 2)\ ,\ (1\ 2\ 4\ 3)\ ,\ (1\ 3\ 4\ 2)\ ,\ (1\ 4\ 2\ 3)\ ,\ (1\ 2)(3\ 4)\ ,\ (1\ 3)(2\ 4)\ ,\ (1\ 4)(2\ 3)\ \}. \end{aligned}$$

Zu beachten ist noch, dass die Zykelschreibweise nicht ganz eindeutig ist. So gilt in S_4 beispielsweise

$$(1\ 2\ 3\ 4) \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad = \quad (2\ 3\ 4\ 1) \quad ,$$

also bezeichnen die Schreibweisen (1 2 3 4) und (2 3 4 1) dasselbe Element der Gruppe S_4.

Satz 1.4 Die Gruppe S_n ist für $n \leq 2$ abelsch und für $n \geq 3$ nicht abelsch.

Beweis: Im Fall $n = 1$ ist die Aussage klar, denn es gilt $S_1 = \{\mathrm{id}\}$. Für $n = 2$ besteht S_n aus den beiden Elementen id und (1 2). Hier kann man die Gleichung $\sigma \circ \tau = \tau \circ \sigma$ für alle $\sigma, \tau \in S_2$ leicht „von Hand“ überprüfen, indem man die vier Möglichkeiten einzeln durchgeht; beispielsweise ist $(1\ 2) \circ \mathrm{id} = (1\ 2) = \mathrm{id} \circ (1\ 2)$. Für $n \geq 3$ gilt dagegen $(1\ 2) \circ (2\ 3) = (1\ 2\ 3)$ und $(2\ 3) \circ (1\ 2) = (1\ 3\ 2)$, und diese Elemente sind offenbar voneinander verschieden. □

Aus der Linearen Algebra sind uns noch weitere Beispiele für nicht-abelsche Gruppen bekannt.

(1) Ist $n \in \mathbb{N}$ und K ein Körper, dann ist das Paar $(\mathrm{GL}_n(K), \cdot)$ bestehend aus der Menge $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$-Matrizen über K mit der Multiplikation $\cdot$ von Matrizen als Verknüpfung eine Gruppe, die sog. ***allgemeine lineare Gruppe*** über dem Körper K. Sie ist nur für $n = 1$ abelsch, ansonsten nicht-abelsch.

(2) Auch die Teilmenge $\mathrm{SL}_n(K)$ bestehend aus den Matrizen $A \in \mathrm{GL}_n(K)$ mit $\det(A) = 1_K$ bildet mit der Multiplikation von Matrizen eine Gruppe. Man bezeichnet sie als ***spezielle lineare Gruppe***. Auch sie ist für alle $n \geq 2$ nicht-abelsch.

(3) Über dem Körper $K = \mathbb{R}$ haben wir im dritten Semester noch für beliebiges $n \in \mathbb{N}$ die ***orthogonale Gruppe*** $\mathcal{O}(n)$ kennengelernt. Diese besteht aus den orthogonalen Matrizen von $\mathrm{GL}_n(\mathbb{R})$, also den Matrizen A mit der Eigenschaft ${}^tA \cdot A = E_n$. Eine zur Orthogonalität äquivalente Bedingung kann, wie wir wissen, mit dem euklidischen Standard-Skalarprodukt formuliert werden und lautet, dass $\langle Av, Aw \rangle = \langle v, w \rangle$ für alle Vektoren $v, w \in \mathbb{R}^n$ gilt. Die Matrizen der Teilmenge $\mathrm{SO}(n) = \mathcal{O}(n) \cap \mathrm{SL}_n(\mathbb{R})$ bilden ebenfalls mit der Multiplikation von Matrizen eine Gruppe, die ***spezielle orthogonale Gruppe***. In der Vorlesung hatten wir gesehen, dass beispielsweise $\mathrm{SO}(3)$ aus Drehungen besteht (um eine beliebige Achse durch $0_{\mathbb{R}^3}$, den Koordinatenursprung), und dass bei $\mathcal{O}(3)$ die Spiegelungen an einer Ebene durch $0_{\mathbb{R}^3}$ hinzukommen.

(4) Über dem Körper $K = \mathbb{C}$ gibt es entsprechend die ***unitäre Gruppe*** $\mathcal{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t\bar{A} \cdot A = E_n\}$ und die ***spezielle unitäre Gruppe*** $\mathrm{SU}(n) = \mathcal{U}(n) \cap \mathrm{SL}_n(\mathbb{C})$. Die Elemente von $\mathcal{U}(n)$ werden auch als *unitäre Matrizen* bezeichnet. Eine Matrix $A \in \mathrm{GL}_n(\mathbb{C})$ ist genau dann unitär, wenn $\langle Av, Aw\rangle = \langle v, w\rangle$ für alle $v, w \in \mathbb{C}^n$ erfüllt ist, wobei $\langle\cdot,\cdot\rangle$ in diesem Fall das *hermitesche Standard-Skalarprodukt* gegeben durch $\langle v, w\rangle = \sum_{j=1}^n v_j \bar{w}_j$ bezeichnet.

Auch bei den allgemeinen und den speziellen linearen Gruppen kann man sich die Frage stellen, aus wievielen Elemente diese bestehen. Ist K ein unendlicher Körper (z.B. $K = \mathbb{R}$), dann ist die Elementezahl von $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$ ebenfalls unendlich. Wir werden später in der Körpertheorie zeigen, dass es für jede Primzahlpotenz q einen im Wesentlichen eindeutig bestimmten Körper $\mathbb{F}_q$ im q Elementen gibt. (Vorsicht: Ist q keine Primzahl, dann stimmt $\mathbb{F}_q$ nicht mit dem Restklassenring $\mathbb{Z}/q\mathbb{Z}$ überein.) Es gilt nun

$$|\mathrm{GL}_n(\mathbb{F}_q)| \quad = \quad q^{\frac{1}{2}n(n-1)} \prod_{k=1}^{n} (q^k - 1) \quad \text{für alle } n \in \mathbb{N} \text{ und jede Primzahlpotenz } q.$$

Diese Gleichung kann man sich folgendermaßen klarmachen: Aus der Linearen Algebra wissen wir, dass eine Matrix $A \in \mathcal{M}_n(\mathbb{F}_q)$ genau dann invertierbar ist, wenn ihre n Spaltenvektoren, die wir hier mit $v_1, ..., v_n \in \mathbb{F}_q^n$ bezeichnen wollen, linear unabhängig sind, was wegen $\dim \mathbb{F}_q^n = n$ dazu äquivalent ist, dass diese Vektoren eine Basis des $\mathbb{F}_q$-Vektorraums $\mathbb{F}_q^n$ bilden. Der *Basisergänzungssatz* aus der Linearen Algebra besagt, dass wir jedes linear unabhängige System von Vektoren zu einer Basis ergänzen können. Dies bedeutet, dass wir jede Basis von $\mathbb{F}_q^n$ dadurch aufbauen können, dass wir die Vektoren $v_1, v_2, ..., v_n$ nacheinander geeignet wählen.

Wir überlegen uns nun, wieviele Möglichkeiten es für die Wahl einer Basis gibt. Für jeden Vektor $v_1 \in \mathbb{F}_q^n$ ist $\{v_1\}$ genau dann linear unabhängig, wenn $v_1 \neq 0_{\mathbb{F}_q^n}$ gilt. Dies bedeutet, dass wir $q^n - 1$ Möglichkeiten haben, das erste Element v_1 unserer Basis zu wählen. Ist nun v_1 bereits bewählt, so ist für jeden Vektor v_2 die Menge $\{v_1, v_2\}$ genau dann linear unabhängig, wenn v_2 nicht in $\langle v_1\rangle_{\mathbb{F}_q}$, dem von v_1 aufgespannten Untervektorraum, enthalten ist. Da dieser Untervektorraum aus q Elementen besteht, bleiben also $q^n - q$ Möglichkeiten für die Wahl von v_2. Bei der Wahl von v_3 sind entsprechend die q^2 Elemente von $\langle v_1, v_2\rangle_{\mathbb{F}_q}$ ausgeschlossen usw. Auf diese Weise kommen wir auf $\prod_{k=0}^{n-1}(q^n - q^k)$ Möglichkeiten für das gesamte System $v_1, v_2, ..., v_n$. Für den k-ten Faktor gilt $q^n - q^k = q^k(q^{n-k} - 1)$. Schreiben wir die Faktoren q^k vor das Produkt, so erhalten wir die angegebene Formel, mit dem Vorfaktor $q^{\sum_{k=0}^{n-1} k} = q^{\frac{1}{2}(n-1)n}$, wobei die Gleichheit $\prod_{k=0}^{n-1}(q^{n-k} - 1) = \prod_{k=1}^{n}(q^k - 1)$ durch Umparametrisierung zu Stande kommt. Mit Hilfe von etwas Gruppentheorie beweisen wir später noch die Gleichung

$$|\mathrm{SL}_n(\mathbb{F}_q)| \quad = \quad q^{\frac{1}{2}n(n-1)} \prod_{k=2}^{n} (q^k - 1).$$

Gruppen spielen unter anderem in der Geometrie, und hier besonders bei der Klassifikation geometrischer Strukturen, eine wichtige Rolle. Auf diesen Aspekt soll nun etwas genauer eingegangen werden. Im Linearen Algebra-Teil des dritten Semesters war uns der Begriff der ***Bewegung*** begegnet. Dabei handelte es sich um eine Abbildung $\phi : \mathbb{R}^n \to \mathbb{R}^n$, unter der Abstände zwischen beliebigen gleich bleiben, d.h. es gilt $\|\phi(v) - \phi(w)\| = \|v - w\|$ für alle $v, w \in \mathbb{R}^n$, wobei $\|\cdot\|$ die bekannte eudklidische Standard-Norm auf dem $\mathbb{R}^n$ bezeichnet. Dort hatten wir auch erfahren, dass für jede Bewegung ϕ jeweils ein eindeutig bestimmter Vektor $u \in \mathbb{R}^n$ und eine eindeutig bestimmte Matrix $A \in \mathcal{O}(n)$ existieren, so dass $\phi(v) = u + Av$ für alle $v \in \mathbb{R}^n$ erfüllt ist. Wir verwenden für die Bewegung, die durch diesen Vektor u und diese Matrix A gegeben ist, die Bezeichnung $\phi_{u,A}$. In dem Fall, dass A in $\mathrm{SO}(n)$ liegt, hatten wir von einer *orientierungserhaltenden* Bewegung gesprochen, ansonsten von einer *orientierungsumkehrenden* Bewegung.

Definition 1.5 Die Menge der Bewegungen im $\mathbb{R}^n$ bildet zusammen mit der Komposition eine Gruppe, die wir mit $\mathcal{B}_n$ bezeichnen. Die orientierungserhaltenden Bewegungen bilden ebenso eine Gruppe; diese bezeichnen wir mit $\mathcal{B}_n^+$.

Für den Nachweis der Gruppeneigenschaften müssen wir zunächst überprüfen, dass die Komposition zweier Bewegungen wiederum eine Bewegung ist. Seien dazu $A, A' \in \mathcal{O}(n)$ und $u, u', v \in \mathbb{R}^n$ vorgegeben. Es gilt

$$(\phi_{u,A} \circ \phi_{u',A'})(v) \quad = \quad \phi_{u,A}(u' + A'v) \quad = \quad u + A(u' + A'v) \quad = \quad (u + Au') + AA'v.$$

Dies zeigt, dass $\phi_{u,A} \circ \phi_{u',A'}$ mit $\phi_{u+Au',AA'}$ übereinstimmt, und dies ist wiederum eine Bewegung, weil mit A und A' auch AA' ein Element von $\mathcal{O}(n)$ ist. Da sich die Komposition beliebiger Abbildungen assoziativ verhält, gilt auch in $\mathcal{B}_n$ das Assoziativgesetz. Das Neutralelement in $\mathcal{B}_n$ ist durch die identische Abbildung $\mathrm{id}_{\mathbb{R}^n}$ gegeben. Dass es sich dabei um eine orthogonale Abbildung handelt, erkennt man daran, dass $\mathrm{id}_{\mathbb{R}^n} = \phi_{0_{\mathbb{R}^n},E_n}$ gilt und die Einheitsmatrix E_n orthogonal ist. Schließlich müssen wir noch zeigen, dass jedes Element $\phi_{u,A} \in \mathcal{B}_n$ (mit $u \in \mathbb{R}^n$ und $A \in \mathcal{O}(n)$) ein Inverses besitzt. Für alle $v, w \in \mathbb{R}^n$ gilt die Äquivalenz

$$w = \phi_{u,A}(v) \quad \Leftrightarrow \quad w = u + Av \quad \Leftrightarrow \quad A^{-1}w = A^{-1}u + v \quad \Leftrightarrow \quad v = A^{-1}(-u) + A^{-1}w \quad \Leftrightarrow \quad v = \phi_{A^{-1}(-u),A^{-1}}.$$

Dies zeigt, dass $\phi_{A^{-1}(-u),A^{-1}}$ die Umkehrabbildung von $\phi_{u,A}$ ist, und weil mit A auch A^{-1} in $\mathcal{O}(n)$ liegt, handelt es sich dabei um eine Bewegung. In der Gruppe $\mathcal{B}_n$ ist also $\phi_{A^{-1}(-u),A^{-1}}$ das zu $\phi_{u,A}$ inverse Element. Nach demselben Schema zeigt man, dass auch $\mathcal{B}_n^+$ eine Gruppe ist.

Definition 1.6 Ist $T \subseteq \mathbb{R}^n$ eine beliebige Teilmenge, dann bezeichnet man

$$\mathrm{Sym}(T) \quad = \quad \{\phi \in \mathcal{B}_n \mid \phi(T) = T\}$$

als ***Symmetriegruppe*** von T. Die Elemente von $\mathrm{Sym}^+(T) = \mathrm{Sym}(T) \cap \mathcal{B}_n^+$ bezeichnet man als ***orientierungserhaltende Symmetrien*** der Menge T.

Für alle $\phi, \psi \in \mathrm{Sym}(T)$ sind auch $\phi \circ \psi$ und ϕ^{-1} in $\mathrm{Sym}(T)$ enthalten. Denn auf Grund der Gruppeneigenschaft von $\mathcal{B}_n$ sind die beiden Abbildungen ebenfalls in $\mathcal{B}_n$ enthalten; außerdem gilt $(\phi \circ \psi)(T) = \phi(\psi(T)) = \phi(T) = T$ und auf Grund der Bijektivität von ϕ auch $\phi^{-1}(T) = \phi^{-1}(\phi(T)) = (\phi^{-1} \circ \phi)(T) = \mathrm{id}_{\mathbb{R}^n}(T) = T$. Der Nachweis der Gruppeneigenschaften von $\mathrm{Sym}(T)$ ist nun reine Routine. (Er wird sich im nächsten Kapitel noch etwas weiter vereinfachen, wenn wir $\mathrm{Sym}(T)$ als sog. *Untergruppe* von $\mathcal{B}_n$ erkennen.) Auch der Nachweis, dass $\mathrm{Sym}^+(T)$ eine Gruppe ist, bereitet keine Schwierigkeiten.

Zu interessanten geometrischen Anwendungen kommt man nun, indem man Teilmengen $T \subseteq \mathbb{R}^n$ mit einer bestimmten geometrischen Bedeutung betrachtet. In der Analysis mehrerer Variablen haben wir den Begriff der *konvexen Teilmenge* des $\mathbb{R}^n$ eingeführt. Eine Teilmenge $T \subseteq \mathbb{R}^n$ haben wir ***konvex*** genannt, wenn für alle $v, w \in T$ jeweils die Verbindungsstrecke $[v, w]$ ganz in T enthalten ist. Ist $X \subseteq \mathbb{R}^n$ eine beliebige Teilmenge des $\mathbb{R}^n$ und sind $T, T' \subseteq \mathbb{R}^n$ beliebige konvexe Mengen mit $T \supseteq X$ und $T' \supseteq X$, dann ist auch $T \cap T'$ eine konvex Menge mit dieser Eigenschaft.

Die *kleinste* konvexe Teilmenge des $\mathbb{R}^n$, die eine Teilmenge $X \subseteq \mathbb{R}^n$ enthält, wird die ***konvexe Hülle*** von X genannt und mit $\mathrm{conv}(X)$ bezeichnet. Die konvexe Hülle einer endlichen Teilmenge vom $\mathbb{R}^n$ bezeichnet man als ***Polytop***. Ist X nicht in einem echten affinen Unterraum des $\mathbb{R}^n$ enthalten, spricht man von einem *nicht ausgearteten* Polytop.

Definition 1.7 Sei $n \in \mathbb{N}$ mit $n \geq 3$, und für $0 \leq k < n$ sei der Punkt $P_{n,k} \in \mathbb{R}^2$ gegeben durch $P_{n,k} = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$. Dann bezeichnen wir die konvexe Hülle der endlichen Punktmenge $\{P_{n,k} \mid 0 \leq k < n\}$ als das *regelmäßiges Standard-n-Eck* Δ_n. Die Symmetriegruppe $D_n = \mathrm{Sym}(\Delta_n)$ wird die n-te ***Diedergruppe*** genannt.

Es bezeichne $\rho \in \mathcal{B}_n^+$ die Drehung um den Koordinatenursprung $0_{\mathbb{R}^2}$ mit dem Winkel $\frac{2\pi}{n}$ und $\tau \in \mathcal{B}_n$ die Spiegelung an der x-Achse. Wie man leicht überprüft, bleibt die Punktmenge $\{P_{n,k} \mid 0 \leq k < n\}$ unter ρ und τ unverändert, und daraus kann auch leicht $\rho(\Delta_n) = \Delta_n$ und $\tau(\Delta_n) = \Delta_n$ abgeleitet werden. Dies bedeutet, dass ρ und τ in $D_n = \mathrm{Sym}(\Delta_n)$ enthalten sind. Auf Grund der Gruppeneinschaft liegen auch beliebige Kompositionen von ρ und τ in D_n. Mit den Methoden der *Diskreten Geometrie* kann man zeigen, dass D_n aus genau $2n$ Elementen besteht; es gilt

$$D_n \quad = \quad \{\rho^k \mid 0 \leq k < n\} \cup \{\rho^k \circ \tau \mid 0 \leq k < n\}.$$

Wir werden später sehen, wie sich zumindest mit geringem Aufwand überprüfen lässt, dass die Elemente der Menge rechts eine Gruppe bilden. Der erste Teil der Menge aus Drehungen; genauer gesagt ist ρ^k die Drehung um $0_{\mathbb{R}^n}$ mit dem Winkel $\frac{2k\pi}{n}$. Bei den Abbildungen $\rho^k \circ \tau$ handelt es sich um Spiegelungen unterschiedlichen Typs. Ist n ungerade, dann durchläuft die Achse jeder Spiegelung durch eine Ecke und eine gegenüberliegende Kante des Polytops. Ist n dagegen gerade, dann läuft die Spiegelungsachse entweder durch zwei gegenüberliegende Ecken oder durch zwei gegenüberliegende Seiten von Δ_n.

Dass die Abbildungen der Form $\rho^k \circ \tau$ Spiegelungen sind, ist keineswegs offensichtlich, deshalb betrachten wir die Sache etwas genauer. Für jedes $\alpha \in \mathbb{R}$ sei $R_\alpha \in \mathrm{SO}(2)$ die Matrix, welche die Drehung um $0_{\mathbb{R}^2}$ mit dem Winkel α beschreibt, also

$$R_\alpha \quad = \quad \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Wie man sich leicht anschaulich klar macht (oder auch nachrechnen kann), gilt $R_\alpha \circ R_\beta = R_{\alpha+\beta}$ und $\tau \circ R_\alpha \circ \tau = R_{-\alpha}$ für beliebige $\alpha, \beta \in \mathbb{R}$, wobei wir R_α der Einfachheit halber als Bezeichnung für die Abbildung $v \mapsto R_\alpha v$ verwenden. Nach Definition gilt $\rho^k = R_{2k\pi/n}$ für $0 \leq k < n$.

Der Einfachheit halber beschränken wir uns auf den Fall, dass n ungerade ist. Sei $k \in \mathbb{Z}$ mit $0 \leq k < n$. Die Spiegelung an der Achse, die durch $0_{\mathbb{R}^n}$ und den Punkt $P_{n,k}$ verläuft, ist gegeben durch $\rho^k \circ \tau \circ \rho^{-k}$. Denn durch ρ^{-k} wird der Punkt $P_{n,k}$ auf den Punkt $P_{n,0}$ der x-Achse gedreht, anschließend durch τ gespiegelt und anschließend der Punkt $P_{n,0}$ durch ρ^k wieder zurückbewegt. Wendet man die Gleichung $\tau \circ R_\alpha \circ \tau = R_{-\alpha}$ auf den Wert $\alpha = -\frac{2k\pi}{n}$ an, so erhält man die Gleichung $\tau \circ \rho^{-k} \circ \tau = \rho^k$, was auf Grund der Identität $\tau^2 = \mathrm{id}_{\mathbb{R}^2} \Leftrightarrow \tau^{-1} = \tau$ zu $\tau \circ \rho^{-k} = \rho^k \circ \tau$ umgeformt werden kann. Einsetzen ergibt

$$\rho^k \circ \tau \circ \rho^{-k} \quad = \quad \rho^k \circ \rho^k \circ \tau \quad = \quad \rho^{2k} \circ \tau.$$

Es gilt $\rho^n = R_{2\pi/n}^n = R_{2\pi} = \mathrm{id}_{\mathbb{R}^2}$. Wählen wir $m \in \{0, 1\}$ so, dass $\ell = 2k - mn$ die Bedingung $0 \leq \ell < n$ erfüllt, dann gilt $\rho^{2k} = R_{2k\pi/n} = R_{2k\pi/n - 2m\pi} = R_{(2k-mn)\pi/n} = R_{2\ell\pi/n} = \rho^\ell$. Es gilt also $\rho^k \circ \tau \circ \rho^{-k} = \rho^\ell \circ \tau$. Damit ist nachgewiesen, dass es sich bei dem Element $\rho^\ell \circ \tau$ tatsächlich um eine Spiegelung von Δ_n handelt. Wie man leicht überprüft, durchläuft ℓ alle ganzen Zahlen mit $0 \leq \ell < n$, wenn k denselben Bereich durchläuft (sofern n ungerade ist). Dies zeigt, dass der zweite Teil der Menge von oben tatsächlich vollständig aus Spiegelungen besteht.

Es gibt noch eine andere Möglichkeit, dies zu überprüfen. Wie ρ wird auch die Bewegung τ durch eine orthogonale Matrix dargestellt, nämlich durch

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Diese Matrix hat die Determinate -1, während für alle $\alpha \in \mathbb{R}$ jeweils $\det(R_\alpha) = +1$ gilt. Die Abbildung $\rho^\ell \circ \tau$ besitzt nun die Darstellungsmatrix $R_{2\ell\pi/n}S$, und deren Determinante ist gleich $\det(R_{2\ell\pi/n}S) = \det(R_{2\ell\pi/n})\det(S) = (+1)(-1) = -1$. Nun verwendet man die bekannte Tatsache, dass die orthogonalen Matrizen mit Determinante -1 genau die linearen Abbildungen sind, welche die Spiegelung bzgl. einer Achse durch $0_{\mathbb{R}^2}$ beschreiben. Die Matrizen dieser Form besitzen immer die beiden Eigenwerte ± 1, und die Spiegelungsachse ist durch einen beliebigen Eigenvektor zum Eigenwerte $+1$ gegeben.

Wir betrachten nun einige geometrisch interessante Polytope in Dimension 3. Ein Punkt, den man als Durchschnitt eines Polytops P mit einer (affinen) Ebene erhält, wird als ***Ecke*** von von P bezeichnet. Eine Strecke, die als Durchschnitt von P mit einer Ebene zu Stande kommt, wird ***Kante*** von P genannt. Jede nichtleere Teilmenge, die als Durchschnitt von P mit einer Ebene E zu Stande kommt, bei der der Rest P vollständig auf einer Seite von E liegt und die weder eine Ecke noch eine Kante ist, wird als ***Seite*** von P bezeichnet. Wir bezeichnen zwei Teilmengen $S, T \subseteq \mathbb{R}^3$ als ***kongruent***, wenn ein $\phi \in \mathcal{B}_n$ mit $\phi(S) = T$ existiert. Von grundlegender Bedeutung in der Geometrie ist nun die folgende Definition.

Definition 1.8 Ein nicht ausgeartetes Polytop im $\mathbb{R}^3$ bezeichnet man als ***regulär*** oder auch als ***Platonischen Körper***, wenn all seine Seiten zueinander regelmäßige kongruente n-Ecke sind und sich an jeder Ecke dieselbe Anzahl von Seiten treffen.

Zwei Teilmengen $S, T \subseteq \mathbb{R}^3$ bezeichnet man als ***ähnlich***, wenn ein Skalierungsfaktor $r \in \mathbb{R}^+$ und ein $\phi \in \mathcal{B}_n$ existieren, so dass $T = \phi(rS)$ gilt. Dabei ist $rS = \{rp \mid p \in S\}$ die Teilmenge des $\mathbb{R}^3$, die durch Skalierung von S mit dem Faktor r zu Stande kommt. Seit der Antike ist bekannt, dass es bis auf Ähnlichkeit genau fünf Platonische Körper gibt.

(1) Einen ***Tetraeder*** erhält man als konvexe Hülle der vier Punkte $P_1 = (1,1,1)$, $P_2 = (1,-1,-1)$, $P_3 = (-1,1,-1)$, $P_4 = (-1,-1,1)$. Allgemein kommt eine Tetrader dadurch zu Stande, dass man über dem Schwerpunkt eines gleichseitigen Dreiecks eine weitere Ecke hinzufügt und dabei die Höhe so wählt, dass alle Kanten gleich lang werden. Jeder Tetraeder hat vier regelmäßige Dreiecke als Seiten, außerdem sechs Kanten und vier Ecken.

(2) Einen ***Oktader*** erhält man zum Beispiel als konvexe Hülle der sechselementigen Punktmenge bestehend aus $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$, $(0, 0, \pm 1)$. Allgemein konstruiert man einen Oktaeder dadurch, dass man über und unter dem Mittelpunkt eines Quadrats zwei weitere Ecken hinzufügt, wobei die Abstände so gewählt werden, dass alle Kanten dieselbe Länge haben. Jeder Oktaeder hat acht Seiten, zwölf Kanten und sechs Ecken.

(3) Einen ***Würfel*** erhält man unter anderem als konvexe Hülle der achtelementigen Punktmenge bestehend aus $(\pm 1, \pm 1, \pm 1)$ (d.h. man bildet alle acht Vorzeichenkombinationen). Geometrisch wird jeder Würfel dadurch konstruiert, indem man von einem Quadrat im Raum ausgeht, durch Parallelverschiebung ein weiteres Quadrat bildet und dann die korrespondierenden Ecken miteinander verbindet, wobei der Verschiebungsvektor so gewählt wird, dass die neu entstandenen Kanten auf den Quadraten senkrecht stehen und dieselbe Länge wie die Seiten der Quadrate haben. Jeder Würfel besitzt sechs Seiten, zwölf Kanten und acht Ecken.

(4) Einen ***Dodekaeder*** erhält man zum Beispiel als konvexe Hülle der 20 Punkte

$$(\pm\tau,\pm\tau,\pm\tau),\quad (\pm\tau_1,\pm 1,0),\quad ,(\pm 1,0,\pm\tau_1),\quad ,(0,\pm\tau_1,\pm 1)\quad ,$$

wobei jeweils alle Vorzeichenkombinationen zu berücksichtigen sind, $\tau = \frac{1}{2}(\sqrt{5}+1)$ das Verhältnis des *goldenen Schnitts* bezeichnet und $\tau_1 = \tau + 1$ ist. (Wenn eine Strecke s im Verhältnis $\tau : 1$ in zwei Teilstrecken a und b geteilt wird, dann gilt $\tau = \frac{a}{b} = \frac{s}{a}$.) Für eine geometrische Konstruktion geht man von einem regelmäßigen Fünfeck aus, setzt an jede Seite ein gleichartiges Fünfeck und fügt anschließend die sechs Fünfecke zu einer Halbkugelschale zusammen. Zwei identische Halbkugelschalen dieser Form können dann zu einem Dodekaeder zusammengesetzt werden. Jeder Dodekaeder besitzt 12 Seiten, 30 Kanten und 20 Ecken.

(5) Einen ***Ikosaeder*** erhält man unter anderem als konvexe Hülle der zwölf Punkte

$$(0,\pm 1,\pm\tau),\quad (\pm 1,0,\pm\tau),\quad (\pm 1,\pm\tau,0).$$

Für eine geometrische Konstruktion geht man von zwei parallel übereinanderliegenden, regelmäßigen Fünfecken aus und verdreht diese in einem 36°-Winkel gegeneinander. Jede Ecke des oberen Fünfecks wird mit den zwei nächstgelegenen Ecken des unteren Fünfecks verbunden. Man erhält auf diese Weise zwischen den beiden Fünfecken zehn gleichschenklige Dreiecke. Anschließend wird der Abstand zwischen den parallelen Fünfecken so eingestellt, dass die zehn gleichschenkligen Dreicke zu gleichseitigen Dreiecken werden. Nun setzt man noch einen Punkt senkrecht über den Mittelpunkt des oberen Fünfecks und verbindet diesen Punkt mit den Eckpunkten des Fünfecks. Auf diese Weise erhält man fünf weitere Dreiecke. Die Höhe des neuen Punkts wird so gewählt, dass die fünf Dreiecke zu gleichseitigen Dreiecken werden. Zum Schluss setzt man einen Punkt unter das untere Fünfeck und erzeugt auf dieselbe Weise fünf weitere gleichseitige Dreiecke, die an dem neuen Punkt anliegen. Jeder Ikosaeder besteht aus 20 Seiten, 30 Kanten und besitzt 12 Ecken.

Definition 1.9 Bezeichnet $\mathbb{T}$ einen beliebigen Tetraeder, dann nennt man $\mathrm{Sym}(\mathbb{T})$ eine ***Tetraedergruppe*** und $\mathrm{Sym}^+(\mathbb{T})$ eine ***eigentliche*** Tetraedergruppe. Ist $\mathbb{O}$ ein Oktaeder, dann wird $\mathrm{Sym}(\mathbb{O})$ eine ***Oktaedergruppe*** und $\mathrm{Sym}^+(\mathbb{O})$ eine ***eigentliche Oktaedergruppe***. Entsprechend werden (eigentliche) Würfelgruppen, Dodekaedergruppen und Ikosaedergruppen definiert.

Ein typische Element von $\mathrm{Sym}^+(\mathbb{O})$ erhält man dadurch, dass man zwei gegenüberliegen Ecken, die Mittelpunkte zweier gegenüberliegender Kanten oder die Mittelpunkte zweier gegenüberliegender Seiten durch Achsen miteinander verbindet und dann Rotationen um diese Achse betrachtet, die das Polytop $\mathbb{O}$ in sich überführen. Auf diese Weise erhält man sogenannte ***dreizählige*** bzw. zweizählige bzw. vierzählige Symmetrien. Jedes nicht orientierungserhaltende Element aus $\mathrm{Sym}(\mathbb{O})$ kommt durch eine Spiegelung zu Stande, wobei die Spiegelungsebene durch zwei gegenüberliegende Ecken, Kanten oder Seiten laufen kann.

Nachdem wir nun eine Vielzahl konkreter Beispiele von Gruppen zu sehen bekommen haben, wenden wir nun wieder allgemeineren, abstrakten Konzepten zu.

Definition 1.10 Seien G und H Gruppen. Dann bildet das kartesische Produkt $G \times H$ mit der Verknüpfung $*$ gegeben durch

$$(g_1,h_1)*(g_2,h_2) \quad = \quad (g_1g_2,h_1h_2) \qquad \text{für alle} \quad (g_1,h_1),(g_2,h_2) \in G \times H$$

ebenfalls eine Gruppe. Man nennt sie das ***(äußere) direkte Produkt*** von G und H. Sind G und H abelsch, dann gilt dasselbe für $(G \times H, *)$.

Beweis: Zunächst beweisen wir das Assoziativgesetz. Seien $(g_1,h_1),(g_2,h_2),(g_3,h_3) \in G \times H$ vorgegeben. Nach Definition der Verknüpfung $*$ und auf Grund der Assoziativität der Verknüpfungen von G und H erhalten wir

$$\begin{aligned}((g_1,h_1)*(g_2,h_2))*(g_3,h_3) \quad &= \quad (g_1g_2,h_1h_2)*(g_3,h_3) \quad = \quad ((g_1g_2)g_3,(h_1h_2)h_3) \quad = \\ (g_1(g_2g_3),h_1(h_2h_3)) \quad &= \quad (g_1,h_1)*(g_2g_3,h_2h_3) \quad = \quad (g_1,h_1)*((g_2,h_2)*(g_3,h_3)).\end{aligned}$$

Seien nun e_G, e_H die Neutralelemente der Gruppen G und H. Für alle $(g,h) \in G \times H$ gilt dann $(g,h)*(e_G,e_H) = (ge_G,he_H) = (g,h)$ und ebenso $(e_G,e_H)*(g,h) = (e_Gg,e_Hh) = (g,h)$. Dies zeigt, dass $e_{G\times H} = (e_G,e_H)$ das Neutralelement von $(G \times H, *)$ ist. Schließlich gilt auch $(g,h)*(g^{-1},h^{-1}) = (gg^{-1},hh^{-1}) = (e_G,e_H) = e_{G\times H}$ und $(g^{-1},h^{-1})*(g,h) = (g^{-1}g,h^{-1}h) = (e_G,e_H) = e_{G\times H}$. Dies zeigt, dass (g^{-1},h^{-1}) jeweils ein Inverses von (g,h) ist, für alle $(g,h) \in G \times H$. Insgesamt sind damit alle Gruppenaxiome verifiziert.

Beweisen wir nun noch die zusätzliche Aussage. Laut Annahme sind G und H abelsch. Seien $(g_1,h_1),(g_2,h_2) \in G \times H$ vorgegeben. Dann gilt $(g_1,h_1)*(g_2,h_2) = (g_1g_2,h_1h_2) = (g_2g_1,h_2h_1) = (g_2,h_2)*(g_1,h_1)$. □

Beispielsweise ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ eine achtelementige abelsche Gruppe, und $S_4 \times S_5$ ist eine nicht-abelche Gruppe bestehend aus $(4!)\cdot(5!) = 24\cdot 120 = 2880$ Elementen. Als nächstes sehen wir uns, auf welche Weise der Gruppenbegriff auf einfacheren algebraischen Strukturen aufgebaut ist.

Definition 1.11

(i) Eine ***Halbgruppe*** ist ein Paar $(G, *)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $*$ auf G.

(ii) Ein Element $e \in G$ der Halbgruppe wird als ***Neutralelement*** bezeichnet, wenn $e*a = a$ und $a*e = a$ für alle $a \in G$ erfüllt ist.

(iii) Eine Halbgruppe mit mindestens einem Neutralelement bezeichnet man als ***Monoid***.

Jede Halbgruppe besitzt höchstens ein Neutralelement. Sei nämlich $(G, *,)$ eine Halbgruppe, und seien e, e' Neutralelemente von $(G, *)$. Weil e Neutralelement ist, gilt $a*e = a$ für alle $a \in G$, insbesondere also $e'*e = e'$. Weil e' Neutralelement ist, gilt $e'*a = a$ für alle $a \in G$, also insbesondere $e'*e = e$. Insgesamt erhalten wir $e' = e'*e = e$.

Jedes Monoid $(G, *)$ besitzt also ein eindeutig bestimmtes Neutralelement, für das wir, wie beiden Gruppen, die Bezeichung e oder e_G einführen.

Definition 1.12 Sei $(G, *)$ ein Monoid mit dem Neutralelement e_G. Ein Element $g \in G$ wird ***invertierbar*** in $(G, *)$ genannt, wenn ein $h \in G$ mit $g * h = h * g = e_G$ existiert. Man nennt h in diesem Fall ein ***Inverses*** von g.

Wir formulieren einige einfache Regeln für das Rechnen mit inversen Elementen.

Proposition 1.13 Sei $(G, *)$ ein Monoid.

(i) Jedes Element $g \in G$ besitzt höchstens ein Inverses; sofern es existiert, wird es mit g^{-1} bezeichnet.

(ii) Seien $g, h \in G$ invertierbare Elemente. Dann sind auch die Elemente $g * h$ und g^{-1} invertierbar, und es gilt $(g * h)^{-1} = h^{-1} * g^{-1}$ und $(g^{-1})^{-1} = g$.

(iii) Das Neutralelement e_G ist invertierbar, und es gilt $e_G^{-1} = e_G$.

Beweis: zu (i) Nehmen wir an, dass h und h' beides Inverse von g sind. Dann gilt $g * h = e_G$ und $h' * g = e_G$, und es folgt $h = e_G * h = (h' * g) * h = h' * (g * h) = h' * e_G = h'$.

zu (ii) Die Gleichungen $(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e_G * h = h^{-1} * h = e_G$ und $(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e_G * g^{-1} = g * g^{-1} = e_G$ zeigen, dass $h^{-1} * g^{-1}$ das (eindeutig bestimmte) Inverse von G ist. Ebenso sieht man anhand der Gleichungen $g^{-1} * g = e_G$ und $g * g^{-1} = e_G$, dass es sich bei g um das Inverse von g^{-1} handelt.

zu (iii) Wie unter (ii) folgt dies direkt aus der Gleichung $e_G * e_G = e_G$. □

Als Folge dieser Proposition ist nun klar, dass die Gruppen genau diejenigen Monoide sind, bei denen alle Elemente invertierbar sind. Wie wir nun aber sehen werden, lässt sich aus jedem Monoid stets eine Gruppe gewinnen.

Definition 1.14 Sei $(X, \circ)$ eine Menge mit einer Verknüpfung. Eine Teilmenge $U \subseteq X$ wird ***abgeschlossen*** unter $\circ$ genannt, wenn für alle $x, y \in U$ auch das Element $x \circ y$ in U liegt.

Ist $U \subseteq X$ abgeschlossen unter $\circ$, dann ist die Abbildung $\circ_U : U \times U \to X$, die man durch Einschränkung von $\circ$ auf die Teilmenge $U \times U \subseteq X \times X$ erhält, zugleich eine Abbildung $U \times U \to U$, also eine Verknüpfung auf U.

Beispielsweise ist die Teilmenge $\mathbb{N} \subseteq \mathbb{Z}$ abgeschlossen unter der Addition und der Multiplikation auf $\mathbb{Z}$, denn die Summe und das Produkt von zwei positiven ganzen Zahlen ist wiederum positiv. Dagegen ist die Menge $A = \{1, 2, 3\}$ nicht abgeschlossen unter der Addition auf $\mathbb{Z}$, denn es gilt $1, 3 \in A$, aber das Element $4 = 1+3$ ist nicht in A enthalten. Die Menge A ist auch nicht abgeschlossen unter der Multipliktation, denn einerseits gilt $2, 3 \in A$, andererseits aber $6 = 2 \cdot 3 \notin A$.

Satz 1.15 Sei $(G, *)$ ein Monoid und $G^\times \subseteq G$ die Teilmenge der invertierbaren Elemente. Dann ist $G^\times$ abgeschlossen unter der Verknüpfung $*$, und $(G^\times, *_{G^\times})$ ist eine Gruppe. Das Neutralelement e_G von G ist zugleich das Neutralelement von $(G^\times, *_{G^\times})$.

Beweis: Nach Proposition 1.13 (ii) ist das Produkt zweier invertierbarer Elemente wiederum invertierbar. Die Teilmenge $G^\times \subseteq G$ ist also unter $*$ abgeschlossen, und somit existiert, wie oben erläutert, eine Verknüpfung $*_{G^\times}$ auf $G^\times$. Wir überprüfen nun für $(G^\times, *_{G^\times})$ die Gruppenaxiome. Das Assoziativgesetz ist in $G^\times$ erfüllt, denn für alle $g, h, k \in G^\times$ gilt

$$g *_{G^\times} (h *_{G^\times} k) \quad = \quad g * (h * k) \quad = \quad (g * h) * k \quad = \quad (g *_{G^\times} h) *_{G^\times} k.$$

Das Assoziativgesetz „überträgt“ sich also von $(G, *)$ auf $(G, *_{G^\times})$. Nach Proposition 1.13 (iii) ist e_G in $G^\times$ enthalten, und für alle $g \in G^\times$ gilt $g *_{G^\times} e_G = g * e_G = g$ und $e_G *_{G^\times} g = e_G * g = g$. Dies zeigt, dass e_G in der Halbgruppe $(G^\times, *_{G^\times})$ ein Neutralelement ist. Somit ist $(G^\times, *_{G^\times})$ ein Monoid, mit Neutralelement $e_{G^\times} = e_G$.

Wiederum auf Grund von Proposition 1.13 (ii) folgt aus $g \in G^\times$ auch $g^{-1} \in G^\times$. Wegen $g *_{G^\times} g^{-1} = g * g^{-1} = e_G$ und $g^{-1} *_{G^\times} g = g^{-1} * g = e_G$ ist g^{-1} das Inverse von g in $(G^\times, *)$. Jedes Element aus $G^\times$ ist also im Monoid $(G^\times, *)$ invertierbar. Somit ist $(G^\times, *_{G^\times})$ eine Gruppe. □

Der Einfachheit halber wird die Verknüpfung der Gruppe $(G^\times, *_{G^\times})$ von nun an einfach wieder mit $*$ bezeichnet.

Wie wir anhand der bisherigen Beispiele bereits deutlich geworden ist, werden bei Halbgruppen, Monoiden und Gruppen in zwei unterschiedlichen Schreibweisen verwendet, die von der Form des Verknüpfungssymbols abhängen. Bei einem „punktähnlichen“ Symbol wie $\cdot$ oder $\odot$ bezeichnet man das Neutralelement eines Monoids neben e_G auch mit 1_G, und die Schreibweise für das Inverse eines Elements g ist stets g^{-1}. Man spricht in diesem Zusammenhang von ***multiplikativer Schreibweise***. Häufig wird ein punktähnliches Verknüpfungssymbol auch weggelassen, das Element $g \cdot h$ also mit gh bezeichnet.

Bei einem „plusartigen“ Verknüpfungssymbol wie $+$ oder $\oplus$ verwendet man für das Neutralelement die Notation 0_G, und die Schreibweise für das Inverse von g ist $-g$ statt g^{-1}. Die Gleichungen $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ und $(g^{-1})^{-1} = g$ haben bei additiver Schreibweise also die Form $-(g + h) = (-h) + (-g)$ und $-(-g) = g$. Hier spricht man von ***additiver Schreibweise***; sie ist nur bei abelschen Halbgruppen (bzw. Monoiden oder Gruppen) gebräuchlich.

Ein wichtiges (und zugleich noch weit entferntes) Ziel der Algebra besteht darin, für jede Zahl $n \in \mathbb{N}$ „alle“ Gruppen mit n Elementen zu bestimmen. Ein grundsätzliches Problem besteht aber darin, dass es einerseits unüberschaubar viele n-elementige Mengen M gibt, auf den man jeweils eine Gruppenstruktur definieren könnte (durch Angabe einer Verknüpfung $\cdot$, einem Neutralelement $e \in M$ und einer Inversenabbildung $M \to M$, $a \mapsto a^{-1}$), dass sich aber andererseits viele dieser Gruppen anhand ihrer Strukturmerkmale gar nicht unterscheiden. (Was für Merkmale das sein können, ist das Thema der folgenden Kapitel.) Um diesem Problem zu begegnen, für man den *Isomorphiebegriff* in die Gruppentheorie ein.

Definition 1.16 Man bezeichnet zwei Gruppen $(G, \cdot)$ und $(H, *)$ als ***isomorph*** und schreibt $G \cong H$, wenn eine bijektive Abbildung $\phi : G \to H$ existiert, so dass $\phi(g \cdot g') = \phi(g) * \phi(g')$ für alle $g, g' \in G$ erfüllt ist.

Mit Hilfe des *Chinesischen Restsatzes* werden wir beispielsweise zeigen können, dass die Gruppen $\mathbb{Z}/15\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ zueinander isomorph sind. Durch die Hilfsmittel, die wir im Kapitel über Gruppenoperationen entwickeln werden, werden wir bezüglich der Diedergruppen und der Symmetriegruppen der platonischen Körper zeigen können

(i) Jede Diedergruppe D_n (mit $n \geq 3$) ist isomorph zu einer $2n$-elementigen Untergruppe von S_n.

(ii) Für die Symmetriegruppen des Tetraeders gilt $\mathrm{Sym}^+(\mathbb{T}) \cong A_4$ und $\mathrm{Sym}(\mathbb{T}) \cong S_4$.

(iii) Es gilt $\mathrm{Sym}^+(\mathbb{O}) \cong \mathrm{Sym}^+(\mathbb{W}) \cong S_4$ und $\mathrm{Sym}(\mathbb{O}) \cong \mathrm{Sym}(\mathbb{W}) \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$ für die Symmetriegruppen von Würfel und Oktaeder.

(iv) Für die Symmetriegruppen von Dodekaeder und Ikosaeder gilt $\mathrm{Sym}^+(\mathbb{D}) \cong \mathrm{Sym}^+(\mathbb{I}) \cong A_5$ und $\mathrm{Sym}(\mathbb{D}) \cong \mathrm{Sym}(\mathbb{I}) \cong A_5 \times \mathbb{Z}/2\mathbb{Z}$.

Dass die Symmetriegruppe von Würfel und Oktaeder bzw. Dodekaeder und Ikosaeder isomorph sind, hat folgenden Grund: Jedem nicht-ausgearteten Polytop P mit dem Nullpunkt $0_{\mathbb{R}^3}$ in seinem Inneren kann mit Hilfe des euklidischen Skalarprodukts durch

$$P^\vee \quad = \quad \{x \in \mathbb{R}^3 \mid \langle x, y \rangle \leq 1 \, \forall y \in P\}$$

ein sogenanntes ***duales Polytop*** zugeordnet werden. Dieses ist ebenfalls nicht-ausgeartet und enthält $0_{\mathbb{R}^3}$ als inneren Punkt. Jede Ecke von P entspricht einer Seite von $P^\vee$, jede Seite von P entspricht einer Ecke von $P^\vee$, und es gibt eine bijektive Korrespondenz zwischen den Kanten von P und denen von $P^\vee$. Es ist relativ leicht zu sehen, dass stets P und $P^\vee$ isomorphe Symmetriegruppen besitzen, und dass $(P^\vee)^\vee = P$ gilt. Durch Dualisierung eines Würfels erhält man einen Oktaeder, und ein Dodekaeder wird durch diesen Vorgang in ein Ikosaeder überführt. Ein Tetrader geht durch Dualisierung in einen anderen Tetraeder über.

Wie wir sehen werden, haben stimmen zwei isomorphe Gruppen bezüglich jedes Strukturmerkmals überein. Dazu gehört zum Beispiel die Anzahl der Untegruppen und Normalteiler, die Anzahl der Elemente bestimmter Ordnung und Eigenschaften wie „zyklisch“, „abelsch“ oder „auflösbar“, um nur ein paar der Merkmale zu nennen, mit denen wir uns im weiteren Verlauf befassen. Die Frage, welche „wesentlich voneinander verschiedenen“ Untergruppen einer bestimmten Ordnung n es gibt, lässt sich mit dem Isomorphiebegriff folgendermaßen konkretisieren.

Definition 1.17 Das ***Klassifikationsproblem für endliche Gruppen*** kann folgendermaßen formuliert werden: Gegeben ein $n \in \mathbb{N}$, bestimme alle Gruppen mit n Elementen bis auf Isomorphie. Damit ist gemeint: Bestimme eine Zahl $r(n)$ und Gruppen $G_1, G_2, \ldots, G_{r(n)}$ mit der Eigenschaft, dass *jede* Gruppe G mit $|G| = n$ zu genau einer dieser Gruppen isomorph ist.

Aus der Formulierung ergibt sich unmittelbar, dass in der Liste der $r(n)$ Gruppen für $1 \leq i, j \leq r(n)$ nur dann $G_i \cong G_j$ gilt, wenn $i = j$ ist. Mit Hilfe der Theorie, die wir hier entwickeln, werden wir zeigen können

- Ist p eine Primzahl, dann ist jede Gruppe G mit $|G| = p$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Es gilt also $r(p) = 1$.
- Für jede Primzahl p gilt: Jede Gruppe G mit $|G| = p^2$ ist entweder isomorph zu $\mathbb{Z}/p^2\mathbb{Z}$ oder isomorph zu $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Es gilt also $r(p^2) = 2$.
- Für jede ungerade Primzahl p gilt außerdem: Jede Gruppe der Ordnung $2p$ ist entweder isomorph zu $\mathbb{Z}/2p\mathbb{Z}$ oder zur Diedergruppe D_p. Es gilt also auch $r(2p) = 2$.

Des Weiteren werden wir in der Lage sein, alle Gruppen mit ≤ 15 Elementen bis auf Isomorphie zu bestimmen. Das Ergebnis kann in der folgenden Tabelle zusammengefasst werden.

n	$r(n)$	Gruppen bis auf Isomorphie
1	1	$\mathbb{Z}/1\mathbb{Z}$
2	1	$\mathbb{Z}/2\mathbb{Z}$
3	1	$\mathbb{Z}/3\mathbb{Z}$
4	2	$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	1	$\mathbb{Z}/5\mathbb{Z}$
6	2	$\mathbb{Z}/6\mathbb{Z},\ S_3$
7	1	$\mathbb{Z}/7\mathbb{Z}$
8	5	$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ Q_8$
9	2	$\mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	2	$\mathbb{Z}/10\mathbb{Z},\ D_5$
11	1	$\mathbb{Z}/11\mathbb{Z}$
12	5	$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z},\ D_6,\ A_4,\ \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
13	1	$\mathbb{Z}/13\mathbb{Z}$
14	2	$\mathbb{Z}/14\mathbb{Z},\ D_7$
15	1	$\mathbb{Z}/15\mathbb{Z}$

Dabei bezeichnet Q_8 die sog. ***Quaternionengruppe*** bestehend aus der achtelementigen Menge $\{\pm E, \pm I, \pm J, \pm K\} \subseteq \mathrm{GL}_2(\mathbb{C})$ mit den Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad I = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \quad , \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Bei $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ handelt es sich um ein ***semidirektes Produkt***, eine Verallgemeinerung des direkten Produkts aus diesem Kapitel, das wir zu einem späteren Zeitpunkt noch definieren werden.

§ 2. *Untergruppen und der Satz von Lagrange*

Zusammenfassung. Eine *Untergruppe* ist eine Teilmenge U einer Gruppe G mit der Eigenschaft, dass e_G in U liegt, und mit $g, h \in U$ auch gh und g^{-1} in U enthalten sind. Durch diese Bedingungen ist sichergestellt, dass auch U die Struktur einer Gruppe besitzt. Jeder Teilmenge S einer Gruppe G kann eine Untergruppe $\langle S \rangle$ zugeordnet werden. Es handelt sich dabei um die kleinste Untergruppe von G, die S enthält. Oft reicht eine recht kleine Teilmenge S aus, um sogar ganz G zu erzeugen; bei den symmetrischen Gruppen S_n genügt beispielsweise eine zweielementige Menge. Untergruppen, die von einem einzigen Element erzeugt werden, nennt man *zyklisch*.

Der *Satz von Lagrange* besagt, dass bei einer endlichen Gruppe G die Ordnung jeder Untergruppe U ein Teiler von $|G|$ ist. Der Beweis beruht auf der Beobachtung, dass jede Untergruppe U eine *Zerlegung* der Gruppe in gleich große Teilmengen ermöglicht, die sog. Links- und Rechtsnebenklassen der Untergruppe. Wir wiederholen den bereits aus der Linearen Algebra bekannten Zusammenhang zwischen Zerlegungen und Äquivalenzrelationen. Für den praktischen Umgang mit Nebenklassenzerlegungen ist das Konzept der *Repräsentantensysteme* hilfreich.

Wichtige Grundbegriffe

- n-te Potenz eines Gruppenelements ($n \in \mathbb{Z}$) ´
- Definition der Untergruppen
- Erzeugendensysteme einer Gruppe
- zyklische Gruppe
- Konjugation von Gruppenelementen
- Links- und Rechtsnebenklassen einer Untergruppe
- Repräsentantensystem
- Index $(G : U)$ einer Untergruppe

Zentrale Sätze

- Gruppen-Eigenschaft der Untergruppen
- Existenz und Eindeutigkeit der von einer Teilmenge $S \subseteq G$ erzeugten Untergruppe $\langle S \rangle$
- Vertauschbarkeit von Permutationen mit disjunktem Träger
- Satz von Lagrange
- Kleiner Satz von Fermat

Bereits in der Analysis-Vorlesung wurde die ***n-te Potenz*** eines Körperelements für alle $n \in \mathbb{Z}$ definiert. Die Definition lässt sich problemlos auf die Elemente einer Halbgruppe bzw. eines Monoids übertragen.

Definition 2.1 Ist $(G, *)$ eine Halbgruppe und $g \in G$ ein beliebiges Element, dann definiert man rekursiv $g^1 = g$ und $g^{n+1} = g^n * g$ für alle $n \in \mathbb{N}$. Ist $(G, *)$ ein Monoid, dann setzt man $g^0 = e_G$. Ist g darüber hinaus invertierbar, dann setzt man $g^{-n} = (g^n)^{-1}$ für alle $n \in \mathbb{N}$ und hat damit insgesamt g^n für alle $n \in \mathbb{Z}$ definiert.

Lemma 2.2 Sei $(G, *)$ eine Halbgruppe.

(i) Für alle $g \in G$ und $m, n \in \mathbb{N}$ gilt $g^m * g^n = g^{m+n}$ und $(g^m)^n = g^{mn}$.

(ii) Sind $g, h \in G$ ***vertauschbare*** Elemente, gilt also $g * h = h * g$, dann folgt $(g * h)^n = g^n * h^n$ für $g, h \in G$ und $n \in \mathbb{N}$.

(iii) Ist allgemeiner $\{g_1, ..., g_r, h_1, ..., h_r\}$ eine Menge in G bestehend aus paarweise vertauschbaren Elementen (mit $r \in \mathbb{N}$), dann gilt die Regel

$$(g_1 * ... * g_r) * (h_1 * ... * h_r) \quad = \quad (g_1 * h_1) * ... * (g_r * h_r)$$

und außerdem $(g_1 * ... * g_r)^m = g_1^m * ... * g_r^m$.

In einem Monoid gelten alle Regeln entsprechend für $m, n \in \mathbb{N}_0$, im Falle invertierbarer Elemente g, h für $m, n \in \mathbb{Z}$.

Den *Beweis* dieses Lemmas behandeln wir in den Übungen.

Liegt die Halbgruppe $(G, +)$ in additiver Schreibweise vor, dann schreibt man ng statt g^n. Die rekursive Definition der n-ten Potenz lautet dann $1 \cdot g = g$ und $(n+1)g = ng + g$, und die übrigen Rechenregeln nehmen die folgende Form an.

$$mg + ng = (m+n)g \quad , \quad n(mg) = (mn)g \quad , \quad n(g+h) = ng + nh \quad ,$$
$$(g_1 + ... + g_r) + (h_1 + ... + h_r) = (g_1 + h_1) + ... + (g_r + h_r) \quad , \quad g_1 + ... + g_r = g_r + ... + g_1 \quad ,$$
$$m(g_1 + ... + g_r) = mg_1 + ... + mg_r.$$

Man beachte, dass die dritte bis sechste Regel wiederum die Vertauschbarkeit der Elemente erfordert. Allerdings hatten wir ja bereits bemerkt, dass die additive Schreibweise nur bei kommutativen Strukturen verwendet wird.

Definition 2.3 Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ wird ***Untergruppe*** von G genannt, wenn e_G in U liegt und für alle $a, b \in U$ auch die Elemente $a \cdot b$ und a^{-1} in U liegen.

Die Schreibweise $U \leq G$ bedeutet, dass U eine Untergruppe von G ist.
Wir ergänzen die Definition um zwei Bemerkungen.

(1) In der Definition enthalten ist die Bedingung, dass U eine unter der Verknüpfung $\cdot$ abgeschlossene Teilmenge ist. Wie in § 1 ausgeführt, erhält man somit durch Einschränkung eine Verknüpfung $\cdot_U$ auf U.

(2) Unmittelbar aus Definition ergibt sich auch, dass für alle $a \in U$ und $m \in \mathbb{Z}$ auch a^m in U enthalten ist, und das für jedes $r \in \mathbb{N}$ mit $a_1, ..., a_r \in U$ auch das Produkt $a_1 \cdot ... \cdot a_r$ in U enthalten ist. Beide Aussagen zeigt man durch einfache Induktionsbeweise.

An die Bemerkung (1) schließt sich folgende Feststellung an, durch den Begriff „Untergruppe“ letztlich rechtfertigt.

Proposition 2.4 Das Paar $(U, \cdot_U)$ ist eine Gruppe.

Beweis: Die Verknüpfung $\cdot_U$ stimmt auf ihrem gesamten Definitionsbereich mit $\cdot$ überein. Wieder überträgt sich das Assoziativgesetz von $(G, \cdot)$ auf $(U, \cdot_U)$, d.h. für alle $a, b, c \in U$ gilt $(a \cdot_U b) \cdot_U c = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot_U (b \cdot_U c)$ für alle $a, b, c \in U$. Auf Grund der Voraussetzung $e_G \in U$ und wegen $e_G \cdot_U a = e_G \cdot a = a$, $a \cdot_U e_G = a \cdot e_G = a$ ist e_G ein Neutralelement der Halbgruppe $(U, \cdot_U)$; die Halbgruppe ist also ein Monoid. Für jedes $a \in U$ ist auch a^{-1} in U enthalten. Die Gleichungen $a \cdot_U a^{-1} = a \cdot a = e_G$ und $a^{-1} \cdot_U a = a^{-1} \cdot a = e_G$ zeigen jeweils, dass a im Monoid $(U, \cdot_U)$ ein invertierbares Element ist, und das Inverse von a in $(G, \cdot)$ zugleich das Inverse von a in $(U, \cdot_U)$. Insgesamt ist $(U, \cdot_U)$ also tatsächlich eine Gruppe. □

Bereits im ersten Kapitel sind uns eine Vielzahl von Untergruppen begegnet.

(i) Ist G eine beliebige Gruppe, dann sind $\{e_G\}$ und G Untergruppen von G. Man bezeichnet $\{e_G\}$ auch als die ***triviale*** Untergruppe von G. Für beide Mengen kontrolliert man unmittelbar, dass die Untergruppen-Bedingungen erfüllt sind.

(ii) Die Gruppe $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$, und diese wiederum ist eine Untergruppe von $(\mathbb{R}, +)$.

(iii) Für jedes $n \in \mathbb{N}$ ist die alternierende Gruppe A_n eine Untergruppe der symmetrischen Gruppe S_n. Des Weiteren ist die vierelementige Menge

$$V_4 \quad = \quad \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

ihrerseits eine Untergruppe von A_4. Man nennt sie die ***Kleinsche Vierergruppe***. Zum Nachweis der Untergruppen-Eigenschaft bemerken wir zunächst, dass das Neutralelement id von A_4 in V_4 liegt. Die Verknüpfungstabelle

$\circ$	id	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
id	id	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2)(3 4)	(1 2)(3 4)	id	(1 4)(2 3)	(1 3)(2 4)
(1 3)(2 4)	(1 3)(2 4)	(1 4)(2 3)	id	(1 2)(3 4)
(1 4)(2 3)	(1 4)(2 3)	(1 3)(2 4)	(1 2)(3 4)	id

hat nur Einträge in V_4; dies zeigt, dass V_4 eine bezüglich $\circ$ abgeschlossene Teilmenge von A_4 ist. Außerdem rechnet man unmittelbar nach, dass

$$((1\ 2)(3\ 4))^2 \quad = \quad ((1\ 3)(2\ 4))^2 \quad = \quad ((1\ 4)(2\ 3))^2 \quad = \quad \mathrm{id}$$

gilt und somit neben id auch jedes andere Element in V_4 sein eignes Inverses ist. Für jedes $\sigma \in V_4$ gilt also insbesondere $\sigma^{-1} \in V_4$, wodurch auch die letzte Untergruppen-Eigenschaft nachgewiesen ist.

(iv) Die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ ist eine Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(K)$ (für jeden Körper K und $n \in \mathbb{N}$). Ebenso ist $\mathcal{O}(n)$ eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$, und $\mathcal{U}(n)$ ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{C})$.

(v) Die Gruppe $\mathcal{B}_n$ der Bewegungen ist eine Untergruppe von $\mathrm{Per}(\mathbb{R}^n)$, und $\mathcal{B}_n^+$ ist eine Untergruppe von $\mathcal{B}_n$, und wiederum auch von $\mathrm{Per}(\mathbb{R}^n)$.

(vi) Für jede Teilmenge $T \subseteq \mathbb{R}^n$ ist die Symmetriegruppe $\mathrm{Sym}(T)$ eine Untergruppe von $\mathcal{B}_n$, und $\mathrm{Sym}^+(T)$ ist eine Untergruppe von $\mathcal{B}_n^+$.

Um die Struktur einer Gruppe G zu verstehen, ist es wichtig, einen Überblick über die Untergruppen von G zu erhalten. Als nächstes befassen wir uns deshalb mit der Frage, wie sich die Untergruppen auf möglichst effiziente Weise spezifieren lassen. Dies führt uns auf den Begriff des *Erzeugendensystems*.

Proposition 2.5 Sei $(G, \cdot)$ eine Gruppe, und sei $(U_i)_{i \in I}$ eine Familie von Untergruppen von G. Dann ist auch $U = \bigcap_{i \in I} U_i$ eine Untergruppe von G.

Beweis: Weil jedes U_i eine Untergruppe von $(G, \cdot)$ ist, gilt $e_G \in U_i$ für alle $i \in I$ und damit auch $e_G \in U$. Seien nun $a, b \in U$ vorgegeben. Dann gilt $a, b \in U_i$ für alle $i \in I$, und aus der Untergruppe-Eigenschaft von U_i folgt jeweils $ab \in U_i$ und $a^{-1} \in U_i$, für jedes $i \in I$. Daraus wiederum folgt $ab \in U$ und $a^{-1} \in U$. □

In vielen Situationen ist es wünschenswert, Untergruppen auf möglichst kurze und einfache Art und Weise zu spezifizieren. Eine einfache Möglichkeit ist die Beschreibung von Untergruppen durch Erzeugendensysteme.

Satz 2.6 Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Dann gibt es eine eindeutig bestimmte Untergruppe U von G mit den folgenden Eigenschaften.

(i) $U \supseteq S$

(ii) Ist V eine weitere Untergruppe von G mit $V \supseteq S$, dann folgt $V \supseteq U$.

Beide Bedingungen lassen sich zusammenfassen in der Aussage, dass U die *kleinste* Untergruppe von G ist, die S als Teilmenge enthält.

Beweis: *Existenz:* Sei (U_i) die Familie aller Untergruppen von G mit $U_i \supseteq S$. Dann ist nach Proposition 2.5 auch $U = \bigcap_{i \in I} U_i$ eine Untergruppe von G, und aus $U_i \supseteq S$ für alle $i \in I$ folgt $U \supseteq S$. Sei nun V eine weitere Untergruppe von G mit $V \supseteq S$. Dann gilt $V = U_j$ für ein $j \in I$, und weil nach Definition $U \subseteq U_i$ für alle $i \in I$ gilt, folgt $V \supseteq U$.

Eindeutigkeit: Seien U, U' zwei Untergruppen von G, die beide (i) und (ii) erfüllen. Dann gilt $U \supseteq S$ und $U' \supseteq S$. Aus der Eigenschaft (ii) für U folgt $U' \supseteq U$, und aus Eigenschaft (ii) für U' folgt $U \supseteq U'$, insgesamt also $U = U'$. □

Definition 2.7 Die Untergruppe U aus Satz 2.6 wird die von S ***erzeugte*** Untergruppe genannt und mit $\langle S \rangle$ bezeichnet. Ist V eine beliebige Untergruppe von G, dann wird jede Teilmenge T von G mit $V = \langle T \rangle$ ein ***Erzeugendensystem*** von V genannt.

Ist S eine einelementige Teilmenge einer Gruppe G, $S = \{g\}$ für ein $g \in G$, dann verwendet man die Notation $\langle g \rangle$ an Stelle der korrekten, aber umständlichen Schreibweise $\langle \{g\} \rangle$. Auch bei endlichen Mengen mit mehr Elementen wird häufig an Stelle von $\langle \{g_1, ..., g_n\} \rangle$ die einfachere Notation $\langle g_1, ..., g_n \rangle$ verwendet. Wir betrachten nun eine Reihe von Beispielen für Erzeugendensysteme von Untergruppen.

(i) In jeder Gruppe G gilt $\langle\varnothing\rangle = \{e_G\}$. Denn wie wir bereits festgestellt haben, ist $\{e_G\}$ eine Untergruppe, und diese enthält trivialerweise $\varnothing$ als Teilmenge. Andererseits ist e_G in jeder Untergruppe U von G enthalten, also ist $\{e_G\}$ eine Teilmenge jeder Untergruppe V von G mit $V \supseteq \varnothing$.

(ii) Es ist leicht zu sehen, dass die Gruppe $(\mathbb{Z}, +)$ von der einelementigen Menge $\{1\}$ erzeugt wird, denn jedes Element $k \in \mathbb{Z}$ kann in der Form $k \cdot 1$ dargestellt werden, wobei $k \cdot 1$ die k-te Potenz des Elements 1 in additiver Schreibweise bedeutet. Ebenso ist $\{-1\}$ ein Erzeugendensystem, denn jedes $k \in \mathbb{Z}$ hat die Darstellung $k = (-k) \cdot (-1)$. Allgemein gilt $\langle m\rangle = m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$ für jedes $m \in \mathbb{N}_0$.

Wir werden später sehen, dass alle Untergruppen von $(\mathbb{Z}, +)$ diese Form haben. Dass sich alle Untergruppen einer Gruppe so leicht angeben lassen, ist leider nur sehr selten der Fall.

Definition 2.8 Eine Gruppe G wird ***zyklisch*** genannt, wenn ein $g \in G$ mit $G = \langle g\rangle$ existiert. Existiert eine endliche Teilmenge $S \subseteq G$ mit $G = \langle S\rangle$, dann nennt man G eine ***endlich erzeugte*** Gruppe.

Die zyklischen Gruppen werden wir in § 3 ausführlich studieren. Ein einfaches Beispiel ist, wie wir oben gesehen haben, die Gruppe $(\mathbb{Z}, +)$. Die endlich erzeugten Gruppen sind leider nicht so übersichtlich, aber in § 5 werden wir zumindest die endlich erzeugten *abelschen* Gruppen bis auf Isomorphie klassifizieren. Es ist relativ leicht zu sehen, dass beispielsweise die Gruppe $(\mathbb{Q}, +)$ nicht endlich erzeugt ist. Den Beweis behandeln wir in den Übungen.

Unser nächstes Ziel besteht darin, die in einer Untergruppe der Form $\langle S\rangle$ liegenden Elemente explizit anzugeben. Dazu verwenden wir sowohl die im Anschluss an Definition 2.3 formulierte Eigenschaft von Untergruppen als auch die in Proposition 1.13 formulierten Rechenregeln für invertierbare Elemente. Um die folgenden Aussagen zu vereinfachen, führen wir die folgende Konvention ein: Das Neutralelement e_G einer Gruppe G ist bei uns stets ein Produkt aus null Faktoren. Der Ausdruck $g_1 \cdot \ldots \cdot g_r$ steht also im Fall $r = 0$ für das Element e_G.

Satz 2.9 Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge.

(i) Die Elemente von $\langle S\rangle$ sind gegeben durch

$$\langle S\rangle \quad = \quad \{g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0\ ,\ g_1, \ldots, g_r \in S, \varepsilon_k \in \{\pm 1\} \text{ für } 1 \leq k \leq r\}.$$

(ii) Sei S endlich, $S = \{g_1, \ldots, g_m\}$ für ein $m \in \mathbb{N}_0$, und setzen wir voraus, dass jedes Element der Menge S mit jedem anderen vertauschbar ist. Dann gilt

$$\langle S\rangle = \{g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \mid e_k \in \mathbb{Z} \text{ für } 1 \leq k \leq m\}.$$

Beweis: zu (i) Sei U die Teilmenge auf der rechten Seiten der Gleichung. Zunächst überprüfen wir, dass U eine Untergruppe von G ist. Da wir in der Definition von U Produkte der Länge $r = 0$ eingeschlossen haben, ist das Neutralelement e_G in U enthalten. Seien nun $g, g' \in U$ vorgegeben. Dann gibt es nach Definition Elemente $r, s \in \mathbb{N}_0$,

$g_1, ..., g_r, g'_1, ..., g'_s \in S$ und $\varepsilon_1, ..., \varepsilon_r, \varepsilon'_1, ..., \varepsilon'_s \in \{\pm 1\}$, so dass $g = g_1^{\varepsilon_1} \cdot ... \cdot g_r^{\varepsilon_r}$ und $g' = (g'_1)^{\varepsilon'_1} \cdot ... \cdot (g'_s)^{\varepsilon_s}$ erfüllt ist. Offenbar sind die Elemente

$$gg' = g_1^{\varepsilon_1} \cdot ... \cdot g_r^{\varepsilon_r} \cdot (g'_1)^{\varepsilon'_1} \cdot ... \cdot (g'_s)^{\varepsilon_s} \qquad \text{und} \qquad g^{-1} = g_r^{-\varepsilon_r} \cdot ... \cdot g_1^{-\varepsilon_1}$$

nach Definition ebenfalls in U enthalten. Also handelt es sich bei U tatsächlich um eine Untergruppe von G. Außerdem enthält sie S als Teilmenge: Ist $g \in S$ beliebig vorgegeben, dann setzt man $g_1 = g$, $\varepsilon_1 = 1$ und erhält $g = g_1^{\varepsilon_1} \in U$.

Nun müssen wir noch zeigen, dass U die kleinste Untergruppe von G mit $U \supseteq S$ ist. Sei V eine beliebige Untergruppe von G mit $V \supseteq S$; nachzuweisen ist $V \supseteq U$. Zunächst bemerken wir, dass das Produkt der Länge $r = 0$ in V enthalten ist, denn als Untergruppe von G enthält V das Neutralelement e_G. Seien nun $r \in \mathbb{N}$, $g_1, ..., g_r \in S$ und $\varepsilon_1, ..., \varepsilon_r \in \{\pm 1\}$. Wegen $S \subseteq V$ gilt dann auch $g_1, ..., g_r \in V$. Weil V eine Untergruppe von G ist, folgt $g_k^{\varepsilon_k} \in V$ für $1 \leq k \leq r$ und schließlich $g_1^{\varepsilon_1} \cdot ... \cdot g_r^{\varepsilon_r} \in V$. Damit ist der Nachweis der Inklusion $U \subseteq V$ erbracht.

zu (ii) Hier gehen wir nach demselben Schema vor und zeigen zunächst, dass die Menge auf der rechten Seite der Gleichung, die wir mit U bezeichnen, eine Untergruppe von G ist. Durch Setzen von $e_k = 0$ für $1 \leq k \leq m$ sieht man, dass U das Neutralelement enthält. Seien nun $g, g' \in U$ vorgegeben. Dann gibt es Elemente $e_1, ..., e_m, e'_1, ..., e'_m \in \mathbb{Z}$ mit $g = g_1^{e_1} \cdot ... \cdot g_m^{e_m}$ und $g' = g_1^{e'_1} \cdot ... \cdot g_m^{e'_m}$. Es folgt

$$gg' \quad = \quad (g_1^{e_1} \cdot ... \cdot g_m^{e_m})(g_1^{e'_1} \cdot ..... \cdot g_m^{e'_m}) \quad = \quad (g_1^{e_1} g_1^{e'_1}) \cdot ... (g_m^{e_m} g_m^{e'_m}) \quad = \quad g_1^{e_1+e'_1} \cdot ... \cdot g_m^{e_m+e'_m}$$

und

$$g^{-1} \quad = \quad (g_1^{e_1} \cdot ... \cdot g_m^{e_m})^{-1} \quad = \quad (g_m^{e_m})^{-1} \cdot ... \cdot (g_1^{e_1})^{-1} \quad = \quad g_m^{-e_m} \cdot ... \cdot g_1^{-e_1} \quad = \quad g_1^{-e_1} \cdot ... \cdot g_m^{-e_m} \in U.$$

Damit ist der Nachweis der Untergruppen-Eigenschaft abgeschlossen. Nun zeigen wir, dass $U \supseteq S$ gilt. Sei dazu $k \in \{1, ..., m\}$ vorgegeben. Setzen wir $e_k = 1$ und $e_i = 0$ für $1 \leq i \leq m$ mit $i \neq k$, dann erhalten wir $g_k = g_1^{e_1} \cdot ... \cdot g_m^{e_m} \in U$. Sei nun V eine beliebige Untergruppe von G mit $V \supseteq S$. Dann gilt $g_k \in V$ für $1 \leq k \leq m$. Sind $e_1, ..., e_m \in \mathbb{Z}$ beliebig vorgegeben, dann folgt auf Grund der Untergruppen-Eigenschaft $g_k^{e_k} \in V$ für $1 \leq k \leq m$ und schließlich $g_1^{e_1} \cdot ... \cdot g_m^{e_m} \in V$. Damit ist der Nachweis von $U \subseteq V$ abgeschlossen. □

Folgerung 2.10

(i) Ist G eine Gruppe und $g \in G$, dann gilt $\langle g \rangle = \{g^e \mid e \in \mathbb{Z}\}$.

(ii) Jede zyklische Gruppe ist abelsch.

Beweis: Die Aussage (i) ist der Spezialfall von Satz 2.9 (ii) mit $m = 1$. Zum Beweis von (ii) sei G eine zyklische Gruppe und $g_1 \in G$ ein Element mit $G = \langle g_1 \rangle$. Sind $g, h \in G$ beliebig vorgegeben, dann gilt nach (i) $g = g_1^m$ und $h = g_1^n$ für geeignete $m, n \in \mathbb{Z}$. Es folgt $gh = g_1^m g_1^n = g_1^{m+n} = g_1^{n+m} = g_1^n g_1^m = hg$. □

Als konkretes Beispiel betrachten wir nun Erzeugendensysteme der symmetrischen Gruppen S_n und der alternierenden Gruppen A_n. Für den Beweis benötigen wir den folgenden Begriff: Der ***Träger*** $\mathrm{supp}(\sigma)$ eines Elements $\sigma \in S_n$ ist die Menge aller $j \in M_n$ mit $\sigma(j) \neq j$. Wird σ als Produkt disjunkter Zykel dargestellt, so besteht der Träger aus genau denjenigen Elementen, die in einem der Zykel vorkommen.

Das Konzept des Trägers ist vor allem aus folgendem Grund wichtig: Seien $\sigma, \tau \in S_n$ mit $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$. Dann sind die Elemente σ und τ ***vertauschbar***, d.h. es gilt

$$\sigma \circ \tau \quad = \quad \tau \circ \sigma.$$

Zum Beweis bemerken wir vorweg: Für jedes $\sigma \in S_n$ und jedes $k \in M_n$ gilt $k \in \text{supp}(\sigma)$ genau dann, wenn auch $\sigma(k)$ in $\text{supp}(\sigma)$ liegt. Denn wäre $k \in \text{supp}(\sigma)$ und $\sigma(k) \notin \text{supp}(\sigma)$, dann würde $\sigma(k) = \sigma(\sigma(k))$ gelten, im Widerspruch zur Bijektivität von σ. Der Fall $k \notin \text{supp}(\sigma)$ und $\sigma(k) \in \text{supp}(\sigma)$ kann ebenfalls nicht eintreten, denn aus $k \notin \text{supp}(\sigma)$ folgt $\sigma(k) = k$.

Nun überprüfen wir, dass unter der Voraussetzung $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ die Abbildungen $\sigma \circ \tau$ und $\tau \circ \sigma$ auf jedem $k \in M_n$ übereinstimmen. Für $k \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$ gilt $(\sigma \circ \tau)(k) = k = (\tau \circ \sigma)(k)$. Betrachten wir nun den Fall $k \in \text{supp}(\sigma)$ und $k \notin \text{supp}(\tau)$. Dann gilt $(\sigma \circ \tau)(k) = \sigma(\tau(k)) = \sigma(k)$ und wegen $\sigma(k) \in \text{supp}(\sigma)$ und $\sigma(k) \notin \text{supp}(\tau)$ auch $(\tau \circ \sigma)(k) = \tau(\sigma(k)) = \sigma(k)$. Der Fall $k \notin \text{supp}(\sigma)$ und $k \in \text{supp}(\tau)$ läuft analog. Der Fall $k \in \text{supp}(\sigma)$ und $k \in \text{supp}(\tau)$ schließlich kann auf Grund der Voraussetzung nicht eintreten.

Satz 2.11 Sei $n \in \mathbb{N}$ beliebig.

(i) Die Menge der Transpositionen bildet ein Erzeugendensystem von S_n.

(ii) Die Menge der 3-Zykel bilden ein Erzeugendensystem von A_n.

Beweis: zu (i) Wir beweisen durch vollständige Induktion über $|\text{supp}(\sigma)|$, dass jedes $\sigma \in S_n$ als Produkt von Transpositionen dargestellt werden kann, wobei wir id wie immer als „leeres“ Produkt mit null Faktoren ansehen. Im Fall $|\text{supp}(\sigma)| = 0$ gilt $\text{supp}(\sigma) = \emptyset$ und $\sigma = \text{id}$, also ist hier nichts zu zeigen. Elemente $\sigma \in S_n$ mit $|\text{supp}(\sigma)| = 1$ existieren nicht, und die Elemente mit $|\text{supp}(\sigma)| = 2$ sind genau die Transpositionen.

Sei nun $k \in \{3, \ldots, n\}$ und $\sigma \in S_n$ mit $|\text{supp}(\sigma)| = k$, und setzen wir die Aussage für Werte $< k$ per Induktionsannahme voraus. Sei $i \in \text{supp}(\sigma)$ beliebig gewählt und $\tau = (i\ \sigma(i)) \circ \sigma$. Mit i auch $\sigma(i)$ in $\text{supp}(\sigma)$ enthalten. Damit ist klar, dass jedes $k \notin \text{supp}(\sigma)$ auch nicht in $\text{supp}(\tau)$ enthalten ist, also $\text{supp}(\tau) \subseteq \text{supp}(\sigma)$ gilt. Andererseits ist offenbar $\tau(i) = i$, also $i \in \text{supp}(\sigma) \setminus \text{supp}(\tau)$ und deshalb sogar $\text{supp}(\tau) \subsetneq \text{supp}(\sigma)$. Wir können damit die Induktionsvoraussetzung auf τ anwenden und erhalten eine Darstellung $\tau = \tau_1 \circ \ldots \circ \tau_r$ von τ als Produkt von Transpositionen τ_k. Folglich ist auch $\sigma = (i\ \sigma(i))^{-1} \circ \tau = (i\ \sigma(i))^{-1} \circ \tau_1 \circ \ldots \circ \tau_r$ als Produkt von Transpositionen darstellbar.

zu (ii) Sei $T \subseteq S_n$ die Menge der 3-Zyklen in S_n. Wir zeigen zunächst, dass jedes $\sigma \in A_n$ das Produkt von 3-Zyklen dargestellt werden kann und beweisen damit die Inklusion $A_n \subseteq \langle T \rangle$. Nach (i) besitzt σ eine Darstellung $\sigma = \tau_1 \circ \ldots \circ \tau_r$ als Produkt von Transpositionen, und wegen $\text{sgn}(\sigma) = 1$ und $\text{sgn}(\tau_k) = -1$ für $1 \leq k \leq r$ ist r gerade. Nun gilt allgemein für je zwei Transpositionen mit einem gemeinsamen Element im Träger die Gleichung $(i\ j) \circ (i\ k) = (i\ k\ j)$, wie man unmittelbar überprüft. Stimmen zwei Elemente im Träger überein, dann gilt offenbar $(i\ j) \circ (i\ j) = \text{id}$. Sind $(i\ j)$ und $(k\ \ell)$ schließlich disjunkte Zykel, dann gilt $(i\ j) \circ (k\ \ell) = (i\ k\ j) \circ (i\ k\ \ell)$. Somit kann jeder der Faktoren $\tau_1 \circ \tau_2$, $\tau_3 \circ \tau_4$, ..., $\tau_{r-1} \circ \tau_r$ als Produkt von 0 bis zwei 3-Zyklen dargestellt werden. Damit ist der Beweis von $A_n \subseteq \langle T \rangle$ abgeschlossen. Umgekehrt hat jeder 3-Zykel ein positives Signum, somit gilt $T \subseteq A_n$. Da $\langle T \rangle$ die kleinste Untergruppe ist, die T als Teilmenge enthält, folgt $\langle T \rangle \subseteq A_n$ und insgesamt $\langle T \rangle = A_n$. □

Wie wir gleich sehen werden, genügen sogar *zwei* Elemente, um die gesamte Gruppe S_n zu erzeugen; dieses Resultat wird auch später in der Galoistheorie benötigt. Hierfür benötigen wir den Begriff der ***Konjugation***. Sind g und h Elemente einer Gruppe G, dann bezeichnet man ghg^{-1} als das Element, dass durch Konjugation h mit g entsteht.

Proposition 2.12 Für jedes $n \in \mathbb{N}$ ist die Menge $\{\sigma, \tau\}$ bestehend aus den beiden Elementen $\sigma = (1\ 2\ \ldots\ n)$ und $\tau = (1\ 2)$ ein Erzeugendensystem von S_n. Ist n eine ungerade Primzahl, dann wird S_n sogar von *jeder* zweielementigen Menge bestehend aus einem n-Zykel und einer Transposition erzeugt.

Beweis: Für das Verständnis dieses Beweises ist es hilfreich, sich vorher die Auswirkung der Konjugation eines Elements von S_n mit einem anderen Element klar zu machen. (Wir gehen im Kapitel über die Klassengleichung detailliert darauf ein.) Beispielsweise entsteht durch Konjugation von τ mit σ das Element

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

Ebenso erhält man durch Konjugation von τ mit σ^2, σ^3, ... die Transpositionen (3 4), (4 5), ... und durch Konjugation von τ mit σ^{n-2} schließlich die Transposition $(n-1\ n)$. Sei nun $i \in \{1, ..., n-1\}$ vorgegeben. Dann gilt

$$(i+1\ \ i+2)\circ(i\ \ i+1)\circ(i+1\ \ i+2) = (i\ \ i+2)\,, \quad (i+2\ i+3)\circ(i\ \ i+2)\circ(i+2\ i+3) = (i\ \ i+3) \quad \text{usw.}$$

Insgesamt kann auf diese Weise jedes Element $(i\ \ i+k)$ mit $i+k \leq n$ gebildet werden. Dies zeigt, dass $\langle\sigma, \tau\rangle$ die gesamte Menge $T \subseteq S_n$ aller Transpositionen enthält. Es folgt $\langle\sigma, \tau\rangle = \langle T\rangle$, und wegen $\langle T\rangle = S_n$ nach Satz 2.11 ist damit die erste Aussage bewiesen.

Der Beweis der zweiten Aussage ist recht umfangreich; darüber hinaus müssen wir im hinteren Teil auf ein wenig Zahlentheorie und Kongruenzrechnung zurückgreifen, die wir erst später in der Vorlesung entwickeln. Sei $p = n$ eine ungerade Primzahl, $\sigma = (i_1\ i_2\ \ldots\ i_p)$ ein p-Zykel und τ eine beliebige Transposition. Definieren wir $\rho \in S_p$ durch

$$\rho \quad = \quad \begin{pmatrix} 1 & 2 & \cdots & p \\ i_1 & i_2 & \ldots & i_p \end{pmatrix}^{-1} \quad ,$$

dann ist das Element $\tilde{\sigma} = \rho\sigma\rho^{-1}$ gegeben durch $\tilde{\sigma} = (\rho(i_1) \ldots \rho(i_p)) = (1\ 2\ \ldots\ p)$. Sei außerdem $\tilde{\tau} = \rho\tau\rho^{-1}$. Wie man leicht überprüft, ist durch die Konjugationsabbildung $\phi_\rho(\alpha) = \rho\alpha\rho^{-1}$ ein Automorphismus von S_p definiert. Es gilt $\phi_\rho(\langle\sigma, \tau\rangle) = \langle\phi_\rho(\sigma), \phi_\rho(\tau)\rangle = \langle\tilde{\sigma}, \tilde{\tau}\rangle$, denn einerseits ist $\{\tilde{\sigma}, \tilde{\tau}\}$ eine Teilmenge von $\phi_\rho(\langle\sigma, \tau\rangle)$, und andererseits gilt $\{\sigma, \tau\} \subseteq \phi_\rho^{-1}(\langle\tilde{\sigma}, \tilde{\tau}\rangle)$, woraus $\langle\sigma, \tau\rangle \subseteq \phi_\rho^{-1}(\langle\tilde{\sigma}, \tilde{\tau}\rangle)$ und $\phi_\rho(\langle\sigma, \tau\rangle) = \langle\tilde{\sigma}, \tilde{\tau}\rangle$ folgt. Wenn wir nun zeigen können, dass $\langle\tilde{\sigma}, \tilde{\tau}\rangle = S_p$ gilt, dann folgt daraus $\langle\sigma, \tau\rangle = \phi_\rho^{-1}(S_p) = \phi_{\rho^{-1}}(S_p) = S_p$. Aus diesem Grund dürfen wir im nachfolgenden Teil des Beweises σ, τ durch $\tilde{\sigma}, \tilde{\tau}$ ersetzen und annehmen, dass $\sigma = (1\ 2\ \ldots\ p)$ gilt.

Sei $\tau = (i\ j)$ mit $i, j \in M_p$ und $i < j$. Dann ist auch das Element $\sigma^{1-i}\tau\sigma^{i-1} = (1\ j-i+1)$ in $\langle\sigma, \tau\rangle$ enthalten. Nach Ersetzung von τ durch dieses Element können wir annehmen, dass τ die Form $(1\ i)$ mit $1 < i \leq p$ hat. Wir zeigen nun: Sind $k, r \in \mathbb{N}$ mit $1 \leq k \leq p-1$ und $r \in M_p$, und gilt $r \equiv 1 + k(i-1) \bmod p$, dann liegt das Element $(1\ r)$ in $\langle\sigma, \tau\rangle$. Wir beweisen die Aussage durch vollständige Induktion über k; die Zahl r ist durch k jeweils eindeutig festgelegt. Für $k = 1$ ist $r = i$, und dass $(1\ i)$ in $\langle\sigma, \tau\rangle$ liegt, ist bereits bekannt. Setzen wir nun die Aussage für ein $k \in \mathbb{N}$ mit $1 \leq k < p-1$ voraus, und seien $r, s \in M_p$ die eindeutig bestimmten Elemente mit $r \equiv 1 + k(i-1) \bmod p$ und $s \equiv 1 + (k+1)(i-1) \bmod p$. Ist $r + (i-1) < p$, dann gilt $s = r + (i-1)$ und somit $\sigma^{r-1}(1\ i)\sigma^{1-r} = (r\ s)$. Im Fall $r + (i-1) > p$ gilt $s = r + (i-1) - p$ und $\sigma^{r-1-p}(1\ i)\sigma^{1+p-r} = (r\ s)$. In beiden Fällen zeigt die Gleichung $(r\ s)(1\ r)(r\ s) = (1\ s)$, dass auch $(1\ s)$ in $\langle\sigma, \tau\rangle$ enthalten ist.

Wegen $\mathrm{ggT}(i-1, p) = 1$ existieren nun nach dem Lemma von Bézout $k, \ell \in \mathbb{Z}$ mit $k(i-1) + \ell p = 1$. Dabei ist p kein Teiler von k, da aus der Gleichung ansonsten $p \mid 1$ folgen würde. Sei $x \in \mathbb{Z}$ so gewählt, dass $1 \leq k + px \leq p-1$ gilt. Dann folgt $(k+px)(i-1) + (\ell - x(i-1))p = 1$; nach Ersetzung von k durch $k+px$ und ℓ durch $\ell - x(i-1)$ können

wir also $1 \leq k \leq p-1$ voraussetzen. Wenden wir nun die im vorherigen Abschnitt bewiesene Aussage auf dieses k an und setzen wir $r = 2$, dann gilt $r \in M_p$, $r = 1+1 = 1+k(i-1)+\ell p \equiv 1+k(i-1) \bmod p$ und $(1\ r) = (1\ 2) \in \langle \sigma, \tau \rangle$. Wegen $\sigma = (1\ 2\ \ldots\ p) \in \langle \sigma, \tau \rangle$ enthält $\langle \sigma, \tau \rangle$ auf Grund der ersten Aussage der Proposition also ein vollständiges Erzeugendensystem von S_p. □

Wenden wir uns nun dem zweiten Thema dieses Kapitels zu, dem Satz von Lagrange.

Definition 2.13 Sei $(G, \cdot)$ eine Gruppe und U eine Untergruppe. Eine Teilmenge von G, die mit einem geeigneten $g \in G$ in der Form

$$gU \quad = \quad \{gu \mid u \in U\}$$

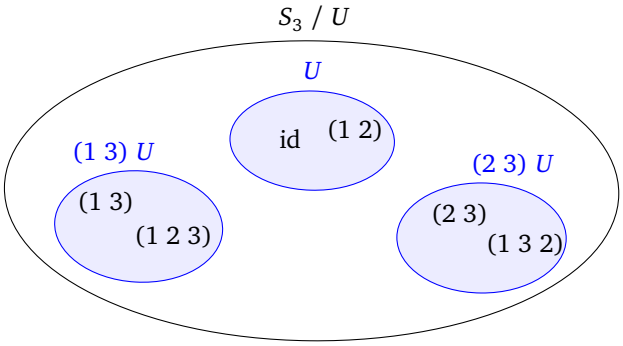
geschrieben werden kann, wird ***Linksnebenklasse*** von U genannt. Ebenso bezeichnet man die Teilmengen der Form $Ug = \{ug \mid u \in U\}$ mit $g \in G$ als ***Rechtsnebenklassen*** von U.

Desweiteren führen wir die Bezeichnung G/U für die Menge der Linksnebenklassen und $U\backslash G$ für die Menge der Rechtsnebenklassen von U ein. Es gilt also $G/U = \{gU \mid g \in G\}$ und $U\backslash G = \{Ug \mid g \in G\}$. Sei beispielsweise $G = S_3$ und $U = \langle (1,2) \rangle = \{\mathrm{id}, (1\ 2)\}$. Dann sind die Linksnebenklassen von U gegeben durch

$$\begin{array}{rcll}
\mathrm{id} \circ U & = & \{\mathrm{id} \circ \mathrm{id}, \mathrm{id} \circ (1\ 2)\} & = & \{\mathrm{id}, (1\ 2)\} \\
(1\ 2) \circ U & = & \{(1\ 2) \circ \mathrm{id}, (1\ 2) \circ (1\ 2)\} & = & \{(1\ 2), \mathrm{id}\} \\
(1\ 3) \circ U & = & \{(1\ 3) \circ \mathrm{id}, (1\ 3) \circ (1\ 2)\} & = & \{(1\ 3), (1\ 2\ 3)\} \\
(2\ 3) \circ U & = & \{(2\ 3) \circ \mathrm{id}, (2\ 3) \circ (1\ 2)\} & = & \{(2\ 3), (1\ 3\ 2)\} \\
(1\ 2\ 3) \circ U & = & \{(1\ 2\ 3) \circ \mathrm{id}, (1\ 2\ 3) \circ (1\ 2)\} & = & \{(1\ 2\ 3), (1\ 3)\} \\
(1\ 3\ 2) \circ U & = & \{(1\ 3\ 2) \circ \mathrm{id}, (1\ 3\ 2) \circ (1\ 2)\} & = & \{(1\ 3\ 2), (2\ 3)\}
\end{array}$$

Es gilt also $S_3/U = \{\ \{\mathrm{id}, (1\ 2)\}\ ,\ \{(1\ 3), (1\ 2\ 3)\}\ ,\ \{(2\ 3), (1\ 3\ 2)\}\ \}$.

Graphisch kann die Menge S_3/U der Linksnebenklassen folgendermaßen dargestellt werden.



Die Elemente von S_3/U sind die Linksnebenklassen U, $(1\ 2)U$ und $(2\ 3)U$, also die blau gezeichneten Objekte. Die Permutation $(1\ 2\ 3)$ ist ein Element von S_3 und auch ein Element der Linksnebenklasse $(1\ 3)U$, die ja ihrerseits eine Teilmenge von S_3 ist. Aber $(1\ 2\ 3)$ ist *kein* Element von S_3/U, denn die Elemente von S_3/U sind nach Definition bestimmte *Teilmengen* von S_3, keine *Elemente* von S_3!

Offenbar ist es möglich, dass zwei Nebenklassen gU und hU übereinstimmen, ohne dass $g = h$ ist. In unserem Beispiel gilt etwa $(1\ 3) \circ U = (1\ 2\ 3) \circ U$. Nach dem gleichen Schema können wir auch die Rechtsnebenklassen von U bestimmen.

$$\begin{array}{lcll} U \circ \mathrm{id} & = & \{\mathrm{id} \circ \mathrm{id}, (1\ 2) \circ \mathrm{id}\} & = & \{\mathrm{id}, (1\ 2)\} \\ U \circ (1\ 2) & = & \{\mathrm{id} \circ (1\ 2), (1\ 2) \circ (1\ 2)\} & = & \{(1\ 2), \mathrm{id}\} \\ U \circ (1\ 3) & = & \{\mathrm{id} \circ (1\ 3), (1\ 2) \circ (1\ 3)\} & = & \{(1\ 3), (1\ 3\ 2)\} \\ U \circ (2\ 3) & = & \{\mathrm{id} \circ (2\ 3), (1\ 2) \circ (2\ 3)\} & = & \{(2\ 3), (1\ 2\ 3)\} \\ U \circ (1\ 2\ 3) & = & \{\mathrm{id} \circ (1\ 2\ 3), (1\ 2) \circ (1\ 2\ 3)\} & = & \{(1\ 2\ 3), (2\ 3)\} \\ U \circ (1\ 3\ 2) & = & \{\mathrm{id} \circ (1\ 3\ 2), (1\ 2) \circ (1\ 3\ 2)\} & = & \{(1\ 3\ 2), (1\ 3)\} \end{array}$$

Die Menge der Rechtsnebenklassen $U\backslash G$ ist also gegeben durch $\{U\ ,\ \{(1\ 3), (1\ 3\ 2)\}\ ,\ \{(2\ 3), (1\ 2\ 3)\}\}$.

Das Beispiel zeigt, dass Links- und Rechtsnebenklassen im Allgemeinen nicht übereinzustimmen brauchen. Beispielsweise ist $\{(1\ 3), (1\ 2\ 3)\}$ zwar eine Links- aber keine Rechtsnebenklasse von U. Ist U aber Untergruppe einer *abelschen* Gruppe, dann gilt $gU = Ug$ für alle $g \in G$. Ist nämlich $h \in gU$ vorgegeben, dann gilt $h = gu = ug$ für ein $u \in U$, und es folgt $h \in Ug$. Damit ist $gU \subseteq Ug$ nachgewiesen, und die umgekehrte Inklusion beweist man genauso.

Wir bemerken noch, dass jedes $g \in G$ sowohl in der Linksnebenklasse gU als auch in der Rechtsnebenklasse Ug enthalten ist. Dies folgt direkt aus den Gleichungen $g = g \cdot e_G = e_G \cdot g$ und der Tatsache, dass e_G in U liegt.

Bei unserem Beispiel fällt auf, dass jede Links- oder Rechtsnebenklasse genauso viele Elemente enthält wie die Untergruppe U selbst. Diese Beobachtung ist auch im allgemeinen Fall zutreffend.

Lemma 2.14 Sei G eine Gruppe, U eine Untergruppe von G und $g \in G$ ein beliebiges Element. Dann sind die Abbildungen

$$\tau_g^\ell : U \to gU\ ,\ h \mapsto gh \qquad \text{und} \qquad \tau_g^r : U \to Ug\ ,\ h \mapsto hg \qquad \text{jeweils bijektiv.}$$

Ist U endlich, dann gilt also $|U| = |gU| = |Ug|$ für alle $g \in G$.

Beweis: Wir beschränken und auf den Beweis der Surjektivität und der Injektivität der Abbildung τ_g^ℓ. Sei $h \in gU$ vorgegeben. Dann existiert nach Definition von gU ein $u \in U$ mit $h = gu$. Es gilt also $\tau_g^\ell(u) = gu = h$. Damit ist die Surjektivität bewiesen. Seien nun $u_1, u_2 \in U$ mit $\tau_g^\ell(u_1) = \tau_g^\ell(u_2)$. Dann folgt $u_1 = g^{-1}gu_1 = g^{-1}\tau_g^\ell(u_1) = g^{-1}\tau_g^\ell(u_2) = g^{-1}gu_2 = u_2$. Dies zeigt, dass τ^ℓ auch injektiv ist. Die letzte Aussage folgt unmittelbar aus der Tatsache, dass zwei Mengen, zwischen denen eine Bijektion existiert, gleichmächtig sind. □

Für das Hauptziel dieses Abschnitts, den Beweis des Satzes von Lagrange, ist die Beobachtung entscheidend, dass die Linksnebenklassen in G/U eine Zerlegung der Menge G bilden, ein Begriff, den wir bereits aus der Linearen Algebra kennen. Zur Erinnerung: Unter einer Zerlegung einer Menge X verstehen wir ein System $\mathcal{Z} \subseteq \mathcal{P}(X)$ von Teilmengen von X mit den Eigenschaften $\emptyset \notin \mathcal{Z}$, $\bigcup_{A \in \mathcal{Z}} A = X$ und $\forall A, B \in \mathcal{Z} : A \neq B \Rightarrow A \cap B = \emptyset$; zwei verschiedene Mengen in einer Zerlegung sind also disjunkt. Man vergewissere sich anhand des Beispiels vom Anfang des Kapitels mit $G = S_3$ und $U = \langle (1\ 2) \rangle$, dass sowohl G/U als auch $U\backslash G$ in der Tat eine Zerlegung von S_3 liefert.

Aus der Linearen Algebra wissen wir auch, dass der Begriff der Zerlegung mit dem Konzept der Äquivalenzrelation eng verbunden ist. Eine Äquivalenzrelation $\equiv$ auf einer Menge X ist eine reflexive, symmetrische und transitive Relation. Für jedes $x \in X$ wird $[x] = \{y \in X \mid x \equiv y\}$ die Äquivalenzklasse von x bezüglich $\equiv$ genannt. Zwischen den Äquivalenzrelationen auf einer Menge X und den Zerlegungen von X besteht nun der folgende Zusammenhang: Ist

$\equiv$ eine Äquivalenzrelation auf X, so bilden die Äquivalenzklassen bezüglich $\equiv$ eine Zerlegung von X. Ist umgekehrt $\mathcal{Z}$ eine Zerlegung von X, so erhält man durch

$$x \equiv_{\mathcal{Z}} y \quad \Leftrightarrow \quad \exists A \in \mathcal{Z} : x, y \in A$$

eine Äquivalenzrelation auf X. Für eine Menge X und eine Zerlegung $\mathcal{Z}$ von X gilt offenbar allgemein: Genau dann ist X endlich, wenn sowohl $|\mathcal{Z}|$ als auch $|A|$ für jedes $A \in \mathcal{Z}$ endlich ist, und in diesem Fall ist dann die Gleichung $|X| = \sum_{A \in \mathcal{Z}} |A|$ erfüllt. Diese einfache Beobachtung wird später beim Beweis des Satzes von Lagrange eine wichtige Rolle spielen.

Lemma 2.15 Sei G eine Gruppe und U eine Untergruppe von G. Dann folgt für alle $g, h \in G$ aus $h \in gU$ jeweils $gU = hU$.

Beweis: Setzen wir $h \in gU$ voraus. Dann gibt es ein $u \in U$ mit $h = gu$. Zum Nachweis der Inklusion „$\subseteq$“ sei $h_1 \in gU$ vorgegeben. Dann gibt es ein $u_1 \in U$ mit $h_1 = gu_1$, und es folgt $h_1 = h(u^{-1}u_1) \in hU$. Ist umgekehrt $h_1 \in hU$, dann gilt $h_1 = hu_2$ für ein $u_2 \in U$. Wir erhalten $h_1 = g(u_1u_2) \in gU$. □

Satz 2.16 Sei G eine Gruppe und $U \leq G$. Dann ist sowohl durch G/U als auch durch $U\backslash G$ eine Zerlegung von G gegeben. Die zugehörigen Äquivalenzrelationen auf G sind definiert durch $g \equiv_\ell h \Leftrightarrow h \in gU$ bzw. $g \equiv_r h \Leftrightarrow h \in Ug$.

Beweis: Wir beweisen die beiden Teilaussagen lediglich für die Menge G/U der Linksnebenklassen. Zunächst zeigen wir, dass es sich dabei um eine Zerlegung von G handelt, und überprüfen dafür die drei definierenden Bedingungen, die wir gerade wiederholt haben. Jede Teilmenge $A \in G/U$ hat die Form $A = gU$ für ein $g \in G$, und es gilt $g = g \cdot e_G \in gU$ wegen $e_G \in U$. Dies zeigt, dass $A \neq \emptyset$ gilt, die leere Menge in G/U also nicht vorkommt. Weil jedes $g \in G$ in gU liegt, also einem Element von G/U, ist auch die Eigenschaft $G = \bigcup_{A \in G/U} A$ erfüllt. Seien nun $A, B \in G/U$ mit $A \cap B \neq \emptyset$ vorgegeben, und sei $h \in A \cap B$. Nach Lemma 2.15 folgt daraus $A = hU = B$. Setzen wir für $A, B \in G/U$ umgekehrt $A \neq B$ voraus, dann muss also $A \cap B = \emptyset$ gelten.

Nach Definition ist die zur Zerlegung G/U gehörende Äquivalenzrelation $\equiv_\ell$ definiert durch die Bedingung, dass für je zwei Elemente $g, h \in G$ jeweils genau dann $g \equiv_\ell h$ erfüllt ist, wenn ein $A \in G/U$ mit $g, h \in A$ existiert. Aber wegen Lemma 2.15 folgt aus $g \in A$ bereits $A = gU$, so dass $g \equiv_\ell h$ also $h \in gU$ impliziert. Setzen wir umgekehrt $h \in gU$ voraus, dann ist durch $A = gU$ ein Element von G/U mit $g, h \in A$ gegeben, und es folgt $g \equiv_\ell h$. □

Im weiteren Verlauf bezeichnen wir mit $X/\equiv$ die Menge der Äquivalenzklassen einer Äquivalenzrelation $\equiv$. Es handelt sich also nach Definition um die Menge $\{[x] \mid x \in X\}$.

Definition 2.17 Sei X eine Menge und $\equiv$ eine Äquivalenzrelation auf X. Eine Teilmenge $R \subseteq X$ wird ***Repräsentantensystem*** der Äquivalenzklassen von $\equiv$ genannt, wenn durch $R \to X/\equiv$, $x \mapsto [x]$ eine bijektive Abbildung gegeben ist. Mit anderen Worten, in jeder Äquivalenzklasse ist genau ein Element aus R enthalten.

Im Beispiel $G = S_3$, $U = \langle(1\ 2)\rangle$ von oben ist $\{\mathrm{id}, (1\ 3), (2\ 3)\}$ ein Repräsentantensystem von G/U. Gleiches gilt für die Mengen $\{\mathrm{id}, (1\ 2\ 3), (2\ 3)\}$ und $\{(1\ 2), (1\ 3), (1\ 3\ 2)\}$. Die Wahl eines Repräsentantensystems ist also keineswegs eindeutig.

Als nächstes zeigen wir, wie sich aus einem Repräsentantensystem der Linksnebenklassen ein Repräsentantensystem der Rechtsnebenklassen gewinnen lässt.

Proposition 2.18 Sei G eine Gruppe und U eine Untergruppe. Ist R ein Repräsentantesystem der Linksnebenklassen, dann ist $R' = \{g^{-1} \mid g \in R\}$ ein Repräsentantensystem der Rechtsnebenklassen, und durch $g \mapsto g^{-1}$ ist eine Bijektion zwischen R und R' definiert.

Beweis: Zu zeigen ist, dass für jedes $h \in G$ die Rechtsnebenklasse Uh genau ein Element aus R' enthält. Sei also $h \in G$ vorgegeben. Zunächst beweisen wir, dass in Uh ein Element aus R' liegt. Nach Voraussetzung enthält die Linksnebenklasse $h^{-1}U$ ein Element $g \in R$. Es gibt also ein $u \in U$ mit $g = h^{-1}u$. Daraus folgt $g^{-1} = u^{-1}h$. Diese Gleichung wiederum zeigt, dass die Rechtsnebenklasse Uh das Element $g^{-1} \in R'$ enthält.

Nehmen wir nun an, die Rechtsnebenklasse Uh enthält die beiden Elemente $h_1, h_2 \in R'$. Dann gibt es $u, v \in U$ mit $h_1 = uh$ und $h_2 = vh$. Nach Definition von R' gibt es außerdem $g_1, g_2 \in R$ mit $g_1^{-1} = h_1$, $g_2^{-1} = h_2$. Es folgt $g_1 = h_1^{-1} = h^{-1}u^{-1}$ und $g_2 = h_2^{-1} = h^{-1}v^{-1}$. Die Gleichungen zeigen, dass die Elemente $g_1, g_2 \in R$ beide in der Linksnebenklasse $h^{-1}U$ liegen. Weil R ein Repräsentantensystem der Linksnebenklassen ist, muss $g_1 = g_2$ gelten. Daraus wiederum folgt $h_1 = h_2$.

Dass die Abbildung $R \to R'$, $g \mapsto g^{-1}$ surjektiv ist, folgt direkt aus der Definition von R'. Andererseits folgt aus $g^{-1} = h^{-1}$ sofort $g = h$, somit ist die Abbildung auch injektiv. □

Aus der Proposition folgt unmittelbar, dass zwischen G/U und $U\backslash G$ eine Bijektion existiert, die aus den Bijektionen $G/U \to R \to R' \to U\backslash G$ zusammengesetzt ist. Dies bedeutet, dass die Mengen G/U und $U\backslash G$ gleichmächtig sind.

Definition 2.19 Sei G eine Gruppe und U eine Untergruppe. Die Mächtigkeit $|G/U|$ der Menge G/U wird der ***Index*** von U in G genannt und mit $(G : U)$ bezeichnet.

Aus unserer Vorüberlegung folgt, dass man zur Definition des Index genauso gut die Mächtigkeit der Menge $U\backslash G$ der Rechtsnebenklassen verwenden könnte. Im Beispiel oben haben wir gesehen, dass es im Fall $G = S_3$ und $U = \langle(1\ 2)\rangle$ jeweils drei Links- und drei Rechtsnebenklassen gibt. Hier gilt also $(G : U) = 3$.

Satz 2.20 *(Satz von Lagrange)*

Sei G eine endliche Gruppe und U eine Untergruppe. Dann gilt $|G| = (G : U)|U|$. Insbesondere ist die Ordnung $|U|$ der Untergruppe immer ein Teiler der Gruppenordnung $|G|$.

Beweis: Sei $R \subseteq G$ ein Repräsentantensystem der Linksnebenklassen. Weil nach Definition der Repräsentantensysteme eine Bijektion $R \to G/U$ existiert, gilt $|R| = |G/U| = (G : U)$. Nach Proposition 2.16 ist G/U eine Zerlegung von G,

und nach Lemma 2.14 gilt $|gU| = |U|$ für alle Linksnebenklassen. Wir erhalten

$$|G| \quad = \quad \sum_{A \in G/U} |A| \quad = \quad \sum_{g \in R} |gU| \quad = \quad \sum_{g \in R} |U| \quad = \quad |R| \cdot |U| \quad = \quad (G : U)|U|. \qquad \square$$

Im Beispiel oben ist die Gleichung aus dem Satz von Lagrange offenbar erfüllt, denn im Fall $G = S_3$, $U = \langle (1\ 2) \rangle$ gilt $|G| = 6$ und $(G : U)|U| = 3 \cdot 2 = 6$. Die Untergruppe $V = \langle (1\ 2\ 3) \rangle$ in S_3 ist von Ordnung 3, da $(1\ 2\ 3)$ ein Element der Ordnung 3 ist. Der Satz von Langrange liefert hier für den Index den Wert

$$(G : V) \quad = \quad \frac{|G|}{|V|} \quad = \quad \frac{6}{3} \quad = \quad 2.$$

Die Zerlegung einer Gruppe in ihre Linksnebenklassen liefert auch eine Aussage für beliebige, nicht notwendigerweise endliche, Gruppen.

Folgerung 2.21 Sei G eine Gruppe und U eine Untergruppe. Genau dann ist G endlich, wenn sowohl U als auch G/U endliche Mengen sind (und in diesem Fall gilt dann natürlich der Satz von Lagrange).

Beweis: „⇒“ Ist G endlich, dann ist U als Teilmenge von G offenbar ebenfalls endlich. Sei $R \subseteq G$ ein Repräsentantensystem der Menge G/U der Linksnebenklassen. Dann gibt es eine Bijektion von R nach G/U. Weil R als Teilmenge von G endlich ist, handelt es sich auch bei G/U um eine endliche Menge.

„⇐“ Setzen wir nun voraus, dass U und G/U endlich sind. Weil für jedes $g \in G$ zwischen U und gU jeweils eine Bijektion existiert, ist damit auch jede Linksnebenklasse endlich. Weil es nach Voraussetzung nur endlich viele Linksnebenklassen gibt, ist G als Vereinigung der endlich vielen Linksnebenklassen selbst eine endliche Menge. $\square$

Wir haben beim Beweis der bisherigen Sätze mehrmals verwendet, dass für die Linksnebenklassen einer Untergruppe U in einer Gruppe G stets ein Repräsentantensystem existiert. Dass dies tatsächlich der Fall ist, wird durch das sogenannte ***Auswahlaxiom*** der Mengenlehre gewährleistet. Dieses stellt sicher, dass aus jeder Linksnebenklasse ein Repräsentant ausgewählt und die ausgewählten Elemente zu einer neuen Menge R zusammengeführt werden können. Da in den Vorlesungen die Axiome der Mengenlehre normalerweise nicht behandelt werden, fällt die Verwendung des Auswahlaxioms nicht auf, zumal seine Gültigkeit selbstverständlich und trivial erscheint.

Wir notieren noch zwei Folgerungen aus dem Satz von Lagrange.

Satz 2.22

(i) Jede Gruppe von Primzahlordnung ist zyklisch.

(ii) Sei G eine Gruppe, und seien $U, V \subseteq G$ endliche Untergruppen teilerfremder Ordnung. Dann gilt $U \cap V = \{e_G\}$.

Beweis: zu (i) Wegen $|G| > 1$ gibt es mindestens ein Element $g \in G \setminus \{e_G\}$. Nach dem Satz von Lagrange ist $\mathrm{ord}(g) = |\langle g \rangle|$ ein Teiler der Gruppenordnung p. Weil p eine Primzahl ist, gibt es nur die beiden Möglichkeiten $\mathrm{ord}(g) = 1$ oder $\mathrm{ord}(g) = p$. Wegen $g \neq e_G$ scheidet die erste Möglichkeit aus. Es gilt damit $|\langle g \rangle| = p = |G|$, also $G = \langle g \rangle$.

zu (ii) Sei $U_1 = U \cap V$. Dann ist U_1 eine Untergruppe von U, und nach dem Satz von Lagrange ist $|U_1|$ ein Teiler von $|U|$. Ebenso ist U_1 eine Untergruppe von V, also teilt $|U_1|$ auch $|V|$. Die Zahl $|U_1|$ ist also ein gemeinsamer Teiler von $|U|$ und $|V|$. Weil $|U|$ un d $|V|$ teilerfremd sind, folgt $|U_1| = 1$ und $U_1 = \{e_G\}$. □

§ 3. *Elementordnungen und die Struktur zyklischer Gruppen*

Zusammenfassung. Die *Ordnung* $\operatorname{ord}(g)$ eines Gruppenelements ist die kleinste natürliche Zahl m mit $g^m = e_G$; existiert eine solche Zahl nicht, dann setzt man $\operatorname{ord}(g) = \infty$. Die Ordnung kann auf zwei weitere Arten charakterisiert werden. Kennt man $\operatorname{ord}(g)$, so kann $\operatorname{ord}(g^a)$ für jedes $a \in \mathbb{Z}$ berechnet werden. Im weiteren Verlauf des Kapitels untersuchen wir die Untergruppenstruktur zyklischer Gruppen. Eine Besonderheit dieser Gruppen besteht darin, dass die Anzahl der Untergruppen mit der Anzahl der Teiler ihrer Ordnung übereinstimmt.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Ordnung einer Gruppe	– äquivalente Charakterisierung der Elementordnung
– Ordnung eines Gruppenelements	– Rechenregeln für die Elementordnung
– Eulersche φ-Funktion	– Beschreibung der Untergruppen zyklischer Gruppen
	– Charakterisierung zyklischer Gruppen
	– Kleiner Satz von Fermat

Wir beginnen mit der Definition der Gruppen- und Elementordnung.

Definition 3.1 Sei G eine Gruppe. Die Anzahl $|G|$ der Elemente von G wird die ***Ordnung*** von G genannt. Ist $g \in G$ ein beliebiges Element, dann bezeichnen wir $\operatorname{ord}(g) = |\langle g \rangle|$ als die Ordnung von g.

Da $\langle g \rangle$ für jedes $g \in G$ jeweils eine Untergruppe von G ist, folgt aus dem Satz von Lagrange unmittelbar: Ist $n = |G|$ endlich, dann folgt

$$\operatorname{ord}(g) \mid n \quad \text{für alle } g \in G.$$

In § 2 wurde gezeigt, dass die Elemente einer zyklischen Gruppe $\langle g \rangle$ genau die ganzahligen Potenzen von a sind, also die Elemente der Form g^a mit $a \in \mathbb{Z}$. Es kann allerdings vorkommen, dass $g^a = g^b$ gilt, obwohl $a \neq b$ ist.

Lemma 3.2 Sei G eine Gruppe, $g \in G$ und $m \in \mathbb{N}$ mit $g^m = e_G$. Dann ist die von g erzeugte Untergruppe gegeben durch $\langle g \rangle = \{g^r \mid 0 \leq r < m\}$.

Beweis: Die Inklusion „$\supseteq$“ ergibt sich direkt aus Folgerung 2.10. Zum Nachweis von „$\subseteq$“ sei $h \in \langle g \rangle$ vorgegeben. Wiederum auf Grund der Proposition gibt es ein $n \in \mathbb{Z}$ mit $h = g^n$. Dividieren wir n durch m mit Rest, so erhalten wir ein $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 \leq r < m$. Es gilt $h = g^n = g^{qm+r} = (g^m)^q \cdot g^r = e_G^q \cdot g^r = g^r$. Also ist h in der Menge auf der rechten Seite enthalten. □

Satz 3.3 Sei G eine Gruppe und $g \in G$ ein beliebiges Element. Dann sind für jedes $n \in \mathbb{N}$ die folgenden Aussagen äquivalent.

(i) $n = \text{ord}(g)$

(ii) Es gibt ein $m \in \mathbb{N}$ mit $g^m = e_G$, und darüber hinaus ist n die ***minimale*** natürliche Zahl mit dieser Eigenschaft.

(iii) Für alle $m \in \mathbb{Z}$ gilt $g^m = e_G$ genau dann, wenn m ein Vielfaches von n ist.

Beweis: „(i) ⇒ (ii)“ Da $\text{ord}(g)$ und damit die Menge $\langle g \rangle$ nach Voraussetzung endlich ist, können die Elemente $g, g^2, g^3, \ldots$ nicht alle voneinander verschieden sein. Es gibt also $i, j \in \mathbb{N}$ mit $i < j$ und $g^i = g^j$. Setzen wir $m = j - i$, dann gilt $g^m = g^{j-i} = g^j \cdot (g^i)^{-1} = e_G$, also existiert ein $m \in \mathbb{N}$ mit $g^m = e_G$.

Weil die zyklische Gruppe $\langle g \rangle$ insgesamt nur n verschiedene Elemente besitzt, können bereits die Elemente g, g^2, ..., g^{n+1} nicht alle verschieden sein. Wir können also für das j von oben $j \leq n+1$ und damit $m \leq n$ voraussetzen. Wäre $m < n$, dann würde $\langle g \rangle$ auf Grund des Lemmas aus der höchstens m-elementigen Menge $\{e_G, g, \ldots, g^{m-1}\}$ bestehen, im Widerspruch zu $|\langle g \rangle| = n$. Es gilt also $m = n$, und n ist die minimale natürliche Zahl mit der Eigenschaft $g^n = e_G$.

„(ii) ⇒ (iii)“ Sei $m \in \mathbb{Z}$ mit $g^m = e_G$ vorgegeben. Dann gibt es $q, r \in \mathbb{Z}$ mit $m = qn + r$ und $0 \leq r < n$. Es gilt $g^r = g^{m-qn} = g^m \cdot (g^n)^{-q} = e_G \circ e_G = e_G$. Da n nach Voraussetzung die *minimale* natürliche Zahl mit $g^n = e_G$ ist, muss $r = 0$ gelten, und m ist somit ein Vielfaches von n. Setzen wir umgekehrt voraus, dass m ein Vielfaches von n ist, $m = kn$ für ein $k \in \mathbb{Z}$, dann gilt $g^m = g^{kn} = (g^n)^k = e_G^k = e_G$.

„(iii) ⇒ (i)“ Nach Voraussetzung gilt $g^n = e_G$, und auf Grund des Lemmas ist $\langle g \rangle = \{e_G, g, \ldots, g^{n-1}\}$. Würden zwei Elemente in dieser Menge übereinstimmen, dann gäbe es $i, j \in \mathbb{Z}$ mit $0 \leq i < j \leq n-1$ und $g^i = g^j$, es wäre also $g^{j-i} = e_G$. Dies aber wäre ein Widerspruch zur Voraussetzung, da n wegen $0 < j - i < n$ kein Teiler von $j - i$ ist. Dies zeigt, dass $\langle n \rangle$ tatsächlich aus genau n verschiedenen Elementen besteht, also $\text{ord}(g) = |\langle g \rangle| = n$ gilt. □

Wir geben einige Beispiele für Elementordnungen an.

(i) Ist $n \in \mathbb{N}$ und $G = (\mathbb{Z}/n\mathbb{Z}, +)$, dann ist $\bar{1} = 1 + n\mathbb{Z}$ ein Element der Ordnung n, denn es gilt $k \cdot \bar{1} = \bar{k} \neq \bar{0}$ für $1 \leq k < n$ und $n \cdot \bar{1} = n + n\mathbb{Z} = 0 + n\mathbb{Z} = \bar{0}$.

(ii) In § 1 (auf Seite 9) haben wir für jedes $\alpha \in \mathbb{R}$ das Element R_α der orthogonalen Gruppe $\mathcal{O}(2)$ definiert. Es handelte sich dabei um die Matrix, die eine Drehung um den Ursprung $0_{\mathbb{R}^2}$ mit dem Winkel α im Bogenmaß beschreibt. Wie man leicht überprüft, ist $R_{2\pi/n}$ für jedes $n \in \mathbb{N}$ ein Element der Ordnung n in $\mathcal{O}(2)$.

(iii) In den Diedergruppen D_n (mit $n \geq 3$) sind die n Spiegelungen alles Elemente der Ordnung 2.

Mit Hilfe von Satz 3.3 können wir die Elemente einer endlichen, zyklischen Gruppe nun genau angeben.

Folgerung 3.4 Sei G eine Gruppe. Besitzt $g \in G$ die endliche Ordnung n, dann sind durch $e_G, g, g^2, \ldots, g^{n-1}$ die n verschiedenen Elemente der zyklischen Gruppe $\langle g \rangle$ gegeben.

Beweis: Nach Satz 3.3 gilt $g^n = e_G$, und auf Grund von Lemma 3.2 gilt $\langle g\rangle = \{e_G, g, g^2, ..., g^{n-1}\}$. Wegen $|\langle g\rangle| = n$ sind alle Elemente in dieser Aufzählung verschieden. □

Für Elemente unendlicher Ordnung lässt sich eine zu Satz 3.3 weitgehend analoge Äquivalenzaussage formulieren.

Satz 3.5 Ist G eine Gruppe und $g \in G$, dann sind die folgenden Aussagen äquivalent.

(i) $\text{ord}(g) = \infty$

(ii) Es gibt kein $n \in \mathbb{N}$ mit $g^n = e_G$.

(iii) Die Abbildung $\phi : \mathbb{Z} \to G$, $k \mapsto g^k$ ist injektiv.

Beweis: „(i) ⇒ (ii)“ Angenommen, es gilt $g^n = e_G$ für ein $n \in \mathbb{N}$. Dann würde aus Lemma 3.2 die Gleichung $\langle g\rangle = \{e_G, g, ..., g^{n-1}\}$ folgen, im Widerspruch dazu, dass $\text{ord}(g) = |\langle g\rangle|$ unendlich ist.

„(ii) ⇒ (iii)“ Angenommen, ϕ ist nicht injektiv. Dann gäbe es Elemente $k, \ell \in \mathbb{Z}$ mit $k < \ell$ und $\phi(k) = \phi(\ell)$. Daraus würde $g^k = g^\ell \Leftrightarrow g^\ell (g^k)^{-1} = e_G \Leftrightarrow g^{\ell-k} = e_G$ folgen, was aber wegen $\ell - k \in \mathbb{N}$ im Widerspruch zur Voraussetzung steht.

„(iii) ⇒ (i)“ Es gilt $\phi(\mathbb{Z}) = \{g^k \mid k \in \mathbb{Z}\} = \langle g\rangle$. Auf Grund der Injektivität von ϕ erhalten wir $\text{ord}(g) = |\langle g\rangle| = |\phi(\mathbb{Z})| = |\mathbb{Z}| = \infty$. □

Beispielsweise ist 1 ein Element unendlicher Ordnung in $(\mathbb{Z}, +)$, denn es gilt $n \cdot 1 \neq 0$ für alle $n \in \mathbb{N}$.

In den symmetrischen Gruppen lassen sich die Ordnungen von Elementen leicht ermitteln. Zur Vorbereitung erinnern wir an die Definition des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen einer endlichen Menge ganzer Zahlen. Seien $a_1, ..., a_r \in \mathbb{Z}$ vorgegeben. Eine Zahl $d \in \mathbb{N}$ heißt ***gemeinsamer Teiler*** dieser Zahlen, wenn $d \mid a_k$ für $1 \leq k \leq r$ gilt. Man nennt d den ***größten*** gemeinsamen Teiler dieser Zahlen und schreibt $d = \text{ggT}(a_1, ..., a_r)$, wenn $d' | d$ für jeden gemeinsamen Teiler d' von $a_1, ..., a_r$ gilt. Zwei Zahlen a und b werden als ***teilerfremd*** bezeichnet, wenn $\text{ggT}(a, b) = 1$ ist.

Eine natürliche Zahl $d \in \mathbb{N}$ heißt ***gemeinsames Vielfaches*** von $a_1, ..., a_r$, wenn $a_k \mid d$ für $1 \leq k \leq r$ gilt, und ***kleinstes gemeinsames Vielfaches***, wenn $d \mid d'$ für jedes gemeinsame Vielfache d' dieser Zahlen erfüllt ist. Wir bezeichnen das kleinste gemeinsame Vielfache mit $\text{kgV}(a_1, ..., a_r)$. Sowohl der größte gemeinsame Teiler als auch das kleinste gemeinsame Vielfache existieren, sobald die Zahlen $a_1, ..., a_r$ nicht alle gleich Null sind, und sie sind in diesem Fall auch eindeutig bestimmt.

Satz 3.6 Sei $n \in \mathbb{N}$ und $\sigma \in S_n$.

(i) Ist σ ein k-Zykel ($2 \leq k \leq n$), dann gilt $\text{ord}(\sigma) = k$.

(ii) Ist σ ein Element vom Zerlegungtyp $(k_1, ..., k_r)$, dann gilt $\text{ord}(\sigma) = \text{kgV}(k_1, ..., k_r)$.

Beweis: zu (i) Nach Voraussetzung gibt es eine k-elementige Teilmenge $\{a_1, ..., a_k\} \subseteq M_n$ mit $\sigma = (a_1\ a_2\ ...\ a_k)$. Durch vollständige Induktion über $m \in \mathbb{N}_0$ kontrollieren wir zunächst, dass für alle $m \in \mathbb{N}_0$ und $\ell, j \in \{1, ..., k\}$ mit $\sigma^m(a_\ell) = a_j$ jeweils die Kongruenz $\ell + m \equiv j \bmod k$ erfüllt ist.

Für $m = 0$ gilt dies wegen $\sigma^0(a_\ell) = \mathrm{id}(a_\ell) = a_\ell$ und $\ell + 0 \equiv \ell \bmod k$. Sei nun $m \in \mathbb{N}_0$, und sei $j \in \{1, ..., k\}$ die eindeutig bestimmte Zahl mit $\sigma^m(a_\ell) = a_j$; dann gilt $\ell + m \equiv j \bmod k$ auf Grund der Induktionsvoraussetzung. Ist nun $j < k$, dann gilt $\sigma^{m+1}(a_\ell) = \sigma(\sigma^m(a_\ell)) = \sigma(a_j) = a_{j+1}$ und $\ell + (m+1) \equiv j + 1 \bmod k$. Im Fall $j = k$ gilt $\sigma^{m+1}(a_\ell) = \sigma(a_k) = a_1$, und wegen $\ell + (m+1) \equiv k + 1 \equiv 1 \bmod k$ ist die Kongruenz auch in diesem Fall erfüllt.

Es ist nun leicht zu sehen, dass k die kleinste natürliche Zahl mit $\sigma^k = \mathrm{id}$ ist. Ist nämlich $m \in \mathbb{N}$ mit $m < k$ und $\sigma^m(a_1) = a_j$, dann gilt $j \equiv 1 + m \not\equiv 1 \bmod k$, und somit erst recht $j \neq 1$ und $a_j \neq a_1$, also $\sigma^m \neq \mathrm{id}$. Für $\ell, j \in \{1, ..., k\}$ mit $\sigma^k(a_\ell) = a_j$ gilt dagegen $\ell + k \equiv j \bmod k$, also $\ell \equiv j \bmod k$ und damit $\ell = j$. Die Zahlen $a_1, ..., a_k$ werden also durch σ^k auf sich abgebildet, und für die Elemente von $i \in M_n \setminus \{a_1, ..., a_k\}$ gilt dies wegen $\sigma(i) = i$ natürlich ebenso.

zu (ii) Nach Definition des Zerlegungstyps existiert für $1 \leq j \leq r$ jeweils ein k_j-Zykel σ_j, so dass $\sigma = \sigma_1 \circ ... \circ \sigma_r$ gilt und die Zykel σ_j paarweise disjunkt sind. Wie wir in § 2 festgestellt haben, sind σ_i und σ_j für $1 \leq i, j \leq r$ als Elemente mit disjunktem Träger jeweils vertauschbar, und wegen Lemma 2.2 folgt daraus $\sigma^n = \sigma_1^n \circ ... \circ \sigma_r^n$ für alle $n \in \mathbb{Z}$. Auf Grund der Disjunktheit der Träger ist auch leicht zu sehen, dass genau dann $\sigma^n = \mathrm{id}$ gilt, wenn $\sigma_j^n = \mathrm{id}$ für $1 \leq j \leq r$ erfüllt ist.

Sei nun $m = \mathrm{ord}(\sigma)$; wir zeigen, dass m die definierenden Eigenschaften des kgV von $k_1, ..., k_r$ besitzt. Aus der Gleichung $\sigma_1^m \circ ... \circ \sigma_r^m = \sigma^m = \mathrm{id}$ folgt $\sigma_j^m = \mathrm{id}$ für $1 \leq j \leq r$. Nach Satz 3.3 zeigt dies, dass m ein gemeinsames Vielfaches von $k_j = \mathrm{ord}(\sigma_j)$ mit $1 \leq j \leq r$ ist. Sei nun n ein beliebiges gemeinsames Vielfaches von $k_1, ..., k_r$. Dann folgt $\sigma_j^n = \mathrm{id}$ für $1 \leq j \leq r$ mit Satz 3.3. Wir erhalten $\sigma^n = \sigma_1^n \circ ... \circ \sigma_r^n = \mathrm{id}$ und somit $m \mid n$, erneut durch eine Anwendung von Satz 3.3. Es handelt sich bei m also tatsächlich um die Zahl $\mathrm{kgV}(k_1, ..., k_r)$. □

Der Satz zeigt uns zum Beispiel, dass in der Gruppe S_5 nur Elemente der Ordnungen $1, 2, 3, 4, 5$ und 6 existieren. Denn neben der Identität, den 2-, 3-, 4- und 5-Zyklen gibt es in S_5 noch Elemente der Zerlegungtypen $(2, 2)$ und $(3, 2)$, und es gilt $\mathrm{kgV}(2, 2) = 2$ und $\mathrm{kgV}(3, 2) = 6$. Insbesondere ist $\sigma = (1\ 2\ 3)(4\ 5)$ ein Element der Ordnung 6 in S_5. Im weiteren Verlauf beschäftigen wir uns nun mit der Untergruppenstruktur zyklischer Gruppen.

Satz 3.7 Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer gilt: Sei G eine zyklische Gruppe, g ein Element mit $G = \langle g \rangle$ und U eine Untergruppe $\neq \{e_G\}$. Dann gibt es ein $m \in \mathbb{N}$ mit $U = \langle g^m \rangle$. Ist $\mathrm{ord}(g) = n$ endlich, dann kann die Zahl m so gewählt werden, dass sie ein Teiler von n ist.

Beweis: Weil U nichttrivial ist, gibt es ein $r \in \mathbb{Z}$, $r \neq 0$ mit $g^r \in U$. Weil mit g^r auch $(g^r)^{-1} = g^{-r}$ in U enthalten ist, gibt es auch natürliche Zahlen r mit $g^r \in U$. Sei nun $m \in \mathbb{N}$ die *minimale* natürliche Zahl mit der Eigenschaft $g^m \in U$. Wir zeigen, dass dann $U = \langle g^m \rangle$ gilt.

Die Inklusion „$\supseteq$“ gilt nach Definition der erzeugten Untergruppe. Nehmen wir nun an, dass „$\subseteq$“ nicht erfüllt ist. Dann gibt es ein Element $h \in U \setminus \langle g^m \rangle$ und ein $b \in \mathbb{Z}$ mit $h = g^b$. Durch Division mit Rest erhalten wir $q, r \in \mathbb{Z}$ mit $b = qm + r$ und $0 \leq r < m$. Dabei ist der Fall $r = 0$ ausgeschlossen, denn ansonsten wäre b ein Vielfaches von m und h damit doch in $\langle g^m \rangle$ enthalten. So aber gilt $h \cdot (g^m)^{-q} = g^r \in U$, im Widerspruch zur Minimalität von m. Damit ist die Gleichung $U = \langle g^m \rangle$ bewiesen.

Sei nun $n = \text{ord}(g)$ endlich, und nehmen wir an, dass m kein Teiler von n ist. Dann gibt es $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 < r < m$. Es gilt dann $g^r = g^{n-mq} = g^n \cdot (g^m)^{-q} = (g^m)^{-q} \in U$, im Widerspruch dazu, dass m mit der Eigenschaft $g^m \in U$ minimal gewählt wurde. □

Aus der Klassifikation der Untergruppen einer zyklischen Gruppe können wir das folgende zahlentheoretische Resultat herleiten.

Satz 3.8 *(Lemma von Bézout)*

Seien $m, n \in \mathbb{Z}$, $(m, n) \neq (0, 0)$. Dann gibt es $a, b \in \mathbb{Z}$ mit $am + bn = \text{ggT}(m, n)$.

Beweis: Sei $G = (\mathbb{Z}, +)$ und $U = \langle m, n \rangle$, die von m und n erzeugte Untergruppe. Nach Satz 2.9 (ii) gilt $U = \mathbb{Z}m + \mathbb{Z}n = \{am + bn \mid a, b \in \mathbb{Z}\}$. Weil $(\mathbb{Z}, +)$ zyklisch ist, gibt es nach Satz 3.7 ein $d \in \mathbb{N}$ mit $U = \langle d \rangle$. Wir zeigen, dass $d = \text{ggT}(m, n)$ erfüllt ist.

Wegen $m, n \in \langle d \rangle$ gibt es $k, \ell \in \mathbb{Z}$ mit $m = kd$ und $n = \ell d$. Dies zeigt, dass d jedenfalls ein gemeinsamer Teiler von m und n ist. Sei nun d' ein weiterer gemeinsamer Teiler. Dann gibt es $k', \ell' \in \mathbb{Z}$ mit $m = k'd'$ und $n = \ell' d'$. Die Elemente m, n liegen also in der Untergruppe $\langle d' \rangle$, und nach Definition der erzeugten Untergruppe folgt $\langle d \rangle = U = \langle m, n \rangle \subseteq \langle d' \rangle$. Insbesondere ist d in $\langle d' \rangle$ enthalten, es gibt also ein $r \in \mathbb{Z}$ mit $d = rd'$. Folglich ist d' ein Teiler von d. Damit ist der Beweis der Gleichung $d = \text{ggT}(m, n)$ abgeschlossen. Wegen $d \in U$ gibt es nun $a, b \in \mathbb{Z}$ mit $am + bn = d = \text{ggT}(m, n)$. □

Mit Hilfe des Lemma von Bézout lassen sich wichtige Rechenregeln für Elementordnungen herleiten.

Satz 3.9 Sei G eine Gruppe und $g \in G$ ein Element der endlichen Ordnung n.

(i) Für beliebiges $m \in \mathbb{Z}$ gilt $\text{ord}(g^m) = n$ genau dann, wenn $\text{ggT}(m, n) = 1$ ist.

(ii) Ist $d \in \mathbb{N}$ ein Teiler von n, dann gilt $\text{ord}(g^d) = \frac{n}{d}$.

(iii) Für beliebiges $m \in \mathbb{Z}$ gilt $\text{ord}(g^m) = \frac{n}{d}$ mit $d = \text{ggT}(m, n)$.

Beweis: zu (i) „⇒“ Wegen $g^m \in \langle g \rangle$ ist $\langle g^m \rangle$ eine Untergruppe von $\langle g \rangle$. Ist $\text{ord}(g^m) = n = \text{ord}(g)$, dann muss $\langle g^m \rangle = \langle g \rangle$ gelten. Es existiert also ein $k \in \mathbb{Z}$ mit $g = (g^m)^k = g^{km}$. Wir erhalten $g^{1-km} = e_G$ und damit $n | (1 - km)$, weil n die Ordnung von g ist. Sei nun $d \in \mathbb{N}$ ein Teiler von n und m. Aus $d | n$ folgt dann insbesondere $d | (1 - km)$. Damit ist d auch ein Teiler von $km + (1 - km) = 1$, also muss $d = 1$ sein. Wir haben damit gezeigt, dass 1 der einzige (natürliche) gemeinsame Teiler von m und n ist, und es folgt $\text{ggT}(m, n) = 1$ wie gewünscht.

„⇐“ Wegen $g^m \in \langle g \rangle$ ist $\langle g^m \rangle$ eine Untergruppe von $\langle g \rangle$. Auf Grund des Lemmas von Bézout gibt es $a, b \in \mathbb{Z}$ mit $am + bn = \text{ggT}(m, n) = 1$. Es folgt

$$g \quad = \quad g^1 \quad = \quad g^{am+bn} \quad = \quad (g^m)^a \cdot (g^n)^b \quad = \quad (g^m)^a \cdot e_G^b \quad = \quad g^{am} \quad \in \quad \langle g^m \rangle.$$

Also ist auch umgekehrt $\langle g \rangle$ eine Untergruppe von $\langle g^m \rangle$. Insgesamt erhalten wir $\langle g \rangle = \langle g^m \rangle$ und $\text{ord}(g^m) = |\langle g^m \rangle| = |\langle g \rangle| = \text{ord}(g) = n$.

zu (ii) Wegen $n = \mathrm{ord}(g)$ gilt für jedes $k \in \mathbb{Z}$ die Äquivalenz $(g^d)^k = e_G \Leftrightarrow g^{dk} = e_G \Leftrightarrow n|(dk) \Leftrightarrow \frac{n}{d} \mid k$. Auf Grund von Satz 3.3 (iii) folgt daraus $\mathrm{ord}(g^d) = \frac{n}{d}$

zu (iii) Seien m' und n' so gewählt, dass $m = m'd$ und $n = n'd$ gilt. Zu zeigen ist, dass $\mathrm{ord}(g^m) = n'$ gilt. Da d ein Teiler von n ist, können wir zunächst den bereits bewiesenen Teil (ii) anwenden und erhalten $\mathrm{ord}(g^d) = n'$. Ferner sind m' und n' teilerfremd. Denn wäre p ein gemeinsamer Primfaktor dieser beiden Zahlen, dann könnten wir $m = m'd = m''pd$ und $n = n'd = n''pd$ mit geeigneten $m'', n'' \in \mathbb{N}$ schreiben. Folglich wäre pd ein größerer gemeinsamer Teiler von m und n als d, im Widerspruch zur Definition von d. So aber können wir (i) auf das Gruppenelement g^d und die Zahl m' anwenden und erhalten $\mathrm{ord}(g^d) = \mathrm{ord}((g^d)^{m'}) = \mathrm{ord}(g^{m'd}) = \mathrm{ord}(g^m)$, insgesamt also das gewünschte Ergebnis. □

Ist beispielsweise G eine Gruppe und $g \in G$ ein Element der Ordnung 24, dann gilt $\mathrm{ord}(g^7) = \mathrm{ord}(g) = 24$, $\mathrm{ord}(g^6) = 4$ und $\mathrm{ord}(g^{10}) = 12$.

Die in der Zahlentheorie eine wichtige Rolle spielende ***Eulersche φ-Funktion*** ist für jedes $n \in \mathbb{N}$ definiert durch

$$\varphi(n) \quad = \quad |\{k \in \mathbb{Z} \mid 0 \le k < n \,,\ \mathrm{ggT}(k,n) = 1\}| \,.$$

In der Ringtheorie (Kapitel § 13) werden wir zeigen, dass für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ stets $\varphi(mn) = \varphi(m)\varphi(n)$ gilt, außerdem $\varphi(p^r) = p^{r-1}(p-1)$ für jede Primzahl p und jedes $r \in \mathbb{N}$. Damit lässt sich $\varphi(n)$ für jede natürliche Zahl n leicht berechnen.

Ist $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung n, dann sind g^k mit $0 \le k < n$ nach Folgerung 3.4 (i) die n verschiedenen Elemente von G. Aus Satz 3.9 (i) kann daher unmittelbar abgeleitet werden, dass G insgesamt $\varphi(n)$ Elemente der vollen Ordnung n enthält. Es gibt also genau $\varphi(n)$ Elemente h in G mit der Eigenschaft $G = \langle h \rangle$. Beispielsweise besitzt jede zyklische Gruppe der Ordnung 24 jeweils genau $\varphi(24) = \varphi(2^3)\varphi(3) = 4 \cdot 2 = 8$ erzeugende Elemente.

Gelegentlich ist auch das folgende Kriterium für die Bestimmung der Ordnung hilfreich.

Satz 3.10 Sei G eine Gruppe und $n \in \mathbb{N}$. Ein Element $g \in G$ hat genau dann die Ordnung n, wenn $g^n = e_G$ und für jeden Primteiler p von n jeweils $g^{n/p} \neq e_G$ gilt.

Beweis: „⇒“ Ist $n = \mathrm{ord}(g)$, dann ist $n \in \mathbb{N}$ nach Satz 3.3 minimal mit $g^n = e_G$. Insbesondere gilt dann $g^{n/p} \neq e_G$ für jeden Primteiler p von n. „⇐“ Sei $m = \mathrm{ord}(g)$ und das angegebene Kriterium für ein $n \in \mathbb{N}$ erfüllt. Aus der Gleichung $g^n = e_G$ folgt zunächst $m|n$. Nehmen wir nun an, dass m ein echter Teiler von n ist. Dann besitzt die Zahl $\frac{n}{m} \in \mathbb{N}$ einen Primteiler p. Ist $k \in \mathbb{N}$ mit $\frac{n}{m} = kp$, dann folgt $n = kpm$ und $\frac{n}{p} = km$. Wegen $g^m = e_G$ würden wir $g^{n/p} = (g^m)^k = e_G^k = e_G$ erhalten, im Widerspruch zur Annahme $g^{n/p} \neq e_G$. □

Satz 3.11 Sei G eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$.

(i) Ist $\mathrm{ord}(g) = \infty$, dann sind die verschiedenen Untergruppen von G gegeben durch $U_0 = \{e_G\}$ und $U_m = \langle g^m \rangle$, wobei m die natürlichen Zahlen durchläuft.

(ii) Ist $\mathrm{ord}(g) = n$ endlich, dann sind $U_d = \langle g^d \rangle$ die verschiedenen Untergruppen von G, wobei d die Teiler von n durchläuft. Dabei gilt jeweils $|U_d| = \frac{n}{d}$.

In (i) und (ii) gilt $U_m \subseteq U_{m'}$ für $m, m' \in \mathbb{N}$ genau dann, wenn m' ein Teiler von m ist.

Beweis: zu (i) Sei U eine beliebige Untergruppe $\neq \{e_G\}$ von G. Nach Satz 3.7 gibt es ein $m \in \mathbb{N}$ mit $U = \langle g^m \rangle$, also ist $U = U_m$ für dieses m. Seien nun $m, m' \in \mathbb{N}$ vorgegeben. Setzen wir $U_m \subseteq U_{m'}$ voraus, dann gilt insbesondere $g^m \in U_{m'}$, und folglich gibt es ein $k \in \mathbb{Z}$ mit $g^m = (g^{m'})^k = g^{km'}$, also $g^{km'-m} = e_G$. Weil die Ordnung von g unendlich ist, folgt daraus $km' - m = 0 \Leftrightarrow m = km'$, wie wir im Anschluss an Folgerung 3.4 gesehen haben. Also ist m' ein Teiler von m. Sei nun umgekehrt $m' | m$ vorausgesetzt, also $m = km'$ für ein $k \in \mathbb{Z}$. Dann gilt $g^m = (g^{m'})^k \in U_{m'}$ und somit $U_m \subseteq U_{m'}$.

zu (ii) Sei auch hier eine beliebige Untergrupe $U \neq \{e_G\}$ vorgegeben. In diesem Fall folgt aus Satz 3.7, dass $U = U_d$ für einen Teiler d von n gilt. Im Fall $U = \{e_G\}$ ist offenbar $U = U_n$. Für jeden Teiler d von n gilt außerdem $\mathrm{ord}(g^d) = \frac{n}{d}$ nach Satz 3.9 (ii). Daraus folgt jeweils $|U_d| = \frac{n}{d}$.

Der Beweis der Implikation „$m' | m \Rightarrow U_m \subseteq U_{m'}$“ läuft genau wie im Fall unendlicher Ordnung. Auch der Beweis der Umkehrung braucht nur geringfügig modifiziert werden. Aus $g^m \in U_{m'}$ folgt $g^m = (g^{m'})^k = g^{m'k}$ und somit $g^{m-m'k} = e_G$ für ein $k \in \mathbb{Z}$. Wegen $\mathrm{ord}(g) = n$ erhalten wir $n \mid (m - m'k)$ nach Satz 3.3. Es gibt also ein $\ell \in \mathbb{Z}$ mit $\ell n = m - m'k$ oder $m'k = m - \ell n$. Aus $m' \mid (m - \ell n)$ und $m' \mid (\ell n)$ folgt, dass m' ein Teiler von m ist. □

Bei einer zyklischen Gruppe der Ordnung $n \in \mathbb{N}$ stimmt die Anzahl der Untergruppen also überein mit der Anzahl der Teiler $d \in \mathbb{N}$ von n. Die Zahl $12 = 2^2 \cdot 3^1$ besitzt beipielsweise die sechs Teiler $2^i 3^j$ mit $i \in \{0, 1, 2\}$ und $j \in \{0, 1\}$; dies sind die Zahlen $1, 2, 3, 4, 6$ und 12. Dementsprechend besitzt jede zyklische Gruppe der Ordnung 12 genau sechs Untergruppen. Genauer gilt: Ist G zyklisch von Ordnung 12 und $g \in G$ ein erzeugendes Element, dann sind die Untergruppen von G durch folgende Tabelle gegeben.

Untergruppe	U_1	U_2	U_3	U_4	U_6	U_{12}
Ordnung	12	6	4	3	2	1

Dabei ist $U_d = \langle g^d \rangle$ für jeden Teiler d von 12, insbesondere $U_1 = \langle g^1 \rangle = G$ und $U_{12} = \langle g^{12} \rangle = \langle e_G \rangle = \{e_G\}$.

Zum Abschluss zeigen wir noch, dass die zyklischen Gruppen durch die soeben beschriebene Untergruppeneigenschaft sogar charakterisiert werden können.

Satz 3.12 Sei G eine endliche Gruppe der Ordnung n mit der Eigenschaft, dass G für jedes Teiler $d \in \mathbb{N}$ von n genau eine Untergruppe U_d mit $|U_d| = d$ besitzt. Dann ist G eine zyklische Gruppe.

Beweis: Wir beweisen zunächst die Gleichung $\sum_{d|n} \varphi(d) = n$ für die Eulersche φ-Funktion. Sei dazu H eine zyklische Gruppe der Ordnung n. Nach Satz 3.11 gibt es für jeden Teiler $d \in \mathbb{N}$ in H genau eine Untergruppe V_d der Ordnung d. Diese ist nach Satz 3.7 ebenfalls zyklisch, und wie wir oben festgestellt haben, besitzt diese genau $\varphi(d)$ Elemente der Ordnung d. Umgekehrt muss jedes $h \in H$ mit $\mathrm{ord}(h) = d$ in V_d liegen, weil ansonsten $\langle h \rangle$ eine von V_d verschiedene Untergruppe der Ordnung d wäre. Also ist $\varphi(d)$ die Gesamtzahl der Element der Ordnung d in H. Weil nun die Ordnung jedes Elements nach dem Satz von Lagrange ein Teiler von n ist, und weil n auch die Gesamtzahl der Elemente von H ist, erhalten wir die Gleichung $\sum_{d|n} \varphi(d) = n$, wenn die Anzahlen der Elemente der Ordnung d in H für alle Teiler d von n aufaddieren.

Sei nun G eine Gruppe mit den im Satz angegebenen Eigenschaften, und sei d ein echter Teiler von n. Ist $g \in G$ mit $\text{ord}(g) = d$, dann ist $\langle g \rangle$ die einzige Untergruppe der Ordnung d von G, und diese ist zyklisch. Als solche besitzt sie genau $\varphi(d)$ Elemente der Ordnung d. Gäbe es in G mehr als $\varphi(d)$ Elemente der Ordnung d, dann könnten diese nicht alle in $\langle g \rangle$ liegen, und folglich hätte G mehr als eine Untergruppe der Ordnung d, im Widerspruch zur Voraussetzung.

Für jeden echten Teiler d von n gibt es also höchstens $\varphi(d)$ Elemente der Ordnung d in G. Bezeichnet D die Menge der echten Teiler von n in $\mathbb{N}$, dann liefert der Beweisanfang die Ungleichung $\sum_{d \in D} \varphi(d) < n$. Dies zeigt, dass es in G nicht nur Elemente geben kann, deren Ordnung ein echter Teiler von n ist. Statt dessen muss es in G auch Elemente der Ordnung n geben. Daraus folgt, dass G zyklisch ist. □

Aus dem Satz von Lagrange und dem Konzept der Elementordnung ergibt sich noch eine für die elementare Zahlentheorie wichtige Folgerung.

Folgerung 3.13 *(Kleiner Satz von Fermat)*

Für jede Primzahl p und alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \bmod p$. Ist p kein Teiler von a, dann gilt darüber hinaus $a^{p-1} \equiv 1 \bmod p$.

Beweis: Es gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, somit ist $(\mathbb{Z}/p\mathbb{Z})^\times$ eine Gruppe der Ordnung $p-1$. Für jedes $a \in \mathbb{Z}$ ist $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ äquivalent zu $p \nmid a$. Weil die Ordnung jedes Elements der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ die Gruppenordnung teilt, gilt $(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$ für diese a, was zu $a^{p-1} \equiv 1 \bmod p$ äquivalent ist. Durch Multiplikation dieser Kongruenz mit a folgt $a^p \equiv a \bmod p$. Diese Kongruenz ist auch im Fall $p \mid a$ erfüllt, denn dann gilt auch $p \mid a^p$ und somit $a^p \equiv 0 \equiv a \bmod p$. □

§ 4. Homomorphismen und Faktorgruppen

Zusammenfassung. Ein *Homomorphismus* zwischen zwei Gruppen G, H ist eine Abbildung $G \to H$, die verträglich mit den Gruppenverknüpfungen ist. Diese spielen in der Gruppentheorie eine wichtige Rolle, weil man durch sie die Struktur der Gruppen G und H zueinander in Beziehung setzen und sie miteinander vergleichen kann. Beispielsweise hängen die Untergruppen von G und H sowie die in G und H auftretenden Elementordnungen miteinander zusammen.

Als zweites wichtiges Thema dieses Kapitels behanden wir die *Faktorgruppen*. Diese kommen dadurch zu Stande, dass man auf der Menge G/N der Linksnebenklassen einer Untergruppe N von G eine Gruppenstruktur definiert. Dies funktioniert allerdings nur bei Untergruppen N von G mit einer zusätzlichen Eigenschaft, den sogenannten *Normalteilern*. Der Homomorphiesatz für Gruppen stellt zwischen den Homomorphismen und den Faktorgruppen einen Zusammenhang her. Der Korrespondenzsatz bringt zum Ausdruck, dass sich ein Teil der Struktur der Gruppe G auch in der Faktorgruppe G/N widerspiegelt. Allerdings ist Letzere häufig einfacher zu untersuchen, da sie aus weniger Elementen besteht.

Wichtige Grundbegriffe

- Gruppenhomomorphismus
- Mono-, Epi- und Isomorphismus
- Endo- und Automorphismen einer Gruppe
- Normalteiler einer Gruppe (Notation $N \trianglelefteq G$)
- Komplexprodukt zweier Teilmengen einer Gruppe
- inneres (semi-)direktes Produkt
- Faktorgruppe, kanonischer Epimorphismus
- induzierter Homomorphismus

Zentrale Sätze

- Erhaltung der Untergruppen-Eigenschaft unter Homomorphismen
- Isomorphismus $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ für eine zyklische Gruppe G der Ordnung n
- Isomorphismus zwischen innerem und äußerem direkten Produkt zweier Normalteiler
- Homomorphiesatz für Gruppen
- Isomorphiesätze für Gruppen
- Korrespondenzsatz für Gruppen

Wir beginnen mit der Definition der Gruppenhomorphismen.

Definition 4.1 Sind $(G, *)$ und $(H, \circ)$ Gruppen, so bezeichnet man eine Abbildung $\phi : G \to H$ als ***Gruppenhomomorphismus***, wenn $\phi(g * g') = \phi(g) \circ \phi(g')$ für alle $g, g' \in G$ gilt.

Obwohl in der Definition nur gefordert wird, dass ϕ verträglich mit den Verknüpfungen der Gruppen G und H ist, werden auch das Neutralelement und inverse Elemente aufeinander abgebildet.

Lemma 4.2 Sei ϕ ein Homomorphismus zwischen den Gruppen $(G, *)$ und $(H, \circ)$. Dann gilt

$$\phi(e_G) = e_H \qquad \text{und} \qquad \phi(g^{-1}) = \phi(g)^{-1} \quad \text{für alle} \quad g \in G.$$

Beweis: Es gilt $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \circ \phi(e_G)$, und durch Multiplikation beider Seiten von links mit $\phi(e_G)^{-1}$ erhält man

$$\phi(e_G)^{-1} \circ \phi(e_G) \quad = \quad \phi(e_G)^{-1} \circ \phi(e_G) \circ \phi(e_G) \quad ,$$

also $e_H = e_H \circ \phi(e_G)$ und schließlich $e_H = \phi(e_G)$. Für jedes $g \in G$ gilt außerdem $\phi(g) \circ \phi(g^{-1}) = \phi(g * g^{-1}) = \phi(e_G) = e_H$. Multipliziert man beide Seiten von links mit $\phi(g)^{-1}$, so erhält man $\phi(g)^{-1} \circ \phi(g) \circ \phi(g^{-1}) = \phi(g)^{-1} \circ e_H$, somit $e_H \circ \phi(g)^{-1} = \phi(g)^{-1}$ und schließlich $\phi(g^{-1}) = \phi(g)^{-1}$. □

Definition 4.3 Seien $(G, *)$ und $(H, \circ)$ Gruppen und $\phi : G \to H$ ein Homomorphismus von Gruppen. Man bezeichnet ϕ als

(i) ***Monomorphismus***, wenn ϕ injektiv

(ii) ***Epimorphismus***, wenn ϕ surjektiv

(iii) ***Isomorphismus***, wenn ϕ bijektiv ist.

Einen Gruppen-Homomorphismus $\phi : G \to G$ von $(G, \cdot)$ nach $(G, \cdot)$ bezeichnet man als ***Endomorphismus*** von G. Ist die Abbildung ϕ außerdem bijektiv, dann spricht man von einem ***Automorphismus*** der Gruppe G. Die Menge der Automorphismen bezeichnen wir mit $\mathrm{Aut}(G)$. Wir bemerken, dass nach Definition 1.16 zwei Gruppen G und H genau dann zueinander isomorph sind, wenn ein Isomorphismus $\phi : G \to H$ existiert.

Lemma 4.4 Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(g^n) = \phi(g)^n$ für alle $g \in G$ und $n \in \mathbb{Z}$.

Beweis: Sei $g \in G$ vorgegeben. Zunächst beweist man die Gleichung für alle $n \in \mathbb{N}_0$ durch vollständige Induktion. Für $n = 0$ ist die Gleichung wegen $\phi(g^0) = \phi(e_G) = e_H = \phi(g)^0$ erfüllt, und setzen wir sie für n voraus, dann ist sie wegen

$$\phi(g^{n+1}) \quad = \quad \phi(g^n \cdot g) \quad = \quad \phi(g^n) \cdot \phi(g) \quad = \quad \phi(g)^n \cdot \phi(g) \quad = \quad \phi(g)^{n+1}$$

auch für $n + 1$ gültig. Für alle $n \in \mathbb{N}$ gilt außerdem $\phi(g^{-n}) = \phi((g^n)^{-1}) = \phi(g^n)^{-1} = (\phi(g)^n)^{-1} = \phi(g)^{-n}$. Dies zeigt, dass die Gleichung auch für negative Exponenten, und damit insgesamt für alle $n \in \mathbb{Z}$ gültig ist. □

Der folgende Isomorphismus wird später im Kapitel über Gruppenoperationen eine wichtige Rolle spielen.

Satz 4.5 Seien X, Y Mengen und $\phi : X \to Y$ eine Bijektion. Dann ist durch die Abbildung $\hat{\phi} : \mathrm{Per}(X) \to \mathrm{Per}(Y)$, $\sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$ ein Isomorphismus von Gruppen definiert.

Beweis: Sei $\sigma \in \mathrm{Per}(X)$ vorgegeben. Durch Komposition der Abbildungen $\phi^{-1} : Y \to X$, $\sigma : X \to X$ und $\phi : X \to Y$ erhält man eine Abbildung $Y \to Y$, und als Komposition bijektiver Abbildungen ist $\phi \circ \sigma \circ \phi^{-1}$ ebenfalls bijektiv. Also ist durch die angegebene Zuordnung $\hat{\phi}$ tatsächlich eine Abbildung $\mathrm{Per}(X) \to \mathrm{Per}(Y)$ definiert. Um zu zeigen, dass $\hat{\phi}$ ein Homomorphismus von Gruppen ist, seien $\sigma, \tau \in \mathrm{Per}(X)$ vorgegeben. Dann gilt

$$\hat{\phi}(\sigma\circ\tau) \quad = \quad \phi\circ\sigma\circ\tau\circ\phi^{-1} \quad = \quad \phi\circ\sigma\circ(\phi^{-1}\circ\phi)\circ\tau\circ\phi^{-1} \quad =$$
$$(\phi\circ\tau\circ\phi^{-1})\circ(\phi\circ\sigma\circ\phi^{-1}) \quad = \quad \hat{\phi}(\sigma)\circ\hat{\phi}(\tau).$$

Um zu zeigen, dass $\hat{\phi}$ bijektiv ist, genügt es zu bemerken, dass durch die Zuordnung $\sigma \mapsto \phi^{-1}\circ\sigma\circ\phi$ eine Umkehrabbildung $\hat{\psi} : \mathrm{Per}(Y) \to \mathrm{Per}(X)$ von $\hat{\phi}$ gegeben ist. Für jedes $\sigma \in \mathrm{Per}(Y)$ ist nämlich $\phi^{-1}\circ\sigma\circ\phi$ eine Abbildung $X \to X$, und wiederum bijektiv als Komposition bijektiver Abbildungen. Also ist $\hat{\psi}$ tatsächlich eine Abbildung von $\mathrm{Per}(Y)$ nach $\mathrm{Per}(X)$. Außerdem gilt für alle $\sigma \in \mathrm{Per}(X)$ jeweils

$$(\hat{\psi}\circ\hat{\phi})(\sigma) \quad = \quad \hat{\psi}(\hat{\phi}(\sigma)) \quad = \quad \hat{\psi}(\phi\circ\sigma\circ\phi^{-1}) \quad = \quad \phi^{-1}\circ(\phi\circ\sigma\circ\phi^{-1})\circ\phi \quad =$$
$$(\phi^{-1}\circ\phi)\circ\sigma\circ(\phi^{-1}\circ\phi) \quad = \quad \mathrm{id}_X\circ\sigma\circ\mathrm{id}_X \quad = \quad \sigma \quad = \quad \mathrm{id}_{\mathrm{Per}(X)}(\sigma) \quad ,$$

also $\hat{\psi}\circ\hat{\phi} = \mathrm{id}_{\mathrm{Per}(X)}$. Durch eine analoge Rechnung zeigt man $\hat{\phi}\circ\hat{\psi} = \mathrm{id}_{\mathrm{Per}(Y)}$. Dies zeigt, dass $\hat{\psi}$ tatsächlich die Umkehrabbildung von $\hat{\phi}$ ist. □

Nach Satz 4.5 gilt $\mathrm{Per}(X) \cong S_n$ für jede n-elementige Menge X, denn die Gleichung $|X| = n$ bedeutet ja gerade, dass eine bijektive Abbildung zwischen M_n und X existiert.

Wir befassen uns noch mit den Endo- und Automorphismen einer Gruppe und legen dafür eine beliebige Gruppe $(G,\cdot)$ zu Grunde. Sind $\phi_1, \phi_2 : G \to G$ zwei Endomorphismen von G, dann ist auch $\phi_1\circ\phi_2$ ein Endomorphismus von G, denn für alle $g,h \in G$ gilt

$$(\phi_1\circ\phi_2)(gh) \quad = \quad \phi_1(\phi_2(gh)) \quad = \quad \phi_1(\phi_2(g)\cdot\phi_2(h)) \quad =$$
$$\phi_1(\phi_2(g))\cdot\phi_1(\phi_2(h)) \quad = \quad (\phi_1\circ\phi_2)(g)\cdot(\phi_1\circ\phi_2)(h).$$

Ist ϕ_3 ein weiterer Endomorphismus, dann gilt $(\phi_1\circ\phi_2)\circ\phi_3 = \phi_1\circ(\phi_2\circ\phi_3)$; diese Gleichung wurde früher bereits für beliebge Kompositionen von Abbildungen verifiziert. Außerdem gilt $\phi_1\circ\mathrm{id}_G = \mathrm{id}_G\circ\phi_1 = \phi_1$. Dies zeigt, dass die Menge $\mathrm{End}(G)$ der Endomorphismen von G zusammen mit der Komposition $\circ$ als Verknüpfung ein Monoid bildet, mit id_G als Neutralelement. Es gilt nun

> **Proposition 4.6** Die invertierbaren Elemente in $\mathrm{End}(G)$ sind genau die Automorphismen der Gruppe G.

Beweis: Ist ϕ in $\mathrm{End}(G)$ ein invertierbares Element, dann gibt es ein $\psi \in \mathrm{End}(G)$ mit $\psi\circ\phi = \mathrm{id}_G$ und $\phi\circ\psi = \mathrm{id}_G$. Aus den Gleichungen folgt, dass ϕ bijektiv ist. Als bijektiver Homomorphismus ist ϕ nach Definition ein Automorphismus.

Sei nun umgekehrt ϕ ein Automorphismus von G. Dann ist ϕ bijektiv. Wir zeigen weiter unten, dass die Umkehrabbildung ϕ^{-1} von ϕ ein Gruppenhomomorphismus ist. Weil mit ϕ auch ϕ^{-1} bijektiv ist, ist durch ϕ^{-1} dann insgesamt ein Automorphismus gegeben. Darüber hinaus zeigen die Gleichungen $\phi^{-1}\circ\phi = \mathrm{id}_G$ und $\phi\circ\phi^{-1} = \mathrm{id}_G$, dass es sich bei ϕ im Monoid $\mathrm{End}(G)$ um ein invertierbares Element handelt.

Zum Nachweis der Homomorphismus-Eigenschaft von ϕ^{-1} seien $g,h \in G$ vorgegeben. Auf Grund der Homomorphismus-Eigenschaft von ϕ gilt $\phi(\phi^{-1}(g)\cdot\phi^{-1}(h)) = \phi(\phi^{-1}(g))\cdot\phi(\phi^{-1}(h)) = gh$. Durch Anwendung von ϕ^{-1} auf beide Seiten dieser Gleichung erhalten wir $\phi^{-1}(g)\phi^{-1}(h) = \phi^{-1}(gh)$. Also ist ϕ^{-1} verträglich mit der Verknüpfung von G und damit ein Homomorphismus. □

Durch Anwendung von Satz 1.15 erhalten wir nun

Satz 4.7 Die Automorphismen einer Gruppe G bilden mit der Verknüpfung $\circ$ selbst eine Gruppe. Man nennt sie die ***Automorphismengruppe*** $\mathrm{Aut}(G)$ der Gruppe G.

Ergänzend bemerken wir noch, dass allgemein gilt: Ist $\phi : G \to H$ ein Isomorphismus von Gruppen, dann gilt dasselbe für die Umkehrabbildung $\phi^{-1} : H \to G$. Der Nachweis dafür funktioniert genauso wie im zweiten Teil des Beweises von Proposition 4.6. Allerdings lassen sich zwei Isomorphismen $G \to H$ in der Regel nicht verknüpfen (jedenfalls nicht durch die Komposition von Abbildungen), also bilden die Isomorphismen zwischen G und H im Allgemeinen keine Gruppe.

Als nächstes befassen wir uns mit der Beziehung zwischen Homomorphismen und Untergruppen.

Proposition 4.8 Sei $\phi : G \to H$ ein Gruppenhomomorphismus, außerdem U eine Untergruppe von G und V eine Untergruppe von H. Dann gilt

(i) Die Bildmenge $\phi(U)$ ist eine Untergruppe von H.

(ii) Die Urbildmenge $\phi^{-1}(V)$ ist eine Untergruppe von G.

Beweis: zu (i) Wegen $e_G \in U$ und $\phi(e_G) = e_H$ ist $e_H \in \phi(U)$ enthalten. Seien nun $g', h' \in \phi(U)$ vorgegeben. Dann gibt es Elemente $g, h \in U$ mit $\phi(g) = g'$ und $\phi(h) = h'$. Mit g, h liegen auch die Elemente gh und g^{-1} in U. Es folgt $g'h' = \phi(g)\phi(h) = \phi(gh) \in \phi(U)$, und ebenso erhalten wir $(g')^{-1} = \phi(g)^{-1} = \phi(g^{-1}) \in \phi(U)$.

zu (ii) Aus $\phi(e_G) = e_H \in V$ folgt $e_G \in \phi^{-1}(V)$. Sind $g, h \in \phi^{-1}(V)$ vorgegeben, dann gilt $\phi(g), \phi(h) \in V$. Es folgt $\phi(gh) = \phi(g)\phi(h) \in V$ und somit $gh \in \phi^{-1}(V)$. Ebenso gilt $\phi(g^{-1}) = \phi(g)^{-1} \in V$, also $g^{-1} \in \phi^{-1}(V)$. □

Eine besonders wichtige Rolle spielen in der Gruppentheorie der ***Kern*** $\ker(\phi) = \phi^{-1}(\{e_H\})$ und das ***Bild*** $\mathrm{im}(\phi) = \phi(G)$ eines Gruppenhomomorphismus. Nach Proposition 4.8 ist $\ker(\phi)$ eine Untergruppe von G und $\mathrm{im}(\phi)$ eine Untergruppe von H. Beispielsweise ist für jedes $n \in \mathbb{N}$ die ***alternierende Gruppe*** A_n als Kern des Signums-Homomorphismus $\mathrm{sgn} : S_n \to \{\pm 1\}$ eine Untergruppe der symmetrischen Gruppe S_n.

Aus der Linearen Algebra ist bekannt, dass die Determinante auf der Menge $\mathcal{M}_{n,K}$ der $(n \times n)$-Matrizen über einem Körper K die Multiplikativitätsregel $\det(AB) = \det(A)\det(B)$ erfüllt. Außerdem gilt $\det(A) \neq 0$ genau dann, wenn A invertierbar ist. Daraus folgt, dass die Determinantenfunktion einen Gruppenhomomorphismus $\det : \mathrm{GL}_n(K) \to K^\times$ definiert. Die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ ist nach Definition genau der Kern dieses Homomorphismus.

Kerne und Bilder sind bereits aus der Linearen Algebra im Zusammenhang mit linearen Abbildungen bekannt. Wie dort gilt auch hier der Zusammenhang

Proposition 4.9 Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Die Abbildung ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{e_G\}$ gilt.

Beweis: „⇒“ Ist ϕ ein Monomorphismus, dann ist e_G das einzige Element, das auf e_H abgebildet wird. Also gilt $\ker(\phi) = \{e_G\}$. „⇐“ Setzen wir $\ker(\phi) = \{e_G\}$ voraus, und seien $g, h \in G$ mit $\phi(g) = \phi(h)$ vorgegeben. Dann gilt $\phi(g)\phi(h)^{-1} = e_H$, und wir erhalten $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = e_H$. Nach Definition des Kerns folgt $gh^{-1} \in \ker(\phi)$. Auf Grund der Voraussetzung bedeutet dies $gh^{-1} = e_G$ und somit $g = h$. □

In vielen Anwendungen erweist es sich als nützlich, dass ein Homomorphismus $G \to H$ bereits durch die Bilder eines Erzeugendensystems eindeutig festgelegt ist. Der Grund dafür besteht darin, dass viele bedeutende Gruppen (wie zum Beispiel die symmetrische Gruppen) sehr kleine Erzeugendensysteme besitzen.

Satz 4.10 *(Eindeutigkeit von Homomorphismen)*

Seien G, H Gruppen und $S \subseteq G$ ein Erzeugendensystem von G. Sind $\phi, \phi' : G \to H$ Gruppenhomomorphismen mit $\phi(s) = \phi'(s)$ für alle $s \in S$, dann folgt $\phi = \phi'$.

Beweis: Wir zeigen, dass die Teilmenge $U = \{g \in G \mid \phi(g) = \phi'(g)\}$ eine Untergruppe von G ist. Wegen $\phi(e_G) = e_H = \phi'(e_G)$ ist $e_G \in U$. Sind $g, h \in U$ beliebig vorgegeben, dann gilt

$$\phi(gh) = \phi(g)\phi(h) = \phi'(g)\phi'(h) = \phi'(gh) \qquad \text{und} \qquad \phi(g^{-1}) = \phi(g)^{-1} = \phi'(g)^{-1} = \phi'(g^{-1}) \quad ,$$

also gilt $gh \in U$ und $g^{-1} \in U$. Weil U nach Voraussetzung die Menge S enthält, gilt $G = \langle S \rangle \subseteq U$ und somit $G = U$. Die Abbildungen ϕ und ϕ' stimmen also auf der gesamten Gruppe G überein. □

Ist also beispielsweise $S = \{a, b\}$ ein zweielementiges Erzeugendensystem einer Gruppe G, dann ist jeder Homomorphismus $\phi : G \to H$ in eine beliebige Gruppe H bereits durch die Bilder $\phi(a), \phi(b) \in H$ eindeutig festgelegt.

Kommen wir nun zur Frage nach der *Existenz* von Homomorphismen. Für zwei beliebige Gruppen G und H ist durch $G \to H$, $g \mapsto e_H$ ein Homomorphismus definiert; man bezeichnet ihn als den ***trivialen*** Homomorphismus. Ob es weitere Homomorphismen zwischen G und H gibt, ist in der Regel nicht leicht zu entscheiden. Der Fall, dass es sich bei G um eine *zyklische* Gruppe handelt, ist eine der seltenen Situationen, in denen weit reichende allgemeine Aussagen möglich sind.

Proposition 4.11 Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Ist $g \in G$ ein Element von endlicher Ordnung n, dann ist auch $\mathrm{ord}(\phi(g))$ endlich, und ein Teiler von n.

Beweis: Auf Grund der Homomorphismus-Eigenschaft gilt $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$. Aus den Teilen (ii) und (iii) von Satz 3.3 folgt sowohl die Endlichkeit von $\mathrm{ord}(\phi(g))$ als auch die Teiler-Eigenschaft. □

Proposition 4.12 *(Existenz von Homomorphismen auf zyklischen Gruppen)*

Sei G eine zyklische Gruppe, $g \in G$ ein erzeugendes Element, H eine weitere Gruppe und $h \in H$. Ist $\mathrm{ord}(g) = \infty$ oder $\mathrm{ord}(g)$ endlich und ein Vielfaches von $\mathrm{ord}(h)$, dann existiert ein (eindeutig bestimmter) Gruppenhomomorphismus $\phi : G \to H$ mit $\phi(g) = h$.

Beweis: Die Eindeutigkeit folgt in beiden Fällen aus Satz 4.10. Für die Existenz betrachten wir zunächst den Fall $\mathrm{ord}(g) = \infty$ und definieren die Abbildung ϕ durch $\phi(g^n) = h^n$ für alle $n \in \mathbb{Z}$. Dann ist ϕ eine wohldefinierte Abbildung und ein Homomorphismus, denn alle Elemente aus G lassen sich auf eindeutige Weise in der Form g^m mit $m \in \mathbb{Z}$ darstellen, und für alle $m, n \in \mathbb{Z}$ gilt $\phi(g^m g^n) = \phi(g^{m+n}) = h^{m+n} = h^m h^n = \phi(g^m)\phi(g^n)$.

Sei nun $n = \text{ord}(g)$ endlich und ein Vielfaches von $\text{ord}(h)$. Dann definieren wir ϕ als Abbildung durch $\phi(g^k) = h^k$ für $0 \leq k < n$. Wir zeigen, dass dann $\phi(g^m) = h^m$ für alle $m \in \mathbb{Z}$ erfüllt ist. Division von m durch n mit Rest liefert $q, r \in \mathbb{Z}$ mit $m = qn + r$ und $0 \leq r < n$. Da n ein Vielfaches von $\text{ord}(h)$ ist, gilt $h^n = e_H$, und es folgt

$$\phi(g^m) \quad = \quad \phi(g^{qn+r}) \quad = \quad \phi((g^n)^q g^r) \quad = \quad \phi(g^r) \quad = \quad h^r \quad = \quad (h^n)^q h^r \quad = \quad h^{qn+r} \quad = \quad h^m.$$

Wie im Fall unendlicher Ordnung prüft man nun die Homomorphismus-Eigenschaft von ϕ. □

Folgerung 4.13 Je zwei unendliche zyklische Gruppen sind isomorph. Ebenso sind zwei endliche zyklische Gruppen derselben Ordnung isomorph.

Beweis: Seien G und H unendliche zyklische Gruppen und $g \in G$, $h \in H$ mit $G = \langle g \rangle$ sowie $H = \langle h \rangle$. Dann gibt es nach Proposition 4.12 eindeutig bestimmte Homomorphismen $\phi : G \to H$ und $\psi : H \to G$ mit $\phi(g) = h$ und $\psi(h) = g$. Es gilt $(\psi \circ \phi)(g) = g$. Aber nach Satz 4.10 gibt es nur einen Homomorphismus $G \to G$ mit $g \mapsto g$, nämlich id_G. Somit ist $\psi \circ \phi = \text{id}_G$. Ebenso schließt man aus der Gleichung $(\phi \circ \psi)(h) = h$, dass $\phi \circ \psi = \text{id}_H$ gilt. Die Abbildungen ϕ und ψ sind also zueinander invers und damit bijektiv. Es folgt $G \cong H$. Im Fall endlicher Ordnung verläuft der Beweis analog. □

Mit Hilfe dieser Ergebnisse können wir nun die Automorphismengruppe zyklischer Gruppen bestimmen. Dazu betrachten wir die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$. Nach Satz 1.15 bildet diese Menge mit der Multiplikation als Verknüpfung eine Gruppe, die man als ***prime Restklassengruppe*** bezeichnet. Mit dem folgenden Kriterium lasse sich die Elemente dieser Gruppen leicht bestimmen.

Proposition 4.14 Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das Element $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann in $(\mathbb{Z}/n\mathbb{Z})^\times$ enthalten, wenn $\text{ggT}(a, n) = 1$ ist.

Beweis: „⇒“ Ist $a + n\mathbb{Z}$ im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ invertierbar, dann existiert ein $b \in \mathbb{Z}$ mit $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$. Daraus folgt $ab + n\mathbb{Z} = 1 + n\mathbb{Z}$, was wiederum zu $ab \equiv 1 \bmod n$ äquivalent ist. Die Zahl $1 - ab$ ist also teilbar durch n; es existiert also ein $k \in \mathbb{Z}$ mit $1 - ab = kn$, was zu $ab + kn = 1$ umgeformt werden kann. Ist nun $d \in \mathbb{N}$ ein gemeinsamer Teiler von a und n, dann folgt aus der letzten Gleichung, dass d auch ein Teiler von 1 sein und somit $d = 1$ gelten muss. Damit ist $\text{ggT}(a, n) = 1$ nachgewiesen.

„⇐“ Aus $\text{ggT}(a, n) = 1$ folgt mit Satz 3.8, dem Lemma von Bézout, die Existenz von $b, k \in \mathbb{Z}$ mit $ab + kn = 1$. Dasdurch erhalten wir im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ die Gleichung

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) \quad = \quad ab + n\mathbb{Z} \quad = \quad ab + kn + n\mathbb{Z} = 1 + n\mathbb{Z}.$$

Dies zeigt, dass $a + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ invertierbar ist. □

Sei nun G eine zyklische Gruppe der endlichen Ordnung n und $g \in G$ mit $G = \langle g \rangle$. Wegen Satz 3.9 ist $\text{ord}(g^a)$ für jedes $a \in \mathbb{Z}$ ein Teiler von n. Wir können also Proposition 4.12 anwenden und erhalten für jedes $a \in \mathbb{Z}$ einen eindeutig bestimmten Endomorphismus

$$\tau_a : G \to G \qquad \text{mit} \qquad \tau_a(g) = g^a.$$

Wir können nun eine Abbildung $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$ durch $\phi(a+n\mathbb{Z}) = \tau_a$ für $0 \le a < n$ definieren. Es gilt dann $\phi(a+n\mathbb{Z}) = \tau_a$ für alle $a \in \mathbb{Z}$. Teilen wir nämlich a mit Rest durch n, ist also $a = qn+r$ mit $q, r \in \mathbb{Z}$ und $0 \le r < n$, dann gilt $\tau_a(g) = g^a = g^{qn+r} = (g^n)^q \cdot g^r = e_G^q \cdot g^r = g^r = \tau_r(g)$, und somit $\tau_a = \tau_r$ nach Satz 4.10. Es folgt $\phi(a+n\mathbb{Z}) = \phi(r+n\mathbb{Z}) = \tau_r = \tau_a$.

Satz 4.15 Durch Einschränkung der Abbildung ϕ auf $(\mathbb{Z}/n\mathbb{Z})^\times$ erhält man einen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(G)$.

Beweis: Zunächst zeigen wir, dass ϕ verträglich mit der Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ und der Komposition auf $\mathrm{End}(G)$ ist. Für alle $a, b \in \mathbb{Z}$ gilt

$$(\tau_a \circ \tau_b)(g) \quad = \quad \tau_a(\tau_b(g)) \quad = \quad \tau_a(g^b) \quad = \quad \tau_a(g)^b \quad = \quad (g^a)^b \quad = \quad g^{ab} \quad = \quad \tau_{ab}(g).$$

Eine Anwendung von Satz 4.10 liefert $\tau_a \circ \tau_b = \tau_{ab}$, und es folgt $\phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z}) = \phi(ab+n\mathbb{Z})$. Als nächstes überprüfen wir, dass ϕ die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z}$ der invertierbare Elemente von $\mathbb{Z}/n\mathbb{Z}$ surjektiv auf $\mathrm{Aut}(G)$ abbildet. Offenbar ist τ_1 der eindeutig bestimmte Endomorphismus von G, der g auf g abbildet; daraus folgt $\tau_1 = \mathrm{id}_G$. Ist nun $a+n\mathbb{Z}$ ein invertierbares Element, dann existiert ein $b \in \mathbb{Z}$ mit $(a+n\mathbb{Z})(b+n\mathbb{Z}) = 1+n\mathbb{Z}$. Die soeben bewiesene Gleichung liefert

$$\tau_a \circ \tau_b \quad = \quad \phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z}) \quad = \quad \phi(1+n\mathbb{Z}) \quad = \quad \tau_1 \quad = \quad \mathrm{id}_G \quad ,$$

und ebenso erhält man $\tau_b \circ \tau_a = \mathrm{id}_G$. Dies zeigt, dass τ_a ein Automorphismus von G und ϕ somit $(\mathbb{Z}/n\mathbb{Z})^\times$ nach $\mathrm{Aut}(G)$ abbildet. Umgekehrt ist jedes Element $\tau \in \mathrm{Aut}(G)$ ist im Bild von $\phi|_{(\mathbb{Z}/n\mathbb{Z})^\times}$ enthalten. Denn wegen $\tau(g) \in \langle g \rangle$ existiert ein $a \in \mathbb{Z}$ mit $\tau(g) = g^a = \tau_a(g)$, woraus $\tau = \tau_a$ folgt, erneut auf Grund von Proposition 4.10. Wegen $\tau(g^m) = \tau(g)^m = (g^a)^m$ für alle $m \in \mathbb{Z}$ besteht das Bild $\tau(G)$ nur aus Potenzen von g^a. Wegen $\tau \in \mathrm{Aut}(G)$ gilt insbesondere $\tau(G) = G$; also muss g^a in G ein Element der Ordnung n sein. Daraus folgt $\mathrm{ggT}(a, n) = 1$ (nach Teil (i) von Satz 3.9) und somit $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ (nach Proposition 4.14).

Also ist durch $\phi|_{(\mathbb{Z}/n\mathbb{Z})^\times}$ ein surjektiver Gruppenhomomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G)$ gegeben. Dieser ist auch injektiv. Ist nämlich $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\phi(a+n\mathbb{Z}) = \mathrm{id}_G$ vorgegeben, dann folgt $g^a = \tau_a(g) = \phi(a+n\mathbb{Z})(g) = \mathrm{id}_G(g) = g^1$. Wir erhalten $g^{a-1} = e_G$, also $n \mid (a-1)$, damit $a \equiv 1 \bmod n$ und $a+n\mathbb{Z} = 1+n\mathbb{Z}$. Die Injektivität folgt nun aus Proposition 4.9. □

Auch im Fall, dass $G = \langle g \rangle$ unendlich ist, lässt sich die Automorphismengruppe leicht angeben. Nach Proposition 4.12 sind die Endomorphismen einer solchen Gruppe G genau die Abbildungen der Form $\tau_a(g) = g^a$, wobei a die Menge $\mathbb{Z}$ der ganzen Zahlen durchläuft. Im Gegensatz zum endlichen Fall gilt hier $\tau_a = \tau_b$ für $a, b \in \mathbb{Z}$ genau dann, wenn $a = b$ ist, denn nur in diesem Fall ist $g^a = g^b$. Wie in Satz 4.15 überprüft man, dass durch $\mathbb{Z} \to \mathrm{End}(G)$, $a \mapsto \tau_a$ ein Isomorphismus zwischen den Monoiden $(\mathbb{Z}, \cdot)$ und $(\mathrm{End}(G), \circ)$ gegeben ist. Wiederum ist τ_a genau dann ein Automorphismus, wenn a in $(\mathbb{Z}, \cdot)$ invertierbar ist, und die invertierbaren Elemente in dieser Gruppen sind ± 1.

Wie bei den zyklischen Gruppen endlicher Ordnung kommt man so zu dem Ergebnis $(\mathrm{Aut}(G), \circ) \cong (\{\pm 1\}, \cdot)$. Da es sich bei $(\{\pm 1\}, \cdot)$ und $(\mathbb{Z}/2\mathbb{Z}, +)$ um zyklische Gruppen der Ordnung 2 handelt, sind diese nach Folgerung 4.13 isomorph. Somit gilt auch $(\mathrm{Aut}(G), \circ) \cong (\mathbb{Z}/2\mathbb{Z}, +)$ für jede unendliche zyklische Gruppe G.

Ist U eine Untergruppe, dann bilden die Nebenklassen gU lediglich eine Menge, die wir mit G/U bezeichnet haben. Wir betrachten nun im weiteren Verlauf einen speziellen Typ von Untergruppen, die es uns ermöglichen werden, auf der Menge G/U wiederum eine Gruppenstruktur zu definieren.

Definition 4.16 Sei G eine Gruppe. Eine Untergruppe U von G wird ***Normalteiler*** von G genannt (Schreibweise $U \trianglelefteq G$), wenn $gU = Ug$ für alle $g \in G$ gilt.

Für die Normalteiler-Eigenschaft einer Untergruppe gibt es mehrere äquivalente Kriterien.

Proposition 4.17 Sei G eine Gruppe und U eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

(i) U ist Normalteiler von G.

(ii) Es gilt $gUg^{-1} \subseteq U$ für alle $g \in G$, wobei $gUg^{-1} = \{gug^{-1} \mid u \in U\}$ ist.

(iii) Es gilt $gUg^{-1} = U$ für alle $g \in G$.

Beweis: „(i) $\Rightarrow$ (ii)“ Seien $g \in G$ und $h \in gUg^{-1}$ vorgegeben. Dann gibt es ein $u \in U$ mit $h = gug^{-1}$. Auf Grund der Gleichung $gU = Ug$ finden wir ein $u' \in U$ mit $gu = u'g$. Es folgt $h = (u'g)g^{-1} = u' \in U$. Damit ist die Inklusion $gUg^{-1} \subseteq U$ nachgewiesen.

„(ii) $\Rightarrow$ (iii)“ Sei $g \in G$ vorgegeben. Auf Grund der Voraussetzung genügt es, die Inklusion $U \subseteq gUg^{-1}$ zu beweisen. Seien $g \in G$ und $u \in U$ vorgegeben. Nach Voraussetzung gilt auch $g^{-1}Ug \subseteq U$, also liegt das Element $u' = g^{-1}ug$ in U. Es folgt $u = gu'g^{-1} \in gUg^{-1}$.

„(iii) $\Rightarrow$ (i)“ Zunächst beweisen wir die Inklusion $gU \subseteq Ug$. Sei dazu $h \in gU$ vorgegeben. Dann gibt es ein $u \in U$ mit $h = gu$. Nach Voraussetzung liegt das Element $u' = gug^{-1}$ in U. Es gilt also $h = u'g \in Ug$. Zum Beweis von $Ug \subseteq gU$ sei nun umgekehrt $h \in Ug$ enthalten, also $h = ug$ für ein $u \in U$. Wegen $g^{-1}Ug = U$ liegt $u' = g^{-1}ug$ in U. Daraus folgt $h = gu' \in gU$. □

Ist G eine beliebige Gruppe, dann sind $\{e_G\}$ und G stets Normalteiler von G. Man nennt eine Gruppe G ***einfach***, wenn $G \neq \{e_G\}$ gilt und es neben diesen beiden keine weiteren Normalteiler von G gibt. Ist G abelsch, dann ist *jede* Untergruppe von G ein Normalteiler; vgl. die Bemerkung unmittelbar vor Lemma 2.14. Eine abelsche Gruppe ist also nur dann einfach, wenn sie außer $\{e_G\}$ und G keine weiteren Untergruppen besitzt. Wir werden später sehen, dass dies bei abelschen Gruppen nur auf die Gruppen von Primzahlordnung zutrifft. Nicht-kommutative einfache Gruppen haben dagegen (anders als die Bezeichung „einfach“ vermuten lässt) in der Regel eine sehr komplizierte Struktur.

Gilt $N \trianglelefteq G$, dann gilt offenbar auch $N \trianglelefteq U$ für jede Untergruppe U von G mit $U \supseteq N$. Neben dem direkten Nachrechnen lässt sich die Normalteiler-Eigenschaft auch durch folgende Kriterien feststellen.

Satz 4.18

(i) Ist G eine Gruppe und U eine Untergruppe mit $(G:U)=2$, dann gilt $U \trianglelefteq G$.

(ii) Ist G eine Gruppe und $(N_i)_{i\in I}$ eine Familie von Normalteilern, dann ist auch $N=\bigcap_{i\in I} N_i$ ein Normalteiler von G.

(iii) Sei nun $\phi: G \to H$ ein Gruppenhomomorphismus. Ist N ein Normalteiler von H, dann ist $\phi^{-1}(N)$ ein Normalteiler von G.

(iv) Ist ϕ surjektiv und N Normalteiler von G, dann ist $\phi(N)$ Normalteiler von H.

Beweis: zu (i) Sei $g \in G$ beliebig. Ist g in U enthalten, dann gilt $gU = U = Ug$. Setzen wir nun $g \notin U$ voraus. Dann ist gU eine von U verschiedene Linksnebenklasse in G. Wegen $(G:U)=2$ sind U und gU die einzigen Linksnebenklassen, und wir erhalten eine disjunkte Zerlegung $G = U \cup gU$, also $gU = G \setminus U$. Ebenso zeigt man $Ug = G \setminus U$. Insgesamt erhalten wir $gU = Ug$.

zu (ii) Für beliebiges $g \in G$ ist zu zeigen, dass $gNg^{-1} \subseteq N$ gilt. Sei also $h \in gNg^{-1}$. Dann gibt es ein $n \in N$ mit $h = gng^{-1}$. Weil jedes N_i Normalteiler und nach Voraussetzung n in jedem N_i enthalten ist, gilt $h = gng^{-1} \in N_i$ für alle $i \in I$. Also liegt h in N.

zu (iii) Sei $n \in \phi^{-1}(N)$, also $\phi(n) \in N$. Dann gilt $h\phi(n)h^{-1} \in N$ für alle $h \in H$. Insbesondere gilt $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} \in N$ für alle $g \in G$, also $gng^{-1} \in \phi^{-1}(N)$ für alle $g \in G$.

zu (iv) Sei $n \in \phi(N)$, also $n = \phi(n')$ für ein $n' \in G$. Ist nun $h \in H$ beliebig vorgegeben, dann finden wir auf Grund der Surjektivität von ϕ ein $g \in G$ mit $\phi(g) = h$. Weil N Normalteiler von G ist, gilt $gn'g^{-1} \in N$. Es folgt $hnh^{-1} = \phi(g)\phi(n')\phi(g)^{-1} = \phi(gn'g^{-1}) \in \phi(N)$. □

Beispielsweise ist $N = \langle(1\ 2\ 3)\rangle$ ein Normalteiler von S_3, denn aus $|N| = 3$ und $|S_3| = 6$ folgt $(G:N) = 2$ nach dem Satz von Lagrange. Die Untergruppe $U = \langle(1\ 2)\rangle$ ist dagegen *kein* Normalteiler von S_3, denn wie wir bereits in §4 gesehen haben, stimmen Links- und Rechtsnebenklassen von U nicht überein. Für $g = (1\ 2\ 3)$ beispielsweise gilt $gU = \{(1\ 2\ 3), (1\ 3)\}$ und $Ug = \{(1\ 2\ 3), (2\ 3)\}$.

Aus Teil (iii) von Satz 4.18, angewendet auf den Normalteiler $\{e_H\}$ von H, folgt insbesondere, dass ***Kerne von Homomorphismen stets Normalteiler*** sind. Umgekehrt werden wir in Kürze sehen, dass jeder Normalteiler auch Kern eines geeigneten Homomorphismus ist.

Man beachte, dass Teil (iv) ohne die Voraussetzung der Surjektivität falsch wird. Als Beispiel betrachte man die Inklusionsabbildung $\phi: \langle(1\ 2)\rangle \to S_3$, $\sigma \mapsto \sigma$. Offenbar gilt $\phi(\langle(1\ 2)\rangle) = \langle(1\ 2)\rangle$ und $\langle(1\ 2)\rangle \trianglelefteq \langle(1\ 2)\rangle$. Aber andererseits ist $\langle(1\ 2)\rangle$, wie bereits festgestetllt, kein Normalteiler von S_3.

In bestimmten Situationen können Normalteiler verwendet werden, um Gruppen in äußere direkte Produkte kleinerer Gruppen zu zerlegen. Zur Vorbereitung definieren wir

Definition 4.19 Sei G eine Gruppe, und seien $A, B \subseteq G$ beliebige Teilmengen. Dann nennt man die Teilmenge $AB = \{ab \mid a \in A, b \in B\}$ das ***Komplexprodukt*** von A und B.

Bei Gruppen in additiver Schreibweise verwendet man für das Komplexprodukt die Schreibweise $A+B$ statt AB. Die folgenden „Rechenregeln“ für Komplexprodukte werden wir im weiteren Verlauf der Vorlesung an mehreren Stellen verwenden, in diesem Kapitel beispielsweise weiter unten beim Beweis des Korrespondenzsatzes.

Lemma 4.20 Sei G eine Gruppe, und seien U und N Untergruppen von G.

(i) Gilt $U \cap N = \{e\}$, dann hat jedes Element $g \in UN$ eine eindeutige Darstellung der Form $g = un$, mit $u \in U$ und $n \in N$.

(ii) Gilt $U \subseteq N$, dann folgt $UN = N$.

(iii) Gilt $UN = NU$, dann ist UN eine Untergruppe von G. Ersteres ist insbesondere dann gegeben, wenn N ein Normalteiler von G ist.

(iv) Sind N und U beides Normalteiler von G, dann folgt $UN \trianglelefteq G$.

Beweis: zu (i) Sei $g \in UN$. Die Existenz einer Darstellung der angegebenen Form ist auf Grund der Definition des Komplexprodukts offensichtlich. Nehmen wir nun an, es gibt $u, u' \in U$ und $n, n' \in N$ mit $g = un = u'n'$. Dann kann die Gleichung $un = u'n'$ umgeformt werden zu $(u')^{-1}u = n'n^{-1}$. Dieses Produkt liegt in $U \cap N = \{e\}$. Es folgt $(u')^{-1}u = e$ und $n'n^{-1} = e$, also $u = u'$ und $n = n'$.

zu (ii) Ist $g \in N$, dann gilt $g = e_G g \in UN$. Liegt umgekehrt g in UN, dann gibt es $u \in U$ und $n \in N$ mit $g = un$. Da N als Untergruppe von G unter der Verknüpfung abgeschlossen ist und u, n in N liegen, folgt $g = un \in N$.

zu (iii) Wir beweisen die Untergruppen-Eigenschaft von UN unter der gegebenen Voraussetzung. Zunächst ist das Neutralelement $e_G = e_G e_G$ wegen $e_G \in U$ und $e_G \in N$ in UN enthalten. Seien nun $g, g' \in UN$ vorgegeben. Dann gibt es $u, u' \in U$ und $n, n' \in N$ mit $g = un$ und $g' = u'n'$. Auf Grund der Voraussetzung finden wir ein $u'' \in U$ und $n'' \in N$ mit $nu' = u''n''$, so dass das Element

$$gg' \quad = \quad (un)(u'n') \quad = \quad u(nu')n' \quad = \quad u(u''n'')n' \quad = \quad (uu'')(n''n')$$

in UN liegt. Aus $g^{-1} = (un)^{-1} = n^{-1}u^{-1} \in NU$ und $NU = UN$ folgt auch $g^{-1} \in UN$.

Sei nun N ein Normalteiler von G und $g \in UN$. Dann gibt es Elemente $u \in U$ und $n \in N$ mit $g = un$. Auf Grund der Normalteiler-Eigenschaft gilt $uN = Nu$, es existiert also ein $n' \in N$ mit $un = n'u$. Dies zeigt, dass g in NU enthalten ist, und wir haben damit die Inklusion $UN \subseteq NU$ bewiesen. Der Nachweis der Inklusion $NU \subseteq UN$ funktioniert analog.

zu (iv) Sei $g \in G$ beliebig. Um zu zeigen, dass UN Normalteiler von G ist, müssen wir die Inklusion $g(UN)g^{-1} \subseteq UN$ nachrechnen. Ist $h \in g(UN)g^{-1}$, dann gibt es Elemente $u \in U$ und $n \in N$ mit $h = g(un)g^{-1}$. Da U Normalteiler von G ist, gilt $gug^{-1} \in U$, und aus $N \trianglelefteq G$ folgt $gng^{-1} \in G$. Insgesamt erhalten wir $h = g(un)g^{-1} = (gug^{-1})(gng^{-1}) \in UN$. □

Selbst wenn U und N beides Untergruppen von G sind, braucht das Komplexprodukt UN im Allgemeinen keine Untergruppe von G zu sein. Als Beispiel betrachten wir $G = S_3$, $U = \langle(1\ 2)\rangle$ und $N = \langle(1\ 3)\rangle$. Dann ist $UN = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$. Nach dem Satz von Lagrange kann diese vierelementige Teilmenge keine Untergruppe der sechselementigen Gruppe S_3 sein.

In § 1 hatten wir die Diedergruppen D_n für $n \geq 3$ als Symmetriegruppen des regelmäßigen n-Ecks definiert. Mit dem soeben eingeführten Konzept des Komplexprodukts können wir nun auf einfache Art nachweisen, dass die in § 1 angegebene Menge von Elementen eine Untergruppe der orthogonalen Gruppe $\mathcal{O}(2)$ bildet. Als weiteres Hilfsmittel benötigen wir noch den folgenden Begriff.

Definition 4.21 Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann nennt man $N_G(U) = \{g \in G \mid gUg^{-1} = U\}$ den ***Normalisator*** von U in G.

Die Bedeutung des Normalisators wird durch die folgende Proposition deutlich.

Proposition 4.22 Sei G eine Gruppe und U eine Untergruppe. Dann ist $N_G(U)$ die größte Untergruppe H von G mit der Eigenschaft, dass U Normalteiler von H ist.

Beweis: Die Untergruppen-Eigenschaft von $N_G(U)$ haben wir in den Übungen nachgewiesen; wir werden sie später im Kapitel über Gruppenoperationen noch einmal auf einem anderen Weg herleiten. Für jedes $g \in N_G(U)$ gilt $gUg^{-1} = U$ nach Definition von $N_G(U)$. Dies zeigt, dass $U \trianglelefteq N_G(U)$ ist. Sei nun H eine beliebige Untergruppe von G mit der Eigenschaft $U \trianglelefteq H$. Für jedes $h \in H$ gilt dann $hUh^{-1} = U$ und somit $h \in N_G(U)$. Also ist H tatsächlich in $N_G(U)$ enthalten. □

Sei $n \in \mathbb{N}$ mit $n \geq 3$. In § 1 hatten wir die Bezeichnung ρ für die $\frac{2\pi}{n}$-Drehung um den Punkt $(0,0)$ und τ für die Spiegelung an der x-Achse eingführt. Wie man leicht überprüft, gilt $\mathrm{ord}(\rho) = n$ und $\mathrm{ord}(\tau) = 2$. Nach Folgerung 3.4 gilt für die erzeugten zyklischen Untergruppen somit $\langle\rho\rangle = \{\rho^k \mid 0 \leq k < n\}$ und $\langle\tau\rangle = \{\tau^0, \tau^1\}$. Das Komplexprodukt dieser beiden zyklischen Untergruppen von $\mathcal{O}(2)$ ist somit gegeben durch

$$\langle\rho\rangle\langle\tau\rangle \quad = \quad \{\rho \mid 0 \leq k < n\} \cup \{\rho^k\tau \mid 0 \leq k < n\} \quad ;$$

dies sind genau die in § 1 angegebenen Elemente. Um zu zeigen, dass das Komplexprodukt eine Untergruppe von $\mathcal{O}(2)$ ist, genügt es nach Lemma 4.20 zu überprüfen, dass $\langle\rho\rangle$ ein Normalteiler von $\langle\rho,\tau\rangle$ ist. Dazu wiederum reicht es nach Proposition 4.22 nachzuweisen, dass ρ und τ beide im Normalisator $N_{\langle\rho,\tau\rangle}(\langle\rho\rangle)$ enthalten sind, denn daraus folgt, dass $\langle\rho,\tau\rangle$ mit dem Normalisator übereinstimmt. Das Element ρ ist wegen $\rho \in \langle\rho\rangle$ offensichtlich im Normalisator enthalten. Für τ verwenden wir die aus § 1 bekannte Gleichung $\tau\rho^{-k}\tau = \rho^k$ für $0 \leq k < n$, die wegen $\tau = \tau^{-1}$ zu $\tau\rho^k\tau^{-1} = \rho^{-k}$ umgeformt werden kann. Diese zeigt, dass $\tau\langle\rho\rangle\tau^{-1}$ mit $\langle\rho\rangle$ übereinstimmt und τ somit auch im Normalisator enthalten ist.

Als weitere Anwendungen des Komplexprodukts führen wir die folgenden Begriffe ein.

Definition 4.23 Sei G eine Gruppe, und seien U, N Untergruppen von G. Wir bezeichnen G als ***inneres direktes Produkt*** von U und N, wenn U und N beides Normalteiler von G sind und $G = UN$ sowie $U \cap N = \{e\}$ gilt. Ist lediglich N eine Normalteiler von G, aber nicht notwendigerweise die Untergruppe U, dann spricht man von einem inneren ***semidirekten*** Produkt.

Die inneren semidirekten Produkte werden wir erst später genauer untersuchen. Die wesentliche Motivation für die Einführung der inneren direkten Produkte besteht in der Verbindung zu den äußeren direkten Produkten der Form $G \times H$, die wir bereits in § 1 definiert haben.

Proposition 4.24 Sei G eine Gruppe und inneres direktes Produkt ihrer Untergruppen U und N. Dann gilt $G \cong U \times N$.

Beweis: Wir zeigen zunächst, dass für alle $u \in U$ und $n \in N$ die Gleichung $un = nu$ erfüllt ist. Wir beweisen die äquivalente Gleichung $unu^{-1}n^{-1} = e$. Weil N ein Normalteiler von G ist, gilt $unu^{-1} \in N$, und somit liegt auch $unu^{-1}n^{-1}$ in N. Andererseits ist auch U ein Normalteiler von G. Es folgt $nu^{-1}n^{-1} \in U$ und $unu^{-1}n^{-1} \in U$. Insgesamt gilt also $unu^{-1}n^{-1} \in U \cap N = \{e\}$, also $unu^{-1}n^{-1} = e$.

Nun zeigen wir, dass durch die Abbildung $\phi : U \times N \to G$, $(u,n) \mapsto un$ ein Isomorphismus von Gruppen definiert ist. Zum Nachweis der Homomorphismus-Eigenschaft seien $(u_1,n_1),(u_2,n_2) \in U \times N$ vorgegeben. Durch Anwendung der zu Beginn bewiesenen Gleichung $u_1n_2 = n_2u_1$ erhalten wir

$$\begin{aligned}\phi(u_1,n_1)\phi(u_2,n_2) &= (u_1n_1)(u_2n_2) = u_1(n_1u_2)n_2 = u_1(u_2n_1)n_2 = \\ (u_1u_2)(n_1n_2) &= \phi(u_1u_2,n_1n_2) = \phi((u_1,n_1)(u_2,n_2)).\end{aligned}$$

Jedes $g \in G$ kann als Produkt $g = un$ mit $u \in U$ und $n \in N$ dargestellt werden. Dies beweist die Surjektivität von ϕ, und die Eindeutigkeit der Darstellung folgt direkt aus Teil (i) von Lemma 4.20. □

Wir bemerken noch, dass die Bijektivität der Abbildung $U \times N \to UN$, $(u,n) \mapsto un$ auch dann noch gegeben ist, wenn U und N nur Untergruppen, aber keine Normalteiler von G sind. Auch dies ist eine direkte Folgerung aus Teil (i) von Lemma 4.20. Sind U und N insbesondere *endliche* Untergruppen von G mit $U \cap N = \{e\}$, dann gilt also $|UN| = |U| \cdot |N|$.

Sei G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Existiert ein weiterer Normalteiler U von G mit $G = NU$ und $N \cap U = \{e_G\}$, dann kann, wie wir soeben gesehen haben, die Gruppe G in die Bestandteile N und U „zerlegt“ werden. Aber auch, wenn ein solcher Normalteiler U nicht existiert, ist eine Zurückführung der Struktur von G auf „einfachere“ Bestandteile möglich.

Hier kommen die sog. Faktorgruppen ins Spiel. Für die Definition der Verknüpfung auf diesen Gruppen wiederholen wir einen wichtigen, bereits aus der Linearen Algebra bekannten, Satz.

Satz 4.25 Seien X und Y Mengen und sei $\equiv$ eine Äquivalenzrelation auf X.

(i) Ist $f : X \to Y$ eine Abbildung mit der Eigenschaft, dass für alle $x, x' \in X$ aus $x \equiv x'$ jeweils $f(x) = f(x')$ gilt, dann existiert eine eindeutig bestimmte Abbildung $\bar{f} : X/\equiv \to Y$ mit $\bar{f}([x]) = f(x)$ für alle $x \in X$.

(ii) Ist $g : X \times X \to Y$ eine Abbildung mit der Eigenschaft, dass für alle $x, x' \in X$ und $y, y' \in X$ aus $x \equiv x'$ und $y \equiv y'$ jeweils $g(x,y) = g(x',y')$ folgt, dann existiert eine eindeutig bestimmte Abbildung $\bar{g} : (X/\equiv) \times (X/\equiv) \to Y$ mit $\bar{g}([x],[y]) = g(x,y)$ für alle $x, y \in X$

Man nennt $\bar{f}$ bzw. $\bar{g}$ die durch f bzw. g ***induzierte*** Abbildung.

Beweis: Die Eindeutigkeit von $\bar{f}$ und $\bar{g}$ ist jeweils offensichtlich, denn durch die angegebenen Bedingungen sind $\bar{f}$ und $\bar{g}$ auf ihrem Definitionsbereich eindeutig festgelegt. Zum Nachweis der Existenz verwenden wir ein Repräsentantensystem $R \subseteq X$ der Äquivalenzklassen. Für jedes $x \in X$ sei $x_R \in R$ jeweils das eindeutig bestimmte Element

in der Äquivalenzklasse von x. Dann definieren wir $\bar{f}$ und $\bar{g}$ durch $\bar{f}([x]) = f(x_R)$ und $\bar{g}([x],[y]) = g(x_R, y_R)$. (Diese Definitionen sind eindeutig auf Grund der Tatsache, dass x_R und y_R jeweils nur von den Äquivalenzklassen $[x],[y] \in X/\equiv$ abhängen, nicht aber von der Wahl der Elemente x und y innerhalb ihrer jeweiligen Klasse.) Auf Grund unserer Voraussetzungen an die Abbildungen f und g gilt für alle $x, y \in X$ jeweils $f(x_R) = f(x)$ und $g(x_R, y_R) = g(x, y)$, insgesamt also $\bar{f}([x]) = f(x)$ und $\bar{g}([x],[y]) = g(x, y)$ wie gefordert. □

Die Gültigkeit des Satzes ist keineswegs so selbstverständlich, wie es auf den ersten Blick erscheint. Beispielsweise existiert *keine* Abbildung $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ mit $f(a+3\mathbb{Z}) = a+4\mathbb{Z}$ für alle $a \in \mathbb{Z}$. Denn aus der Existenz einer solchen Abbildung würde sich auf Grund der Gleichung $2+3\mathbb{Z} = 5+3\mathbb{Z}$ in $\mathbb{Z}/3\mathbb{Z}$ die Gleichung $2+4\mathbb{Z} = f(2+3\mathbb{Z}) = f(5+3\mathbb{Z}) = 5+4\mathbb{Z}$ ergeben, im Widerspruch zu $5+4\mathbb{Z} = 1+4\mathbb{Z} \neq 2+4\mathbb{Z}$.

Proposition 4.26 Sei G eine Gruppe und N ein Normalteiler von G. Dann gibt es auf der Menge G/N eine eindeutig bestimmte Verknüpfung $\cdot$ mit der Eigenschaft

$$(gN)\cdot(hN) \quad = \quad (gh)N \qquad \text{für alle} \quad g,h \in G.$$

Beweis: Dies erhält man unmittelbar durch Anwendung von Satz 4.25 (ii) auf die Relation $\equiv_\ell$ gegeben durch $g \equiv_\ell g' \Leftrightarrow g' \in gN$ für alle $g, g' \in G$ und auf die Abbildung $G \times G \to G/N$, $(g,h) \mapsto (gh)N$. Die Voraussetzungen des Satzes sind erfüllt, denn sind $g, g', h, h' \in G$ mit $g \equiv_\ell g'$ und $h \equiv_\ell h'$ vorgegeben, dann gibt es Element $n_1, n_2 \in N$ mit $g' = gn_1$ und $h' = hn_2$. Auf Grund der Normalteiler-Eigenschaft ist $n' = h^{-1}n_1h$ in N enthalten. Stellen wir diese Gleichung zu $n_1h = hn'$ um, so erhalten wir $g'h' = (gn_1)(hn_2) = (gh)n'n_2 \in (gh)N$ und somit $g'h' \equiv_\ell gh$. □

Man kann übrigens zeigen, dass für eine beliebige Untergruppe U die Existenz einer Verknüpfung $\cdot$ auf der Menge G/U mit $(gU)\cdot(hU) = (gh)U$ äquivalent zur Normalteiler-Eigenschaft von U ist. Den Beweis dieser Aussage sehen wir uns in den Übungen an.

Um die soeben bewiesene Proposition zu illustrieren, betrachten wir als Beispiel die Gruppe $G = S_3$ und die Untergruppe $N = \langle(1\ 2\ 3)\rangle$. Dann besteht die Menge G/N der Linksnebenklassen aus den beiden Elementen

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

Wegen $(G : N) = 2$ ist N ein Normalteiler von G. Für die soeben definierte Verknüpfung $\cdot$ auf G/N gilt beispielsweise $(\mathrm{id}\ N)\cdot((1\ 2)N) = (\mathrm{id} \circ (1\ 2))N = (1\ 2)N$ und $((1\ 2)N)\cdot((1\ 2)N) = ((1\ 2)\circ(1\ 2)) = \mathrm{id}\ N$. Insgesamt ist die Verknüpfungstabelle von $\cdot$ gegeben durch

$\cdot$	id N	$(1\ 2)N$
id N	id N	$(1\ 2)N$
$(1\ 2)\ N$	$(1\ 2)N$	id N

Stellt man die Nebenklasse $(1\ 2)N$ durch andere Repräsentanten dar, so liefert die Verknüpfung $\cdot$ dennoch dasselbe Ergebnis. Beispielsweise gilt $(1\ 2)N = (2\ 3)N = (1\ 3)N$, und man erhält entsprechend $((2\ 3)N)\cdot((1\ 3)N) = ((2\ 3)\circ(1\ 3))N = (1\ 2\ 3)N = N$. Als nächstes zeigen wir nun, dass die Verknüpfung $\cdot$ auf der Menge G/N eine Gruppenstruktur definiert.

Satz 4.27 Sei G eine Gruppe und N ein Normalteiler. Dann ist die Menge G/N der Linksnebenklassen mit der Verknüpfung $gN \cdot hN = (gh)N$ eine Gruppe, die sogenannte ***Faktorgruppe*** von G modulo N. Die Abbildung $\pi_N : G \to G/N$, $g \mapsto gN$ ist ein Epimorphismus von Gruppen, der sog. ***kanonische Epimorphismus***.

Beweis: Wir müssen für die gegebene Verknüpfung die Gruppenaxiome überprüfen. Zum Nachweis der Assoziativität seien $g_1, g_2, g_3 \in G$ vorgegeben. Dann gilt

$$(g_1N \cdot g_2N) \cdot g_3N = (g_1g_2)N \cdot g_3N = ((g_1g_2)g_3)N = (g_1(g_2g_3))N =$$
$$g_1N \cdot (g_2g_3)N = g_1N \cdot (g_2N \cdot g_3N).$$

Die Nebenklasse $\bar{e} = e_GN = N$ übernimmt die Rolle des Neutralelements, denn für alle $g \in G$ gilt $gN \cdot e_GN = (ge_G)N = gN$ und $e_GN \cdot gN = (e_Gg)N = gN$. Außerdem gilt $gN \cdot g^{-1}N = (gg^{-1})N = e_GN = \bar{e}$ und ebenso $g^{-1}N \cdot gN = e_GN = \bar{e}$, also ist $g^{-1}N$ das zu gN inverse Element in G/N.

Überprüfen wir nun die angegebenen Eigenschaften der Abbildung π_N. Für alle $g, g' \in G$ gilt $\pi_N(gg') = (gg')N = (gN)(g'N) = \pi_N(g)\pi_N(g')$. Somit ist π_N ein Homomorphismus. Ist $gN \in G/N$ vorgegeben, dann gilt $\pi_N(g) = gN$. Also ist π_N surjektiv. □

Wie wir bereits wissen, sind Homomorphismen nicht nur mit der Gruppenverknüpfung, sondern auch mit der Potenzierung von Elementen verträglich. Damit können wir eine naheliegende Potenzierungsregel für Elemente in Faktorgruppen herleiten: Für $g \in G$ und $n \in \mathbb{Z}$ gilt $(gN)^n = \pi_N(g)^n = \pi_N(g^n) = (g^n)N$.

Ein wichtiges Beispiel für Faktorgruppen sind die bereits bekannten ***Restklassengruppen***. Sei $G = (\mathbb{Z}, +)$, $n \in \mathbb{N}$ und $U = \langle n \rangle = n\mathbb{Z}$. Dann sind die Elemente von $G/U = \mathbb{Z}/n\mathbb{Z}$ die schon zuvor erwähnten Restklassen der Form $a + n\mathbb{Z}$ mit $a \in \mathbb{Z}$. Wir bemerken noch, dass jede zyklische Grupper der Ordnung n isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$ ist. Dies ergibt sich unmittelbar aus Folgerung 4.13.

Für viele Anwendungen ist es nützlich, Faktorgruppen mit anderen, möglicherweise „natürlicher“ erscheinenden Gruppen zu identifizieren. Das zentrale Hilfsmittel dazu ist der Homomorphiesatz, dem wir uns nun zuwenden.

Proposition 4.28 Sei $\phi : G \to H$ ein Gruppen-Homomorphismus und $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \ker(\phi)$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\bar{\phi} : G/N \to H$ mit

$$\bar{\phi}(gN) = \phi(g) \qquad \text{für alle } g \in G.$$

Man nennt $\bar{\phi}$ den durch ϕ ***induzierten*** Homomorphismus.

Beweis: Die Eindeutigkeit von $\bar{\phi}$ ist klar, weil durch die Gleichung die Bilder aller Elemente von G/N festgelegt sind. Zum Beweis der Existenz wenden wir wiederum Satz 4.25 an, diesmal Teil (i). Demnach genügt es zu zeigen, dass für alle $g, g' \in G$ mit $g \equiv_\ell g'$ jeweils $\phi(g) = \phi(g')$ gilt. Aber dies ist der Fall, denn $g \equiv_\ell g'$ ist nach Definition äquivalent zu $g' \in gN$, was wiederum mit $(g')^{-1}g \in N$ gleichbedeutend ist. Wegen $N \subseteq \ker(\phi)$ folgt daraus $\phi(g')^{-1}\phi(g) = \phi((g')^{-1}g) = e_H$ und somit $\phi(g) = \phi(g')$. Nun überprüfen wir noch, dass $\bar{\phi}$ ein Homomorphismus ist. Seien $\bar{g}$, $\bar{h} \in G/N$ und $g, h \in G$ mit $\bar{g} = gN$ und $\bar{h} = hN$. Dann gilt $\bar{\phi}(\bar{g}\bar{h}) = \bar{\phi}((gN)(hN)) = \bar{\phi}((gh)N) = \phi(gh) = \phi(g)\phi(h) = \bar{\phi}(gN)\bar{\phi}(hN) = \bar{\phi}(\bar{g})\bar{\phi}(\bar{h})$. □

Satz 4.29 *(Homomorphiesatz für Gruppen)*
Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus

$$\bar{\phi} : G/\ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi).$$

Ist der Homomorphismus ϕ surjektiv, dann erhält man also einen Isomorphismus $G/\ker(\phi) \cong H$.

Beweis: Nach Satz 4.18 (iii) ist $N = \ker(\phi)$ ein Normalteiler von G. Anwendung von Proposition 4.28 auf diesen Normalteiler liefert einen von ϕ induzierten Homomorphismus $\bar{\phi} : G/N \to H$. Auf Grund der Gleichung $\bar{\phi}(gN) = \phi(g)$ für alle $g \in G$ stimmen $\mathrm{im}(\phi)$ und $\mathrm{im}(\bar{\phi})$ überein. Wir können $\bar{\phi}$ somit als *surjektiven* Homomorphismus $G/N \to \mathrm{im}(\phi)$ auffassen. Zusätzlich ist $\bar{\phi}$ injektiv. Ist nämlich $\bar{g} \in \ker(\bar{\phi})$, $\bar{g} = gN$ mit $g \in N$, dann gilt $\phi(g) = \bar{\phi}(\bar{g}) = e_H$. Es folgt $g \in \ker(\phi)$, also $g \in N$, und damit ist $\bar{g} = gN = e_G N = \bar{e}$ das Neutralelement in G/N. Es gilt also $\ker(\bar{\phi}) = \{\bar{e}\}$. Nach Proposition 4.9 folgt daraus die Injektivität von $\bar{\phi}$. □

Wir betrachten nun eine Reihe von Anwendungsbeispielen für den Homomorphiesatz.

(i) Sei G eine Gruppe und $\phi : G \to \{e_G\}$ gegeben durch $g \mapsto e_G$ für alle $g \in G$. Dann ist $\mathrm{im} = \{e_G\}$, und ϕ induziert einen Isomorphismus $G/G \cong \{e_G\}$.

(ii) Die identische Abbildung $\mathrm{id}_G : G \to G$ hat den Kern $\{e_G\}$ und die gesamte Gruppe G als Bild. Sie induziert also einen Isomorphismus $G/\{e_G\} \cong G$.

(iii) Sei K ein Körper und $n \in \mathbb{N}$. Der Determinanten-Homomorphismus $\det : \mathrm{GL}_n(K) \to K^\times$ besitzt, wie wir in § 2 gesehen haben, die Gruppe $\mathrm{SL}_n(K)$ als Kern. Außerdem ist sie surjektiv, denn für jedes $a \in K^\times$ gibt es eine invertierbare Matrix mit Determinante a, beispielsweise die Diagonalmatrix mit den Einträgen $a, 1, ..., 1$. Somit liefert der Homomorphiesatz einen Isomorphismus $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^\times$.

(iv) Die Signumsfunktion $\mathrm{sgn} : S_n \to \{\pm 1\}$ hat als Kern die Untergruppe $A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$, die bereits aus der Linearen Algebra bekannte alternierende Gruppe. Außerdem ist sie für $n \geq 2$ surjektiv, wegen $\mathrm{sgn}(\mathrm{id}) = 1$ und $\mathrm{sgn}((1\ 2)) = -1$. Also induziert sgn einen Isomorphismus $S_n/A_n \cong \{\pm 1\}$.

Eine wichtige Anwendung der Faktorgruppen besteht darin, dass sie in vielen Fällen das Studium der Untergruppen einer Gruppe G vereinfachen. Ist nämlich $N \trianglelefteq G$, dann korrespondieren die Untergruppen von G/N, wie wir gleich sehen werden, zu bestimmten Untergruppen der Gruppe G. Dies ist der Inhalt des Korrespondenzsatzes, den wir als nächstes beweisen werden. Da G/N in der Regel eine einfachere Struktur als G besitzt, lassen sich die Untergruppen dort im allgemeinen leichter bestimmen.

Proposition 4.30 Sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $\pi_N : G \to G/N$ der kanonische Epimorphismus.

(i) Ist U eine Untergruppe von G, dann gilt $\pi_N^{-1}(\pi_N(U)) = UN$.

(ii) Ist $\bar{U}$ eine Untergrupe von G/N, dann gilt $\pi_N(\pi_N^{-1}(\bar{U})) = \bar{U}$.

Beweis: zu (i) Sei $g \in \pi_N^{-1}(\pi_N(U))$. Dann liegt $\pi_N(g)$ in $\pi_N(U)$, es gibt also ein $u \in U$ mit $\pi_N(g) = \pi_N(u)$. Für das Element $n = u^{-1}g$ gilt $nN = \pi_N(n) = \pi_N(u)^{-1}\pi_N(g) = \bar{e} = N$, also ist $nN = N$ und insbesondere $n \in N$. Es

folgt $g = un \in UN$. Ist umgekehrt $g \in UN$, dann gibt es Elemente $u \in U$ und $n \in N$ mit $g = un$. Wir erhalten $\pi_N(g) = \pi_N(un) = \pi_N(u)\pi_N(n) = \pi_N(u)\bar{e} = \pi_N(u)$, und es folgt $g \in \pi_N^{-1}(\pi_N(U))$.

zu (ii) Die Inklusion $\pi_N(\pi_N^{-1}(\bar{U})) \subseteq \bar{U}$ folgt unmittelbar aus der Definition von Bild- und Urbildmenge. Für die umgekehrte Inklusion sei $\bar{g} \in \bar{U}$ vorgegeben und $g \in G$ mit $gN = \bar{g}$. Dann gilt $\pi_N(g) = \bar{g}$ und somit $g \in \pi_N^{-1}(\bar{U})$ nach Definition der Urbildmenge $\pi_N^{-1}(\bar{U})$. Es folgt $\bar{g} = \pi_N(g) \in \pi_N(\pi_N^{-1}(\bar{U}))$. □

Satz 4.31 *(Korrespondenzsatz für Gruppen)*

Sei G eine Gruppe, N ein Normalteiler, $\bar{G} = G/N$ und $\pi_N : G \to \bar{G}$ der kanonische Epimorphismus. Ferner sei $\bar{\mathcal{G}}$ die Menge der Untergruppen von $\bar{G}$ und $\mathcal{G}_N$ die Menge der Untergruppen U von G mit $U \supseteq N$. Dann sind die beiden Abbildungen

$$\mathcal{G}_N \longrightarrow \bar{\mathcal{G}}\ ,\ U \mapsto \pi_N(U) \qquad \text{und} \qquad \bar{\mathcal{G}} \longrightarrow \mathcal{G}_N\ ,\ \bar{U} \mapsto \pi_N^{-1}(\bar{U})$$

bijektiv und zueinander invers. Außerdem gilt:

(i) Für $U, V \in \mathcal{G}_N$ gilt $U \subseteq V$ genau dann, wenn $\pi_N(U) \subseteq \pi_N(V)$ erfüllt ist.

(ii) Genau dann ist $U \in \mathcal{G}_N$ ein Normalteiler von G, wenn $\pi_N(U)$ ein Normalteiler von $\bar{G}$ ist.

(iii) Ist $U \in \mathcal{G}_N$ von endlichem Index in G und $\bar{U} = \pi_N(U)$, dann gilt $(G : U) = (\bar{G} : \bar{U})$.

Beweis: Sei $U \in \mathcal{G}_N$, also eine Untergruppe von G mit $U \supseteq N$. Dann gilt $\pi_N^{-1}(\pi_N(U)) = UN = NU = U$, wobei wir im ersten Schritt Proposition 4.30 (i), im zweiten Lemma 4.20 (iii) und im dritten Lemma 4.20 (ii) verwendet haben. Umgekehrt liefert Teil (ii) von Proposition 4.30 die Gleichung $\pi_N(\pi_N^{-1}(\bar{U})) = \bar{U}$ für alle Untergruppen $\bar{U}$ von $\bar{G}$.

zu (i) Seien $U, V \in \mathcal{G}_N$ mit $U \subseteq V$. Dann gilt offenbar $\pi_N(U) \subseteq \pi_N(V)$. Ist umgekehrt $\pi_N(U) \subseteq \pi_N(V)$ vorausgesetzt, dann folgt $U = \pi_N^{-1}(\pi_N(U)) \subseteq \pi_N^{-1}(\pi_N(V)) = V$.

zu (ii) Weil der kanonische Homomorphismus π_N surjektiv ist, folgen „⇒“ bzw. „⇐“ aus Satz 4.18 (iv) bzw. (iii).

zu (iii) Wir zeigen, dass durch $\bar{g}\bar{U} \mapsto \pi_N^{-1}(\bar{g}\bar{U})$ eine Bijektion zwischen den Linksnebenklassen von $\bar{U}$ und den Linksnebenklassen von U gegeben ist. Sei $\bar{g} \in \bar{G}$ und $g \in G$ ein Element mit $\pi_N(g) = \bar{g}$. Dann gilt $gU = \pi_N^{-1}(\bar{g}\bar{U})$. Ist nämlich $gu \in gU$ mit $u \in U$ vorgegeben, dann folgt $\pi_N(gu) = \pi_N(g)\pi_N(u) = \bar{g}\pi_N(u) \in \bar{g}\bar{U}$ und somit $gu \in \pi_N^{-1}(\bar{g}\bar{U})$. Ist umgekehrt $h \in \pi_N^{-1}(\bar{g}\bar{U})$ vorgegeben, dann folgt $\pi_N(h) \in \bar{g}\bar{U}$, also $\pi_N(h) = \bar{g}\bar{u}$ für ein $\bar{u} \in \bar{U}$. Bezeichnet $u \in U$ ein Urbild von $\bar{u}$, dann gilt also $hN = guN$. Es gibt also ein $n \in N$ mit $h = gun$, und wegen $U \supseteq N$ folgt $h \in gU$.

Es ist unmittelbar klar, dass die Zuordnung surjektiv ist, denn jede Nebenklasse von U hat die Form gU mit einem $g \in G$, und folglich ist $gU = \pi_N^{-1}(\bar{g}\bar{U})$ mit $\bar{g} = \pi_N(g)$. Auch die Injektivität ist offensichtlich. Sind nämlich $\bar{g}_1\bar{U}$ und $\bar{g}_2\bar{U}$ zwei verschiedene Nebenklassen in $\bar{G}/\bar{U}$, dann sind sie als Teilmengen von $\bar{G}$ disjunkt. Die Urbildmengen $\pi_N^{-1}(\bar{g}_1\bar{U})$ und $\pi_N^{-1}(\bar{g}_2\bar{U})$ müssen dann erst recht disjunkt sein, und insbesondere voneinander verschieden. □

Wir verwenden nun den Korrespondenzsatz für Gruppen, um alle Untergruppen von $(\mathbb{Z}, +)$ zu bestimmen, die die Untergruppe $\langle 44 \rangle$ enthalten. Sei $\pi_{\langle 44 \rangle} : \mathbb{Z} \to \mathbb{Z}/44\mathbb{Z}$ der kanonische Epimorphismus. Die Gruppe $(\mathbb{Z}/44\mathbb{Z}, +)$ ist eine zyklische Gruppe der Ordnung 44. Durch Satz 3.11 haben wir eine vollständige Beschreibung der Untergruppen von $(\mathbb{Z}/44\mathbb{Z}, +)$ zur Verfügung: Zu jedem Teiler der Gruppenordnung 44 gibt es eine eindeutig bestimmte Untergruppe, und diese werden erzeugt durch gewisse Potenzen des Erzeugers $\bar{1}$ von $\mathbb{Z}/44\mathbb{Z}$. Die vollständige Liste der

Untergruppen ist also gegeben durch

$$\langle\bar{1}\rangle\ ,\ \langle\bar{2}\rangle\ ,\ \langle\bar{4}\rangle\ ,\ \langle\overline{11}\rangle\ ,\ \langle\overline{22}\rangle\ ,\ \langle\overline{44}\rangle = \{\bar{0}\}.$$

Der Korrespondenzsatz besagt nun, dass es korrespondierend zu diesen sechs Untergruppen von $\mathbb{Z}/44\mathbb{Z}$ genau sechs Untergruppen von $(\mathbb{Z},+)$ gibt, die $\langle 44\rangle$ enthalten. Offenbar ist $\langle 44\rangle$ in $\langle a\rangle$ enthalten für die Zahlen $a \in \{1,2,4,11,22,44\}$, denn jedes ganzzahlige Vielfache von 44 ist auch ein Vielfaches von a für jede Zahl a in dieser Menge. Der Korrespondenzsatz liefert uns die Information, dass es keine weiteren Untergruppen U von $(\mathbb{Z},+)$ mit $U \supseteq \langle 44\rangle$ gibt.

Auch die folgenden beiden Sätze, mit denen wir dieses Kapitel abschließen, erweisen sich beim Umgang mit Faktorgruppen immer wieder als nützlich.

Satz 4.32 *(Isomorphiesätze)*

Sei G eine Gruppe, $N \trianglelefteq G$ und U eine Untergruppe von G.

(i) Dann ist $N \cap U$ ein Normalteiler von U, und es gilt $U/(N \cap U) \cong (UN)/N$.

(ii) Ist auch $U \trianglelefteq G$ und gilt $U \supseteq N$, dann gilt $G/U \cong (G/N)/(U/N)$.

Beweis: zu (i) Zunächst bemerken wir, dass UN nach Lemma 4.20 eine Untergruppe von G ist, und aus $N \trianglelefteq G$ folgt $N \trianglelefteq UN$. Wir wenden nun den Homomorphiesatz, Satz 4.29, an auf den Homomorphismus $\phi : U \to (UN)/N$, $u \mapsto uN$ der durch Komposition der Inklusionsabbildung $U \hookrightarrow G$ mit dem kanonischen Epimorphismus π_N zu Stande kommt. Diese Abbildung ist surjektiv, denn jedes Element in $(UN)/N$ hat die Form $(un)N$ mit $u \in U$ und $n \in N$. Wegen $u^{-1}(un) = n \in N$ gilt $(un)N = uN$, und es folgt $\phi(u) = uN = (un)N$. Der Kern von ϕ ist genau die Untergrupe $N \cap U$, denn für alle $u \in U$ gilt die Äquivalenz

$$u \in \ker(\phi) \quad\Leftrightarrow\quad \phi(u) = N \quad\Leftrightarrow\quad uN = N \quad\Leftrightarrow\quad u \in N \quad\Leftrightarrow\quad u \in N \cap U.$$

Also liefert der Homomorphiesatz tatsächlich den angegebenen Isomorphismus.

zu (ii) Nach Definition gilt $U/N = \pi_N(U)$ mit dem kanonischen Epimorphismus $\pi_N : G \to G/N$. Aus $U \trianglelefteq G$ und Satz 4.18 (iv) folgt somit, dass U/N ein Normalteiler von G/N ist. Wir wenden nun den Homomorphiesatz auf die Abbildung $\psi : G \to (G/N)/(U/N)$, $g \mapsto gN(U/N)$ an, die durch Hintereinanderschaltung der beiden Epimorphismen π_N und $\pi_{U/N}$ zu Stande kommt. Als Komposition zweier Epimorphismen ist auch ψ ein Epimorphismus. Damit der Homomorphiesatz das gewünschte Ergebnis liefert, müssen wir noch zeigen, dass $\ker(\psi) = U$ gilt. Tatsächlich gilt für alle $g \in G$ die Äquivalenz

$$g \in \ker(\psi) \quad\Leftrightarrow\quad \psi(g) = U/N \quad\Leftrightarrow\quad gN(U/N) = U/N \quad\Leftrightarrow\quad gN \in U/N \quad\Leftrightarrow\quad \exists\, u \in U : gN = uN \quad\Leftrightarrow$$

$$\exists\, u \in U : g^{-1}u \in N \quad\Leftrightarrow\quad \exists\, u \in U, n \in N : g^{-1}u = n \quad\Leftrightarrow\quad \exists\, u \in U, n \in N : g = un^{-1} \quad\overset{U \supseteq N}{\Leftrightarrow}\quad g \in U. \qquad \square$$

In Teil (ii) von Satz 4.32 werden tatsächlich Faktorgruppen von Faktorgruppen gebildet, ein auf den ersten Blick etwas unanschaulicher Vorgang. Wir illustrieren diese Aussage deshalb anhand eines Beispiels. Sei $G = (\mathbb{Z}, +)$. Weil G abelsch ist, sind die Untergruppen $N = \langle 6 \rangle$ und $U = \langle 2 \rangle$ Normalteiler von G, und wegen $6 = 3 \cdot 2 \in U$ gilt $N \subseteq U$. Das Bild von U unter dem kanonischen Epimorphismus besteht aus allen Vielfachen von $\bar{2} = 2 + 6\mathbb{Z}$, ist also durch $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ gegeben. Der zweite Isomorphiesatz liefert uns somit

$$\mathbb{Z}/2\mathbb{Z} \quad = \quad G/U \quad \cong \quad (G/N)/(U/N) \quad \cong \quad (\mathbb{Z}/6\mathbb{Z})/\langle \bar{2} \rangle.$$

Nach demselben Schema zeigt man leicht: Sind $m, n \in \mathbb{N}$ und ist m ein Teiler von n, dann gilt $\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/\langle \bar{m} \rangle$, mit $\bar{m} = m + n\mathbb{Z}$.

§ 5. *Endlich erzeugte abelsche Gruppen*

Zusammenfassung. In diesem Kapitel werden wir mit Hilfe der bisher entwickelten theoretischen Werkzeuge alle endlich erzeugten abelschen Gruppen bis auf Isomorphie bestimmen. Genauer zeigen wir, dass jede solche Gruppe isomorph zu einem äußeren direkten Produkt von (unendlichen und endlichen) zyklischen Gruppe ist. Insbesondere können wir dann für jedes $n \in \mathbb{N}$ eine endliche Liste $G_1, ..., G_r$ von Gruppen angeben, so dass jede abelsche Gruppe der Ordnung n zu einem der G_i isomorph ist. Dies wird am Ende des Kapitels für die Zahl $n = 100$ exemplarisch vorgeführt.

Wichtige Grundbegriffe	*Zentrale Sätze*
– freie endlich erzeugte abelsche Gruppe	– Zerlegung endlich erzeugter abelscher Gruppen in einen freien Anteil und eine endliche abelsche Gruppe
– Torsionsuntergruppen abelscher Gruppen	– Zerlegung endlicher abelscher Gruppen in ein Produkt endlicher zyklischer Gruppen
– torsionfreie abelsche Gruppe	– Chinesischer Restsatz für Gruppen

In § 2 haben wir eine Gruppe G als *endlich erzeugt* bezeichnet, wenn eine endliche Teilmenge $S \subseteq G$ mit $G = \langle S \rangle$ existiert. Im weiteren Verlauf werden wir wiederholt auf die folgende Hilfsaussage zurückgreifen.

Lemma 5.1 Seien G, H beliebige Gruppen. Ist G endlich erzeugt und existiert ein surjektiver Homomorphismus $\phi : G \to H$, dann ist auch H endlich erzeugt.

Beweis: Sei $S = \{g_1, ..., g_r\}$ ein endliches Erzeugendensystem von G. Wir zeigen, dass $\phi(S) = \{\phi(g_1), ..., \phi(g_r)\}$ ein Erzeugendensystem von H ist. Sei dazu U eine beliebige Untergruppe von H, die $\phi(S)$ enthält. Zu zeigen ist $U = H$. Nun ist $\phi^{-1}(U)$ nach Proposition 4.8 eine Untergruppe von G, und diese enthält S als Teilmenge. Wegen $G = \langle S \rangle$ folgt $\phi^{-1}(U) = G$. Aber daraus ergibt sich direkt $U = H$. Ist nämlich $h \in H$, dann existiert auf Grund der Surjektivität von ϕ ein $g \in G$ mit $\phi(g) = h$. Dieses ist zugleich in $\phi^{-1}(U)$ enthalten, und daraus folgt $h = \phi(g) \in U$. □

Von nun an sind alle in diesem Kapitel vorkommenden Gruppen abelsch und werden in additiver Schreibweise dargestellt. Für das Komplexprodukt zweier Teilmengen A, B einer Gruppe G verwenden wir entsprechend die Schreibweise $A + B$ statt AB. Für das innere direkte Produkt verwenden wir hier die folgende Notation: Wir schreiben $G = U \oplus V$, wenn U und V Untergruppen von $(G, +)$ sind und G ein inneres direktes Produkt von U und V ist. Diese Schreibweise ist nur bei abelschen Gruppen üblich. Sie erinnert an die Notation für die direkte Summen von Untervektorräumen eines K-Vektorraums V. Tatsächlich werden wir in diesem Kapitel stellenweise den Vektorraum-Begriff zu Hilfe nehmen.

Definition 5.2 Sei G eine abelsche Gruppe und $m \in \mathbb{N}$.

(i) Man nennt $G[m] = \{g \in G \mid mg = 0_G\}$ die ***m*-Torsionsuntergruppe** von G.

(ii) Die Teilmenge $\mathrm{Tor}(G) = \bigcup_{n \in \mathbb{N}} G[n]$ wird die ***Torsionsuntergruppe*** von G genannt.

Man überprüft leicht, dass sowohl $G[m]$ für jedes $m \in \mathbb{N}$ als auch $\mathrm{Tor}(G)$ tatsächlich Untergruppen von G sind. Denn offenbar ist 0_G sowohl in $G[m]$ als auch in $\mathrm{Tor}(G)$ enthalten. Seien nun $g,h \in G[m]$ vorgegeben. Dann gilt $mg = mh = 0_G$, und es folgt $m(g+h) = mg + mh = 0_G + 0_G = 0_G$ und $m(-g) = -(mg) = -0_G = 0_G$. Dies zeigt, dass auch $g+h$ und $-g$ in $G[m]$ liegen. Also ist $G[m]$ tatsächlich eine Untergruppe von G. Zum Nachweis der Untergruppen-Eigenschaft von $\mathrm{Tor}(G)$ seien nun $g,h \in \mathrm{Tor}(G)$. Dann gibt es nach Definition $m,n \in \mathbb{N}$ mit $g \in G[m]$ und $h \in G[n]$, also $mg = 0_G$ und $nh = 0_G$. Es folgt $(mn)g = n(mg) = n0_G = 0_G$ und $(mn)h = m(nh) = m0_G = 0_G$, also $g,h \in G[mn]$. Wie soeben gezeigt, sind damit auch $g+h$ und $-g$ in $G[mn]$ enthalten, und damit erst recht in $\mathrm{Tor}(G)$. Also ist auch $\mathrm{Tor}(G)$ eine Untergruppe von G. Man beachte aber, dass für eine nicht-abelsche Gruppe G die Teilmenge $\{g \in G \mid g^m = e_G\}$ im Allgemeinen keine Untergruppe von G ist!

Definition 5.3 Sei G eine endlich erzeugte abelsche Gruppe.

(i) Wir bezeichnen G als ***torsionsfrei***, wenn $\mathrm{Tor}(G) = \{0_G\}$ gilt.

(ii) Die Gruppe G ist ***frei***, wenn für ein $r \in \mathbb{N}_0$ ein Isomorphismus zwischen G und $(\mathbb{Z}^r,+)$ existiert, wobei $\mathbb{Z}^0 = \{0\}$ gesetzt wird.

Wie man unmittelbar überprüft, ist jede freie endlich erzeugte abelsche Gruppe auch torsionsfrei. Unser erstes Ziel in diesem Abschnitt ist der Nachweis, dass jede endlich erzeugte abelsche Gruppe als äußeres direktes Produkt einer freien endlich erzeugten abelschen Gruppe und einer endlichen abelschen Gruppe dargestellt werden kann.

Proposition 5.4

(i) Jede Untergruppe einer freien endlich erzeugten abelschen Gruppe ist eine freie endlich erzeugte abelsche Gruppe.

(ii) Jede torsionsfreie endlich erzeugte abelsche Grupe ist frei.

Beweis: zu (i) Da jede endlich erzeugte freie abelsche Gruppe nach Definition isomorph zu $\mathbb{Z}^n$ für ein $n \in \mathbb{N}_0$ ist, genügt es, die Aussage für Gruppen dieser Form zu beweisen. Wir zeigen durch vollständige Induktion über $n \in \mathbb{N}_0$: Ist U eine Untergruppe von $\mathbb{Z}^n$, dann ist U eine freie endlich erzeugte abelsche Gruppe. Für $n = 0$ ist $\mathbb{Z}^n = U = \{0\}$ und die Aussage somit offensichtlich. Für $n = 1$ können wir Satz 3.7 anwenden, weil $(\mathbb{Z},+)$ zyklisch ist. Die Untergruppe U stimmt demnach mit $m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$ überein. Sie ist also selbst entweder unendlich zyklisch oder trivial, also isomorph zu $\mathbb{Z}^1$ oder $\mathbb{Z}^0$.

Sei nun $n \geq 1$, und setzen wir voraus, dass die Aussage für Untergruppen von $\mathbb{Z}^n$ gültig ist. Sei U eine Untergruppe von $\mathbb{Z}^{n+1}$ und $\pi : \mathbb{Z}^{n+1} \to \mathbb{Z}$ die Projektionsabbildung auf die letzte Komponente, also gegeben durch $(a_1,\ldots,a_{n+1}) \mapsto a_{n+1}$. Nach Definition gilt $\ker(\pi) = \mathbb{Z}^n \times \{0\} \cong \mathbb{Z}^n$, also ist $\ker(\pi|_U) = \ker(\pi) \cap U$ isomorph zu einer Untergruppe von $\mathbb{Z}^n$. Nach Induktionsvoraussetzung ist $\ker(\pi|_U)$ ebenfalls eine freie endlich erzeugte abelsche Gruppe und somit isomorph zu $\mathbb{Z}^r$ für ein $r \in \mathbb{N}_0$.

Das Bild $\pi(U)$ ist eine Untergruppe von $\mathbb{Z}$ und somit, wie zu Beginn gezeigt, entweder gleich $\{0\}$ oder gleich $m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Im Fall $\pi(U) = \{0\}$ gilt $U = \ker(\pi|_U) \cong \mathbb{Z}^r$, und wir sind fertig. Betrachten wir nun den Fall $\pi(U) = m\mathbb{Z}$ mit $m \in \mathbb{N}$. Wählen wir ein $v \in U$ mit $\pi(v) = m$, dann wird die Untergruppe $\langle v \rangle$ von U isomorph auf $m\mathbb{Z}$ abgebildet.

Wir überprüfen nun, dass U ein inneres direktes Produkt von $\ker(\pi|_U)$ und $\langle v\rangle$ ist. Zunächst einmal sind $\ker(\pi|_U)$ und $\langle v\rangle$ als Untergruppen der abelschen Gruppe U Normalteiler von U. Außerdem gilt $\ker(\pi|_U)\cap\langle v\rangle = \{0_{\mathbb{Z}^{n+1}}\}$. Ist nämlich w ein Element im Durchschnitt, dann gilt $w = kv$ für ein $k\in\mathbb{Z}$. Darüber hinaus gilt $km = k\pi(v) = \pi(kv) = (\pi|_U)(w) = 0$, und somit $k = 0$ und $w = kv = 0_{\mathbb{Z}^{n+1}}$.

Für den Nachweis von $U = \ker(\pi|_U)+\langle v\rangle$ stellen wir zunächst fest, dass „$\supseteq$“ wegen $\ker(\pi|_U)\subseteq U$ und $v\in U$ offenbar erfüllt ist. Zum Beweis von „$\subseteq$“ sei $w\in U$ vorgegeben. Wegen $\pi(U) = m\mathbb{Z}$ gilt $\pi(w) = km$ für ein $k\in\mathbb{Z}$. Setzen wir nun $w' = w-kv$, dann erhalten wir $w = w'+kv$ mit $kv\in\langle v\rangle$ und $(\pi|_U)(w') = \pi(w') = \pi(w)-k\pi(v) = km-km = 0$, also $w'\in\ker(\pi|_U)$. Damit ist $w\in\ker(\pi|_U)+\langle v\rangle$ nachgewiesen. Insgesamt sind damit die Voraussetzungen von Proposition 4.24 erfüllt, und wir erhalten $U\cong\ker(\pi|_U)\times\pi(U)\cong\mathbb{Z}^r\times m\mathbb{Z}\cong\mathbb{Z}^r\times\mathbb{Z} = \mathbb{Z}^{r+1}$.

zu (ii) Sei G eine torsionsfreie endlich erzeugte abelsche Gruppe. Weiter sei S ein endliches Erzeugendensystem und $T = \{g_1,\dots,g_n\}\subseteq S$ eine *maximale* Teilmenge von S mit der Eigenschaft, dass die Abbildung $\phi : \mathbb{Z}^n\to G$, $(a_1,\dots,a_n)\mapsto a_1g_1+\dots+a_ng_n$ injektiv ist. Dann ist die Untergruppe $U = \langle T\rangle$ von G frei, denn als Abbildung $\mathbb{Z}^n\to U$ ist ϕ auch surjektiv, die Gruppe U also isomorph zu $\mathbb{Z}^n$.

Nun sei $g\in S\setminus T$ ein beliebiges Element. Auf Grund der Torsionsfreiheit gilt $ag\neq 0_G$ für alle $a\in\mathbb{Z}$, $a\neq 0$. Wegen der Maximalität von T finden wir aber einen Satz $(a,a_1,\dots,a_n)$ ganzer Zahlen mit $ag+a_1g_1+\dots+a_ng_n = 0_G$ und $a\neq 0$, $a_i\neq 0$ für ein $i\in\{1,\dots,n\}$. Wegen $ag = -a_1g_1-\dots-a_ng_n$ ist dann ag in U enthalten. Auf diese Weise erhalten wir für jedes $g\in S$ ein $a_g\in\mathbb{Z}$ mit $a_gg\in U$, wobei wir im Fall $g\in T$ jeweils $a_g = 1$ setzen können. Weil S endlich ist, können wir das kleinste gemeinsame Vielfache dieser Zahlen bilden und finden so ein $a\in\mathbb{N}$ mit $aS\subseteq U$. Wegen $G = \langle S\rangle$ gilt dann auch $aG\subseteq U$. Nun ist $\psi : G\to G$, $g\mapsto ag$ ein (auf Grund der Torsionsfreiheit) injektiver Homomorphismus, dessen Bild $\psi(G)$ in der freien abelschen Gruppe U enthalten ist. Nach Teil (i) ist $G\cong\psi(G)$ damit selbst eine freie, endlich erzeugte abelsche Gruppe. □

Satz 5.5 Ist G eine endlich erzeugte abelsche Gruppe, dann gilt $G\cong\mathbb{Z}^r\times\mathrm{Tor}(G)$ für ein $r\in\mathbb{N}_0$. Darüber hinaus ist $\mathrm{Tor}(G)$ eine endliche abelsche Gruppe.

Beweis: Zunächst bemerken wir, dass die Faktorgruppe $G/\mathrm{Tor}(G)$ eine torsionsfreie endlich erzeugte abelsche Gruppe ist. Zum Beweis sei $\bar g\in\mathrm{Tor}(G/\mathrm{Tor}(G))$ vorgegeben, mit $\bar g = g+\mathrm{Tor}(G)$ für ein $g\in G$. Dann gilt $m\bar g = 0_{G/\mathrm{Tor}(G)}$ für ein $m\in\mathbb{N}$. Es folgt $mg+\mathrm{Tor}(G) = m(g+\mathrm{Tor}(G)) = m\bar g = 0_{G/\mathrm{Tor}(G)} = 0_G+\mathrm{Tor}(G)$ und somit $mg\in\mathrm{Tor}(G)$. Daraus wiederum folgt, dass ein $n\in\mathbb{N}$ mit $(nm)g = n(mg) = 0_G$ existiert. Aber damit ist auch g in $\mathrm{Tor}(G)$ enthalten und $\bar g = g+\mathrm{Tor}(G) = 0+\mathrm{Tor}(G) = 0_{G/\mathrm{Tor}(G)}$. Insgesamt haben wir $\mathrm{Tor}(G/\mathrm{Tor}(G)) = \{0_{G/\mathrm{Tor}(G)}\}$, also die Torsionsfreiheit der Gruppe $G/\mathrm{Tor}(G)$, nachgewiesen.

Weil $G/\mathrm{Tor}(G)$ torsionsfrei ist, gilt $G/\mathrm{Tor}(G)\cong\mathbb{Z}^r$ für ein $r\in\mathbb{N}_0$, nach Proposition 5.4 (ii). Sei ϕ die Komposition des kanonischen Epimorphismus $G\to G/\mathrm{Tor}(G)$ mit diesem Isomorphismus, seien $v_1,\dots,v_r$ Urbilder der Einheitsvektoren $e_1,\dots,e_r\in\mathbb{Z}^r$ unter ϕ, und sei $U = \langle v_1,\dots,v_r\rangle$. Wir zeigen, dass $G = U\oplus\mathrm{Tor}(G)$ gilt. Weil G abelsch und U und $\mathrm{Tor}(G)$ Untergruppen von G sind, handelt es sich um Normalteiler. Zum Nachweis von $U\cap\mathrm{Tor}(G) = \{0_G\}$ sei g ein Element im Durchschnitt. Wegen $g\in\mathrm{Tor}(G)$ gilt $mg = 0_G$ für ein $m\in\mathbb{N}$. Wegen $g\in U$ gibt es außerdem $k_1,\dots,k_r\in\mathbb{Z}$ mit $g = k_1v_1+\dots+k_rv_r$. Es folgt $mg = mk_1v_1+\dots+mk_rv_r$ und $0_{\mathbb{Z}^r} = \phi(mg) = mk_1e_1+\dots+mk_re_r = (mk_1,\dots,mk_r)$. Es gilt also $mk_i = 0$ und somit auch $k_i = 0$ für $1\le i\le r$, und dies wiederum bedeutet $g = 0_G$. Für den Nachweis von $G = U+\mathrm{Tor}(G)$ sei $g\in G$ vorgegeben. Sei $(k_1,\dots,k_r) = \phi(g)$, $h = k_1v_1+\dots+k_rv_r$ und $g' = g-h$. Dann ist $g = g'+h$, $h\in U$ und $\phi(g') = \phi(g)-\phi(h) = (k_1,\dots,k_r)-(k_1,\dots,k_r) = 0_{\mathbb{Z}^r}$, also $g'\in\ker(\phi)$. Aber der Kern von

ϕ stimmt mit dem Kern des kanonischen Epimorphismus $G \to G/\mathrm{Tor}(G)$ überein, und dies ist $\mathrm{Tor}(G)$. Also ist g' in $\mathrm{Tor}(G)$ enthalten. Also liegt $g = h + g'$ in $U + \mathrm{Tor}(G)$.

Insgesamt ist $G = U + \mathrm{Tor}(G)$ damit nachgewiesen. Mit Proposition 4.24 erhalten wir $G \cong U \times \mathrm{Tor}(G)$. Wie man leicht überprüft, ist die Abbildung $\phi|_U : U \to \mathbb{Z}^r$ surjektiv (denn wegen $\phi(v_i) = e_i$ werden alle Einheitsvektoren getroffen) und injektiv (denn das einzige Urbild von $0_{\mathbb{Z}^r}$ ist 0_G), außerdem ein Homomorphismus. Es gilt also $U \cong \mathbb{Z}^r$. Damit ist $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$ gezeigt. Die Gruppe $\mathrm{Tor}(G)$ ist offenbar abelsch, außerdem ist sie als Bild von G unter dem surjektiven Homomorphismus $G \to \mathrm{Tor}(G)$, der durch Komposition von $G \cong U \times \mathrm{Tor}(G)$ mit der Projektion auf die zweite Komponente zu Stande kommt, nach Lemma 5.1 endlich erzeugt. Sei $\{h_1, ..., h_s\}$ ein endliches Erzeugendensystem von $\mathrm{Tor}(G)$. Wegen $h_i \in \mathrm{Tor}(G)$ gibt es jeweils ein $m_i \in \mathbb{N}$ mit $m_i h_i = 0_G$, für $1 \le i \le s$. Wegen Lemma 3.2 folgt jeweils $\langle h_i \rangle = \{kh_i \mid 0 \le k < m_i\}$. Zusammen mit Satz 2.9 (ii) erhalten wir

$$\mathrm{Tor}(G) \quad = \quad \{k_1h_1 + ... + k_sh_s \mid k_1, ..., k_s \in \mathbb{Z}\} \quad = \quad \{k_1h_1 + ... + k_sh_s \mid 0 \le k_i < m_i\}.$$

Es gibt in $\mathrm{Tor}(G)$ also höchstens $\prod_{i=1}^{s} m_i$ verschiedene Elemente. Insbesondere ist $\mathrm{Tor}(G)$ endlich. □

Wir werden nun zeigen, dass jede endliche abelsche Gruppe in ein äußeres direktes Produkt endlicher *zyklischer* Gruppen zerlegt werden kann. In der Linearen Algebra wurde gezeigt, dass $\mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p ein Körper ist, und die Bezeichnung $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für diesen Körper eingeführt.

Lemma 5.6

(i) Sei G eine abelsche Gruppe, seien $s \in \mathbb{N}_0$, $m_1, ..., m_s \in \mathbb{N}$ und $g_1, ..., g_s \in G$ mit $\mathrm{ord}(g_i) \mid m_i$ für $1 \le i \le s$. Sei $U = \langle g_1, ..., g_s \rangle$. Dann gibt es einen surjektiven Gruppenhomomorphismus $\phi : \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_s\mathbb{Z} \to U$ mit

$$\phi(\bar{a}_1, ..., \bar{a}_s) \quad = \quad a_1g_1 + ... + a_sg_s \qquad \text{für alle} \quad a_1, ..., a_s \in \mathbb{Z}.$$

(ii) Ist G eine abelsche Gruppe mit $G[p] = G$, dann gibt es eine Abbildung $\cdot : \mathbb{F}_p \times G \to G$ mit $\bar{a} \cdot g = ag$ für alle $a \in \mathbb{Z}$ und $g \in G$. Mit dieser Abbildung wird auf G die Struktur eines $\mathbb{F}_p$-Vektorraums definiert.

Beweis: zu (i) Wir definieren die Abbildung ϕ, indem wir $\phi(\bar{a}_1, ..., \bar{a}_s) = a_1g_1 + ... + a_rg_r$ für $0 \le a_i < m_i$ setzen. Die Gleichung ist dann automatisch für beliebige $a_i \in \mathbb{Z}$ erfüllt. Wenden wir nämlich Division mit Rest auf jedes a_i an und schreiben $a_i = q_im_i + r_i$ mit $0 \le r_i < m_i$, dann gilt auf Grund der Elementordnungen jeweils $m_ig_i = 0_G$ und somit $a_ig_i = (q_im_i + r_i)g_i = q_i(m_ig_i) + r_ia_i = q_i \cdot 0_G + r_ia_i = r_ia_i$. Wegen $\bar{a}_i = \bar{r}_i$ in $\mathbb{Z}/m_i\mathbb{Z}$ für $1 \le i \le r$ folgt dann $\phi(\bar{a}_1, ..., \bar{a}_r) = \phi(\bar{r}_1, ..., \bar{r}_s) = r_1g_1 + ... + r_sg_s = a_1g_1 + ... + a_sg_s$. Mit Hilfe dieser Gleichung kann die Homomorphismus-Eigenschaft nun unmittelbar nachgerechnet werden. Nach Satz 2.9 gilt $U = \{a_1g_1 + ... + a_sg_s \mid a_1, ..., a_s \in \mathbb{Z}\}$. Damit ist auch klar, dass ϕ surjektiv ist.

zu (ii) Die Existenz einer solchen Abbildung erhalten wir, indem wir (i) für jedes $g \in G$ auf $s = 1$, $m_1 = p$ und $g = g_1$ anwenden. Wir zeigen nun, dass $(U, +, \cdot)$ die Vektorraum-Axiome erfüllt. Nach Definition ist $(U, +)$ eine abelsche Gruppe. Seien nun $\bar{a}, \bar{b} \in \mathbb{F}_p$ und $g, h \in G$ vorgegeben, und seien $a, b \in \mathbb{Z}$ Urbilder von $\bar{a}, \bar{b}$ unter dem kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{F}_p$. Dann gilt $(\bar{a} + \bar{b}) \cdot g = \overline{a+b} \cdot g = (a+b)g = ag + bg = \bar{a} \cdot g + \bar{b} \cdot g$, $\bar{a} \cdot (g + h) = a(g + h) = ag + ah = \bar{a} \cdot g + \bar{a} \cdot h$, $(\bar{a}\bar{b}) \cdot g = \overline{ab} \cdot g = abg = a(bg) = \bar{a} \cdot (\bar{b} \cdot g)$ und $\bar{1} \cdot g = 1g = g$. □

Satz 5.7 Sei G eine abelsche Gruppe.

(i) Sind $m, n \in \mathbb{N}$ teilerfremd, dann gilt $G[mn] \cong G[m] \times G[n]$.

(ii) Sei $n \in \mathbb{N}$ mit $G[n] = G$, und sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_r$ und Exponenten $e_1, ..., e_r \in \mathbb{N}$. Dann ist $G \cong G[p_1^{e_1}] \times ... \times G[p_r^{e_r}]$.

Beweis: zu (i) Wegen Proposition 4.24 genügt es, $G[mn] = G[m] \oplus G[n]$ nachzuweisen. Offenbar gilt $G[m] \subseteq G[mn]$, denn ist $g \in G[m]$, dann folgt $mg = 0_G$, damit auch $(mn)g = n(mg) = n0_G = 0_G$ und somit $g \in G[mn]$. Ebenso erhält man $G[n] \subseteq G[mn]$, und als Untergruppen der abelschen Gruppe G sind $G[m]$ und $G[n]$ auch Normalteiler. Zum Nachweis von $G[m] \cap G[n] = \{0_G\}$ sei $g \in G[m] \cap G[n]$ vorgegeben. Dann gilt $mg = ng = 0_G$, also ist $\mathrm{ord}(g)$ ein gemeinsamer Teiler von m und n. Auf Grund der Teilerfremdheit von m und n folgt $\mathrm{ord}(g) = 1$, also $g = 0_G$. Daraus folgt $G[m] \cap G[n] \subseteq \{0_G\}$; die Inklusion „$\supseteq$“ ist offensichtlich. Es bleibt $G[mn] = G[m] + G[n]$ zu zeigen. Die Inklusion „$\supseteq$“ folgt direkt aus $G[m] \subseteq G[mn]$ und $G[n] \subseteq G[mn]$. Zum Nachweis von „$\subseteq$“ sei $g \in G[mn]$. Nach dem Lemma 3.8 von Bézout gibt es $k, \ell \in \mathbb{Z}$ mit $km + \ell n = 1$. Es folgt $g = 1g = (km)g + (\ell n)g$. Wegen $n(km)g = k(mn)g = k0_G = 0_G$ liegt $(km)g$ in $G[n]$, und wegen $m(\ell n)g = \ell(mn)g = \ell 0_G = 0_G$ ist $(\ell n)g$ in $G[m]$ enthalten. Damit ist $g = (km)g + (\ell n)g \in G[m] + G[n]$ nachgewiesen.

zum (ii) Wir schicken voraus: Ist G eine abelsche Gruppe und sind $m, n \in \mathbb{N}$ mit $m \mid n$, dann gilt $G[m] = G[n][m]$. Nun beweisen wir die Aussage durch vollständige Induktion über die Anzahl r der verschiedenen Primfaktoren p_i von n. Im Fall $r \in \{0, 1\}$ braucht nichts gezeigt werden. Sei nun $r > 1$, und setzen wir die Aussage für kleinere Werte von r voraus. Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n. Setzen wir $m = \prod_{i=1}^{r-1} p_i^{e_i}$, dann gilt $n = mp_r^{e_r}$ und $\mathrm{ggT}(m, p_r^{e_r}) = 1$. Die Untergruppe $H = G[m]$ erfüllt $H[m] = H$. Wir können also die Induktionsvoraussetzung auf H anwenden; diese liefert einen Isomorphismus $H \cong H[p_1^{e_1}] \times ... \times H[p_{r-1}^{e_{r-1}}] \cong G[p_1^{e_1}] \times ... \times G[p_{r-1}^{e_{r-1}}]$. Nach Teil (i) gilt außerdem $G = G[n] \cong H \times G[p_r^{e_r}]$. Insgesamt erhalten wir somit den angegebenen Isomorphismus. □

Als weiteres Hilfsmittel benötigen wir

Satz 5.8 *(Chinesischer Restsatz für Gruppen)*
Sind $m, n \in \mathbb{N}$ teilerfremd, dann existiert ein Isomorphismus $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ abelscher Gruppen.

Beweis: Die Anwendung von Satz 5.7 auf $G = G[mn] = \mathbb{Z}/(mn)\mathbb{Z}$ liefert $G \cong G[m] \times G[n]$. Dabei ist $G[m] = \langle n + (mn)\mathbb{Z} \rangle$. Denn wegen $m \cdot (n + (mn)\mathbb{Z}) = 0_{\mathbb{Z}/(mn)\mathbb{Z}}$ ist einerseits $n + (mn)\mathbb{Z}$ in $G[m]$ enthalten, woraus sich die Inklusion „$\supseteq$“ ergibt. Ist andererseits $a + (mn)\mathbb{Z} \in G[m]$ vorgegeben, mit $a \in \mathbb{Z}$, dann folgt aus $ma + (mn)\mathbb{Z} = 0_{\mathbb{Z}/(mn)\mathbb{Z}} = (mn)\mathbb{Z}$ unmittelbar $ma \in (mn)\mathbb{Z}$, und daraus wiederum, dass a ein Vielfaches von n ist, also $a = rn$ für ein $r \in \mathbb{Z}$ und $a + (mn)\mathbb{Z} = r(n + (mn)\mathbb{Z}) \in \langle n + (mn)\mathbb{Z} \rangle$ gilt. Weil $1 + (mn)\mathbb{Z}$ ein Element der Ordnung mn ist, ist $n + (mn)\mathbb{Z} = n \cdot (1 + (mn)\mathbb{Z})$ ein Element der Ordnung m nach Satz 3.9 (ii), und somit $G[m] \cong \mathbb{Z}/m\mathbb{Z}$. Ebenso zeigt man $G[n] \cong \mathbb{Z}/n\mathbb{Z}$, und insgesamt erhalten wir $G \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

Wir werden im Kapitel über Kongruenzrechnng zeigen, dass $\mathbb{Z}/(mn)\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sogar als Ringe isomorph sind; dies liefert insbesondere einen Isomorphismus zwischen den abelschen Gruppen. Man beachte aber, dass der

Chinesische Restsatz nur für teilerfremde $m, n \in \mathbb{N}$ gültig ist! Beispielsweise ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$. Denn $\mathbb{Z}/4\mathbb{Z}$ enthält mit $\bar{1}$ ein Element der Ordnung 4, während die Gleichung $2 \cdot (\bar{a}, \bar{b}) = (\bar{0}, \bar{0})$ für alle $(\bar{a}, \bar{b}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ zeigt, dass es in dieser Gruppe nur Elemente der Ordnung 1 und 2 gibt.

Satz 5.9 Sei $e \in \mathbb{N}_0$, p eine Primzahl und G eine endliche abelsche Gruppe mit $G[p^e] = G$. Dann gibt es ein $r \in N_0$ und $n_1, ..., n_r \in \mathbb{N}$, so dass

$$G \quad \cong \quad \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \qquad \text{gilt.}$$

Beweis: Wir beweisen die Aussage durch vollständige Induktion über e. Ist $e = 0$, dann gilt $G[1] = G$, also $g = 1 \cdot g = 0_G$ für alle $g \in G$. Es folgt $G = \{0_G\}$, und die Behauptung ist offenbar mit $r = 0$ erfüllt. Sei nun $e \geq 1$, und setzen wir die Aussage für Werte kleiner als e voraus. Für die Gruppe $H = pG$ gilt $H[p^{e-1}] = H$. Nach Induktionsvoraussetzung gibt es $r \in \mathbb{N}_0$, $n_1, ..., n_r$ und einen Isomorphismus $\phi : \mathbb{Z}/p^{n_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \to H$. Seien $h_1, h_2, ..., h_r \in H$ die Bilder der Elemente

$$(\bar{1}, \bar{0}, \bar{0}, ..., \bar{0}) \quad , \quad (\bar{0}, \bar{1}, \bar{0}, ..., \bar{0}) \quad , \quad ... \quad , \quad (\bar{0}, \bar{0}, \bar{0}, ..., \bar{1}).$$

Wegen $h_i \in pG$ gibt es jeweils ein $g_i \in G$ mit $pg_i = h_i$, für $1 \leq i \leq r$. Wir zeigen nun zunächst, dass die Gruppe $U = \langle g_1, ..., g_r \rangle$ isomorph zu $\mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z}$ ist. Dazu betrachten wir die Abbildung

$$\psi : \mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \to U \quad , \quad (\bar{a}_1, ...\bar{a}_r) \mapsto a_1 g_1 + ... + a_r g_r.$$

Nach Lemma 5.6 (i) ist dies ein surjektiver Gruppenhomomorphismus. Außerdem ist die Abbildung injektiv. Gilt nämlich $\psi(\bar{a}_1, ..., \bar{a}_r) = 0_G$ und ist $a_i \in \mathbb{Z}$ jeweils ein Urbild von $\bar{a}_i$, dann ist $a_1 g_1 + ... + a_r g_r = 0_G$ nach Definition von ψ. Es folgt $\phi(a_1 + p^{n_1}\mathbb{Z}, ..., a_r + p^{n_r}\mathbb{Z}) = a_1 h_1 + ... + a_r h_r = p(a_1 g_1 + ... + a_r g_r) = p0_G = 0_G$. Weil ϕ injektiv ist, erhalten wir $a_i + p^{n_i}\mathbb{Z} = 0 + p^{n_i}\mathbb{Z}$ und $p^{n_i} \mid a_i$, für $1 \leq i \leq r$. Insbesondere gibt es jeweils ein $b_i \in \mathbb{Z}$ mit $pb_i = a_i$. Nun folgt weiter $\phi(b_1 + p^{n_1}\mathbb{Z}, ..., b_r + p^{n_r}\mathbb{Z}) = b_1 h_1 + ... + b_r h_r = pb_1 g_1 + ... + pb_r g_r = a_1 g_1 + ... + a_r g_r = 0_G$. Wiederum auf Grund der Injektivität von ϕ erhalten wir $b_i + p^{n_i}\mathbb{Z} = 0 + p^{n_i}\mathbb{Z}$, also $p^{n_i} \mid b_i$ und $p^{n_i+1} \mid a_i$ für $1 \leq i \leq r$. Dies wiederum bedeutet $(\bar{a}_1, ..., \bar{a}_r) = (\bar{0}, ..., \bar{0})$. Insgesamt ist ψ also tatsächlich ein Isomorphismus.

Nach Lemma 5.6 (ii) besitzen $G[p] \cap U$ und $G[p]$ jeweils die Struktur eines $\mathbb{F}_p$-Vektorraums. Dabei ist $G[p] \cap U$ als Untergruppe offenbar auch ein Untervektorraum von $G[p]$. Wir wählen nun eine Basis $\{v_1, ..., v_s\}$ von $G[p] \cap U$ und ergänzen diese durch $v_{s+1}, ..., v_t$ (mit $s, t \in \mathbb{N}_0$ und $s \leq t$) zu einer Basis von $G[p]$. Anschließend definieren wir $V = \langle v_{s+1}, ..., v_t \rangle$. Als $(t-s)$-dimensionaler $\mathbb{F}_p$-Vektorraum ist V isomorph zu $\mathbb{F}_p^{t-s}$. Als abelsche Gruppe ist V damit isomorph zu $\mathbb{F}_p^{t-s} = (\mathbb{Z}/p\mathbb{Z})^{t-s}$. Wenn wir zeigen können, dass $G = U \oplus V$ gilt, dann folgt $G \cong U \times V \cong \mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^{t-s}$ nach Proposition 4.24. Damit hat G dann bis auf Isomorphie die im Satz angegebene Form.

Als Untergruppen der abelschen Gruppe G sind U und V auch Normalteiler. Zum Beweis der Gleichung $U \cap V = \{0_G\}$ sei $g \in U \cap V$ vorgegeben. Wegen $V \subseteq G[p]$ liegt g dann in $(G[p] \cap U) \cap V$. Wäre g ungleich Null, dann könnte man g als nichttriviale $\mathbb{F}_p$-Linearkombination der Basis $\{v_1, ..., v_s\}$ von $G[p] \cap U$ darstellen, und $-g$ als nichttriviale $\mathbb{F}_p$-Linearkombination der Basis $\{v_{s+1}, ..., v_t\}$ von V. Insgesamt würde man eine nichttriviale Linearkombination von $g + (-g) = 0_G$ durch $\{v_1, ..., v_t\}$ erhalten. Aber dies steht im Widerspruch zur linearen Unabhängigkeit dieser Menge. Also ist nur $g = 0_G$ möglich. Nun zeigen wir noch $G = U + V$. Sei dazu $g \in G$ beliebig vorgegeben. Dann liegt pg in

pG, und folglich gibt es $k_1, ..., k_r \in \mathbb{Z}$ mit $pg = k_1h_1 + ... + k_rh_r$. Setzen wir $g' = k_1g_1 + ... + k_rg_r$ und $g'' = g - g'$, dann gilt $g' \in U$ und $pg'' = pg - pg' = pg - pk_1g_1 - ... - pk_rg_r = k_1h_1 + ... + k_rh_r - k_1h_1 - ... - k_rh_r = 0_G$, also $g'' \in G[p]$. Weil $\{v_1, ..., v_t\}$ eine Basis von $G[p]$ als $\mathbb{F}_p$-Vektorraum ist, kann g'' in der Form $\ell_1v_1 + ... + \ell_tv_t$ geschrieben werden, mit $\ell_1, ..., \ell_t \in \mathbb{Z}$. Es ist dann $g'' = g_1 + g_2$ mit $g_1 = \ell_1v_1 + ... + \ell_sv_s \in U$ und $g_2 = \ell_{s+1}v_{s+1} + ... + \ell_tv_t \in V$. Insgesamt hat g also die Form $g = g' + g'' = (g' + g_1) + g_2$ mit $g' + g_1 \in U$ und $g_2 \in V$. □

Wir können nun das Hauptergebnis dieses Kapitels formulieren.

Satz 5.10 *(Hauptsatz über endlich erzeugte abelsche Gruppe)*
Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, s \in \mathbb{N}_0$ und $d_1, ..., d_s \in \mathbb{N}$ mit

$$G \quad \cong \quad \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}.$$

Dabei können die Zahlen d_i so gewählt werden, dass sie entweder (i) alle Primzahlpotenzen sind oder (ii) $d_i \mid d_{i+1}$ für $1 \leq i < s$ erfüllt ist. Im Fall (ii) gezeichnet man die Zahlen d_i als ***Elementarteiler*** der abelschen Gruppe.

Beweis: Nach Satz 5.5 gilt $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$, und die Gruppe $\mathrm{Tor}(G)$ ist endlich. Setzen wir $H = \mathrm{Tor}(G)$ und $n = |H|$, dann gilt $H[n] = n$. Ist $n = \ prod_{i=1}^{t} p_i^{e_i}$, dann gilt $H \cong H[p_1^{e_1}] \times ... \times H[p_r^{e_r}]$ nach Satz 5.7 (ii), und wegen Satz 5.9 ist $H[p_i^{e_i}]$ jeweils isomorph zu einem äußeres direktes Produkt zyklischer Gruppen von p_i-Potenzordnung. Also ist G insgesamt isomorph zu einem äußeren direkten Produkt der Form (i).

Im Ringtheorie-Teil der Vorlesung wird der Begriff des ***Exponenten*** $\exp(G)$ einer Gruppe G eingeführt und gezeigt, dass der Exponent einer Gruppe, die zu $\mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_u\mathbb{Z}$ mit $m_1, ..., m_u \in \mathbb{N}$ isomorph ist, mit dem kgV von $m_1, ..., m_u$ übereinstimmt. Wir beweisen durch vollständige Induktion über $|H|$, dass G auch eine Zerlegung der unter (ii) beschriebenen Form besitzt, und setzen $d = \exp(H)$. Sei $H \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_u\mathbb{Z}$ die Darstellung nach (i) von H als äußeres direktes Produkt zyklischer Gruppe von Primzahlpotenzordnung m_i.

Im Fall $|H| = 1$ ist nichts zu zeigen. Setzen wir nun voraus, dass H nicht trival ist, und sei $p_1^{f_1} \cdot ... \cdot p_v^{f_v}$ die Primfaktorzerlegung von d. Wegen $\mathrm{kgV}(m_1, ..., m_u) = d$ müssen die Faktoren $p_1^{f_1}, ..., p_v^{f_v}$ unter $m_1, ..., m_u$ vorkommen, andererseits darf es aber keine höheren Potenzen von $p_1, ..., p_v$ unter diesen Zahlen geben. Setzen wir $H_1 = \mathbb{Z}/p_1^{f_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_v^{f_v}\mathbb{Z}$, dann gilt $H \cong H_1 \times H_2$ bis auf Reihenfolge der Faktoren, wobei in H_2 die Faktoren der Form $\mathbb{Z}/m_i\mathbb{Z}$ zusammengefasst sind, die in H, aber nicht in H_1 vorkommen. Es gilt dann $|H_2| < |H|$, und nach Induktionsvoraussetzung gibt es Zahlen $d_1, ..., d_s$ mit $H_2 \cong \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}$ und der oben beschriebenen Eigenschaft. Außerdem gilt $H_1 \cong \mathbb{Z}/d\mathbb{Z}$ nach dem Chinesischen Restsatz, Satz 5.8, denn die Zahlen $p_j^{f_j}$ sind paarweise teilerfremd. Weil der Exponent von H_2 ein Teiler von d ist, gilt $d_i \mid d$ für $1 \leq i \leq s$. Setzen wir $d_{s+1} = d$, dann ist $d_1, ..., d_{s+1}$ eine Folge natürlicher Zahlen mit den gewünschten Eigenschaften. □

Sowohl die Bedingung (i) als auch die Bedingung (ii) in Satz 5.10 kann dazu genutzt werden, um zum Beispiel alle abelschen Gruppen der Ordnung $100 = 2^2 5^2$ bis auf Isomorphie anzugeben. Durch (i) erhält man die vier Isomorphietypen

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \quad , \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Andererseits finden wir zur Zahl 100 die Elementarteilerketten 100, 2|50, 5|20 und 10|10, was die Isomorphietypen

$$\mathbb{Z}/100\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z} \quad , \quad \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \quad , \quad \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$

liefert. Mit dem Chinesischen Restsatz überprüft man leicht, dass diese vier Gruppen mit den vier zuvor gefundenen bis auf Isomorphie übereinstimmen.

Zu bemerken ist noch, dass im Fall (ii) der Wert $r+s$ die ***minimale*** Anzahl der Elemente eines Erzeugendensystems von G angibt. Insbesondere gilt $r+s=1$ genau dann, wenn G eine zyklische Gruppe ist. Ist nämlich p ein beliebiger Primteiler von d_1, dann existiert ein Epimorphismus

$$\phi : \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^{r+s} \quad , \quad (a_1, ..., a_r, b_1 + d_1\mathbb{Z}, ..., b_s + d_s\mathbb{Z}) \mapsto (a_1 + p\mathbb{Z}, ..., b_s + p\mathbb{Z}).$$

Sei $g_1, ..., g_t$ ein t-elementiges Erzeugendensystem von G. Dann liefern die Bilder der Elemente in der Gruppe $H = (\mathbb{Z}/p\mathbb{Z})^{r+s}$ ein Erzeugendensystem von H. Dieses Erzeugendensystem ist dann zugleich eine Basis von H als $\mathbb{F}_p$-Vektorraum. Da in einem $(r+s)$-dimensionalen Vektorraum jedes Erzeugendensystem aus mindestens $r+s$ Elementen besteht, muss $t \geq r+s$ gelten. Andererseits besitzt die Gruppe $\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}$ offenbar ein $(r+s)$-elementiges Erzeugendensystem (gegeben durch die Einheitsvektoren), somit auch die Gruppe G.

§ 6. Semidirekte Produkte und Auflösbarkeit

Zusammenfassung. In § 4 hatten wir neben den inneren direkten auch die inneren semidirekten Produkte definiert. Der Isomorphismus $G \cong N \times U$, den wir dort für die inneren direkten Produkte hergeleitet haben, ist für die semidirekten in dieser Form nicht gültig. An die Stelle des äußeren direkten Produkts tritt hier eine neue Gruppe $N \rtimes_\phi U$, die als Menge mit $N \times U$ übereinstimmt, deren Gruppenverknüpfung aber nicht komponentenweise definiert ist, sondern von einem Homomorphismus $\phi : U \to \mathrm{Aut}(N)$ abhängt. Dieses Objekt wird dann als *äußeres semidirektes Produkt* bezeichnet. Das Ziel dieses Abschnitts besteht darin, die Gruppe $N \rtimes_\phi U$ zu definieren und den Zusammenhang mit dem inneren semidirekten Produkt herzustellen.

Aus dem Korrespondenzsatz aus § 4 hatte sich ergeben, dass die Struktur von G/N auch zumindest teilweisen Aufschluss über die Struktur von G selbst gibt, falls N einen Normalteiler von G bezeichnet. Am einfachsten lässt sich die Struktur von G/N untersuchen, wenn es sich um eine *abelsche* Gruppe handelt, was sich an der Ergebnissen von § 5 deutlich gezeigt hatte. Im Allgemeinen lässt sich in einer Gruppe G kein Normalteiler N finden mit der Eigenschaft, dass die Gruppen N und G/N beide abelsch sind. Zumindest aber kann man hoffen, dass dieser Prozess, mit dem man G gewissermaßen in die Gruppen N und G/N „zerlegt“ hat, durch Anwendung auf N und G/N iteriert werden kann, und man auf diese G in endlich vielen Schritte in lauter abelsche „Komponenten“ zerlegen kann. Gruppen, bei denen dies gelingt, werden als *auflösbar* bezeichnet. Der Grund für diese Namensgebung ist ein Zusammenhang zwischen der Auflösbarkeit von Gruppen und der expliziten Lösbarkeit von Polynomgleichungen, den wir später im Rahmen der Galoistheorie erkunden werden.

Wichtige Grundbegriffe

- äußeres semidirektes Produkt zweier Gruppen, gegeben durch einen Homomorphismus
- höhere Kommutatorgruppen $G^{(n)}$ einer Gruppe G
- Auflösbarkeit einer Gruppe

Zentrale Sätze

- Isomorphie zwischen innerem und äußerem semidirekten Produkt
- Charakterisierung auflösbarer Gruppen durch Subnormalreihen
- Kriterium zur Untersuchung der Auflösbarkeit mit Normalteilern

Sei G eine Gruppe, die ein inneres semidirektes Produkt einer Untergruppe U und eines Normalteiler N ist. Solange U nicht auch Normalteiler von G ist, reichen U und N allein leider nicht aus, um die Gruppe G vollständig zu rekonstruieren; man benötigt noch einen Homomorphismus, der diese beiden Gruppen miteinander verbindet. Um was für einen Homomorphismus es dabei geht, sehen wir in der folgenden Proposition.

Proposition 6.1 Sei G eine Gruppe, N ein Normalteiler und U eine Untergruppe von G. Dann ist jedem $u \in U$ durch $\tau_u(n) = unu^{-1}$ ein Automorphismus von N zugeordnet. Die Abbildung $\phi : U \to \mathrm{Aut}(N)$, $u \mapsto \tau_u$ ist ein Homomorphismus von Gruppen.

Beweis: Wegen $N \trianglelefteq G$ gilt $\tau_u(n) = unu^{-1} \in N$ für jedes $n \in N$ und $u \in U$, also definiert τ_u eine Abbildung $N \to N$. Außerdem ist τ_u ein Endomorphismus, denn für alle $n_1, n_2 \in N$ gilt jeweils

$$\tau_u(n_1 n_2) \quad = \quad u(n_1 n_2)u^{-1} \quad = \quad (un_1u^{-1})(un_2u^{-1}) \quad = \quad \tau_u(n_1)\tau_u(n_2).$$

Da durch $n \mapsto u^{-1}nu$ eine Umkehrabbildung von τ_u gegeben ist, handelt es sich bei τ_u sogar um einen Automorphismus von N. Schließlich ist die angegebene Abbildung ϕ ein Homorphismus, denn für $u_1, u_2 \in U$ und $n \in N$ gilt

$$\begin{aligned}\tau_{u_1u_2}(n) &= (u_1u_2)n(u_1u_2)^{-1} = u_1u_2nu_2^{-1}u_1^{-1} = \tau_{u_1}(u_2nu_2^{-1}) \\ &= \tau_{u_1}(\tau_{u_2}(n)) = (\tau_{u_1} \circ \tau_{u_2})(n)\end{aligned}$$

und somit $\phi(u_1u_2) = \tau_{u_1u_2} = \tau_{u_1} \circ \tau_{u_2} = \phi(u_1) \circ \phi(u_2)$. □

Proposition 6.2 Sei G eine Gruppe und inneres semidirektes Produkt von $N \trianglelefteq G$ und $U \leq G$. Unter diesen Voraussetzungen ist G genau dann ein inneres *direktes* Produkt von N und U, wenn $\phi(u) = \mathrm{id}_N$ für alle $u \in U$ gilt, wobei ϕ den Homomorphismus aus Proposition 6.1 bezeichnet.

Beweis: „⇐“ Gilt $\phi(u) = \mathrm{id}_N$ für alle $u \in U$, dann folgt $unu^{-1} = \phi(u)(n) = \mathrm{id}_N(n) = n$ für alle $u \in U$ und $n \in N$. Es folgt $un = nu$ und somit auch $unu^{-1} = n$ für alle $u \in U$ nun $n \in N$. Seien nun $g_1 \in G$ und $u \in U$ vorgegeben. Wegen $G = NU$ gibt es $n_1 \in N$ und $u_1 \in U$ mit $g_1 = n_1u_1$. Wie soeben gezeigt, ist jedes Element aus N mit jedem Element aus U vertauschbar, so auch die Elemente $n_1 \in N$ und $u_1uu_1^{-1} \in U$. Es folgt $g_1ug_1^{-1} = n_1(u_1uu_1^{-1})n_1^{-1} = n_1n_1^{-1}(u_1uu_1^{-1}) = u_1uu_1^{-1} \in U$; damit ist $U \trianglelefteq G$ nachgewiesen.

„⇒“ Ist G ein inneres direktes Produkt von N und U, dann gilt außer $N \trianglelefteq G$ auch $U \trianglelefteq G$. Seien nun $n \in N$ und $u \in U$ beliebig vorgegeben. Wegen $N \trianglelefteq G$ gilt $un^{-1}u^{-1} \in N$ und somit auch $nun^{-1}u^{-1} = n(un^{-1}u^{-1}) \in N$. Wegen $U \trianglelefteq N$ gilt andererseits auch $nun^{-1}u^{-1} = (nun^{-1})u^{-1} \in U$, insgesamt also $nun^{-1}u^{-1} \in N \cap U = \{e_G\}$. Für alle $n \in N$ und $u \in U$ gilt somit $nun^{-1}u^{-1} = e_G$, was zu $nu = un$ und $unu^{-1} = n$ umgeformt werden kann. Es folgt $\phi(u)(n) = unu^{-1} = n = \mathrm{id}_N(n)$ für alle $u \in U$ und $n \in N$. Damit ist $\phi(u) = \mathrm{id}_N$ für alle $u \in U$ nachgewiesen. □

Satz 6.3 Seien U und N Gruppen und $\phi : U \to \mathrm{Aut}(N)$ ein Homomorphismus. Wir definieren auf $N \times U$ eine Verknüpfung $*$ durch

$$(n_1, u_1) * (n_2, u_2) = (n_1\phi(u_1)(n_2), u_1u_2) \quad \text{für } (n_1, u_1), (n_2, u_2) \in N \times U.$$

Dann ist $(N \times U, *)$ eine Gruppe. Man nennt sie das ***äußere semidirekte Produkt*** von N und U und bezeichnet sie mit $N \rtimes_\phi U$.

Beweis: Wir überprüfen für $(N \times U, *)$ die Gruppenaxiome. Zur Verifikation des Assoziativgesetzes seien (n_1, u_1), (n_2, u_2), $(n_3, u_3) \in N \times U$ vorgegeben. Dann gilt $((n_1, u_1) * (n_2, u_2)) * (n_3, u_3) = (n_1\phi(u_1)(n_2), u_1u_2) * (n_3, u_3) = (n_1\phi(u_1)(n_2)\phi(u_1u_2)(n_3), u_1u_2u_3)$ und ebenso

$$\begin{aligned}(n_1, u_1) * ((n_2, u_2) * (n_3, u_3)) &= (n_1, u_1) * (n_2\phi(u_2)(n_3), u_2u_3) = (n_1\phi(u_1)(n_2\phi(u_2)(n_3)), u_1u_2u_3) \\ &= (n_1\phi_1(u_1)(n_2)(\phi(u_1) \circ \phi(u_2))(n_3), u_1u_2u_3) = (n_1\phi(u_1)(n_2)\phi(u_1u_2)(n_3), u_1u_2u_3).\end{aligned}$$

Nun überprüfen wir, dass (e_N, e_U) ein bezüglich $*$ neutrales Element ist. Für jedes $(n, u) \in N \times U$ gilt $(e_N, e_U) * (n, u) = (e_N\phi(e_U)(n), e_Uu) = (e_Nn, e_Uu) = (n, u)$ und $(n, u) * (e_N, e_U) = (n\phi(u)(e_N), ue_U) = (ne_N, ue_U) = (n, u)$. Damit (n_1, u_1)

ein Inverses von (n,u) ist, muss $(n\phi(u)(n_1),uu_1) = (n,u)*(n_1,u_1) = (e_N,e_U)$ gelten, also $u_1 = u^{-1}$ und $\phi(u)(n_1) = n^{-1} \Leftrightarrow n_1 = \phi(u)^{-1}(n^{-1}) = \phi(u^{-1})(n^{-1})$. Dieses Element (n_1,u_1) erfüllt außer $(n,u)*(n_1,u_1) = (e_N,e_U)$ auch die Gleichung

$$\begin{aligned}(n_1,u_1)*(n,u) &= (n_1\phi(u_1)(n),uu_1) = (\phi(u^{-1})(n^{-1})\phi(u^{-1})(n),uu^{-1}) = \\ (\phi(u^{-1})(n^{-1}n),e_U) &= (\phi(u^{-1})(e_N),e_U) = (e_N,e_U) \quad ,\end{aligned}$$

also handelt es sich tatsächlich um das zu (n,u) inverse Element. □

Ist der Homomorphismus ϕ in Satz 6.3 trivial, gilt also $\phi(u) = \mathrm{id}_N$ für alle $u \in U$, dann gilt für die Verknüpfung $(n,u)*(n_1,u_1) = (n\phi(u)(n_1),uu_1) = (n\mathrm{id}_N(n_1),uu_1) = (nn_1,uu_1)$, für alle $(n,u),(n_1,u_1) \in N \times U$. In diesem Fall stimmt das äußere semidirekte Produkt also mit dem äußeren direkten Produkt aus § 1 überein.

Wir illustrieren das Rechnen in semidirekten Produkten an einem Beispiel. Sei $n \in \mathbb{N}$ und $N = \mathbb{Z}/n\mathbb{Z}$ mit dem Automorphismus $\iota : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{a} \mapsto -\bar{a}$. Sei außerdem $U = \mathbb{Z}/2\mathbb{Z}$. Dann ist durch $\bar{0} \mapsto \mathrm{id}_N$ und $\bar{1} \mapsto \iota$ ein Homomorphismus $\phi : U \to \mathrm{Aut}(N)$ definiert. Sei nun $G = N \rtimes_\phi U$, und seien nun $g,h \in$ gegeben durch $g = (\bar{1},\bar{0})$ und $h = (\bar{0},\bar{1})$. Wir zeigen, dass $G = \langle g,h\rangle$ gilt sowie die Gleichungen

$$\mathrm{ord}(g) = n \quad , \quad \mathrm{ord}(h) = 2 \quad \text{und} \quad g*h*g*h = e_G = (\bar{0},\bar{0}).$$

Zunächst gilt für alle $\bar{a},\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ jeweils

$$(\bar{a},\bar{0})*(\bar{b},\bar{0}) = (\bar{a}+\phi(\bar{0})(\bar{b}),\bar{0}+\bar{0}) = (\bar{a}+\mathrm{id}_N(\bar{b}),\bar{0}) = (\bar{a}+\bar{b},\bar{0}).$$

Durch vollständige Induktion folgt $(\bar{1},\bar{0})^m = (\bar{m},\bar{0})$ für alle $m \in \mathbb{N}$. Somit ist n die kleinste natürliche Zahl mit $g^n = (\bar{1},\bar{0})^n = (\bar{0},\bar{0}) = 0_G$, und es folgt $\mathrm{ord}(g) = n$. Ebenso gilt für alle $\bar{c},\bar{d} \in \mathbb{Z}/2\mathbb{Z}$ die Gleichung

$$(\bar{0},\bar{c})*(\bar{0},\bar{d}) = (\bar{0}+\phi(\bar{c})(\bar{0}),\bar{c}+\bar{d}) = (\bar{0}+\bar{0},\bar{c}+\bar{d}) = (\bar{0},\bar{c}+\bar{d}).$$

Also gilt auch $h^m = (\bar{0},\bar{1})^m = (\bar{0},\bar{m})$ für alle $m \in \mathbb{N}$, und wir erhalten $\mathrm{ord}(h) = 2$. Für alle $a,c \in \mathbb{N}$ gilt

$$g^a*h^c = (\bar{a},\bar{0})*(\bar{0},\bar{c}) = (\bar{a}+\phi(\bar{0})(\bar{0}),\bar{0}+\bar{c}) = (\bar{a}+\bar{0},\bar{c}) = (\bar{a},\bar{c}).$$

Jedes Element in G kann also als Produkt der Form g^a*h^c dargestellt werden, mit $a,c \in \mathbb{N}$. Dies beweist die Gleichung $G = \langle g,h\rangle$. Schließlich gilt noch

$$\begin{aligned}g*h*g*h &= (\bar{1},\bar{1})*(\bar{1},\bar{1}) = (\bar{1}+\phi(\bar{1})(\bar{1}),\bar{1}+\bar{1}) = (\bar{1}+\iota(\bar{1}),\bar{0}) \\ &= (\bar{1}+(-\bar{1}),\bar{0}) = (\bar{0},\bar{0}).\end{aligned}$$

Der folgende Satz stellt einen Zusammenhang zwischen dem inneren und äußeren semidirekten Produkten her.

Satz 6.4 Sei G eine Gruppe, U eine Untergruppe und N ein Normalteiler von G. Wir setzen voraus, dass G das innere semidirekte Produkt N und U ist. Definieren wir $\phi : U \to \mathrm{Aut}(N)$ wie in Proposition 6.1, dann ist durch $(n,u) \mapsto nu$ ein Isomorphismus $N \rtimes_\phi U \cong G$ definiert.

Beweis: Die Abbildung $\psi : N \rtimes_\phi U \to G$, $(n,u) \mapsto nu$ ist surjektiv, denn wegen $G = NU$ hat jedes $g \in G$ eine Darstellung $g = nu$ mit $n \in N$ und $u \in U$. Ist $(n,u) \in N \times U$ ein Paar mit $\psi(n,u) = e_G$, dann folgt $nu = e_G$ und $n = u^{-1} \in N \cap U = \{e_G\}$, also $(n,u) = (e_G, e_G)$. Ist ψ ein Homomorphismus, dann ist ψ somit auch injektiv. Es muss also nur noch die Homomorphismus-Eigenschaft nachgewiesen werden.

Seien dazu $(n_1,u_1),(n_2,u_2) \in N \times U$ vorgegeben. Zu zeigen ist $\psi((n_1,u_1)*(n_2,u_2)) = \psi(n_1,u_1)\psi(n_2,u_2)$. Definieren wir wie in Proposition 6.1 den Automorphismus $\tau_{u_1} \in \mathrm{Aut}(N)$ durch $\tau_{u_1}(n) = u_1 n u_1^{-1}$ für $n \in N$, dann ist die rechte Seite der Gleichung gegeben durch

$$\psi(n_1,u_1)\psi(n_2,u_2) \quad = \quad n_1u_1n_2u_2 \quad = \quad n_1u_1n_2u_1^{-1}u_1u_2 \quad = \quad n_1\tau_{u_1}(n_2)u_1u_2 \quad = \quad n_1\phi(u_1)(n_2)u_1u_2$$

und auch für die linke Seite erhalten wir $\psi((n_1,u_1)*(n_2,u_2)) = \psi(n_1\phi(u_1)(n_2),u_1u_2) = n_1\phi(u_1)(n_2)u_1u_2$. □

Die aus § 1 bekannten Diedergruppen liefern ein wichtiges konkretes Beispiel für innere semidirekte Produkte.

> **Proposition 6.5** Für jedes $n \geq 3$ ist die Diedergruppe D_n ein inneres semidirektes Produkt des Normalteilers $N = \langle \rho_n \rangle$ und der Untergruppe $U = \langle \tau \rangle$. Somit ist D_n isomorph zu einem äußeren semidirekten Produkt von zyklischen Gruppen der Ordnung n bzw. 2.

Beweis: In § 4 haben wir gezeigt, dass D_n mit dem Komplexprodukt NU übereinstimmt. Dass τ nicht in N enthalten und der Schnitt von N und $U = \{\mathrm{id}_{\mathbb{R}^2}, \tau\}$ somit nur aus dem Neutralelement besteht, ist ebenfalls bekannt. Ebenfalls wurde an der entsprechenden Stelle von § 4 gezeigt, dass N im Gegensatz zu U nicht nur eine Untergruppe, sondern auch ein Normalteiler von $D_n = \langle \rho_n, \tau \rangle$ ist. Insgesamt liegt also tatsächlich ein inneres semidirektes Produkt vor. Die zweite Teilaussage der Proposition ergibt sich nun direkt aus Satz 6.4 und der Tatsache, dass $\mathrm{ord}(\rho_n) = n$ und $\mathrm{ord}(\tau) = 2$ gilt. □

Man kann zeigen, dass D_n für jedes $n \geq 3$ darüber hinaus zum weiter oben konstruierten äußeren semidirekten Produkt von $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}$ isomorph ist. Kommen wir nun zum zweiten Thema dieses Kapitels, den auflösbaren Gruppen.

> **Definition 6.6** Sei G eine Gruppe. Für beliebige $g,h \in G$ bezeichnet man das Element $[g,h] = ghg^{-1}h^{-1}$ als den ***Kommutator*** von g und h. Bezeichnet $S = \{[g,h] \mid g,h \in G\}$ die Menge aller Kommutoren in G, so wird die Untergruppe $G' = \langle S \rangle$ die ***Kommutatorgruppe*** von G genannt.

Entscheidend für die Nützlichkeit der Kommutatoren ist die Beziehung $gh = [g,h]hg$. Tatsächlich gilt

$$[g,h]hg \quad = \quad (ghg^{-1}h^{-1})hg \quad = \quad ghg^{-1}(h^{-1}h)g \quad = \quad gh(g^{-1}g) \quad = \quad gh$$

für alle $g,h \in G$ ab. Ist G eine abelsche Gruppe, dann gilt stets $[g,h] = ghg^{-1}h^{-1} = (gg^{-1})(hh^{-1}) = e$. Daraus folgt, dass die Kommutatorgruppe in diesem Fall trivial ist, also $G' = \{e\}$ gilt. Im allgemeinen Fall erhält man das folgende wichtige Resultat.

Satz 6.7 Sei G eine Gruppe.

(i) Die Kommutatorgruppe G' ist ein Normalteiler von G.

(ii) Für einen beliebigen Normalteiler N von G gilt $N \supseteq G'$ genau dann, wenn die Faktorgruppe G/N abelsch ist.

Also ist G/G' die größte abelsche Faktorgruppe von G.

Beweis: zu (i) Sei $g_1 \in G$ vorgegeben und S die Menge der Kommutatoren. Es genügt, die Inklusion $S \subseteq g_1^{-1}G'g_1$ nachzuweisen. Denn weil $g_1^{-1}G'g_1$ eine Untergruppe von G ist, folgt daraus $G' = \langle S \rangle \subseteq g_1^{-1}G'g_1$. Für jedes $n \in G'$ gibt es damit ein $n' \in G'$ mit $n = g_1^{-1}n'g_1$. Es folgt $g_1 n g_1^{-1} = n' \in G'$, also ist $g_1 G' g_1^{-1} \subseteq G'$ und damit $G' \trianglelefteq G$ erfüllt. Beweisen wir nun die Inklusion $S \subseteq g_1^{-1}G'g_1$. Jedes Element in S hat die Form $[g,h] = ghg^{-1}h^{-1}$ mit $g,h \in G$. Es folgt

$$\begin{aligned} ghg^{-1}h^{-1} &= g_1^{-1}(g_1ghg^{-1}h^{-1}g_1^{-1})g_1 = g_1^{-1}(g_1gg_1^{-1})(g_1hg_1^{-1})(g_1g^{-1}g_1^{-1})(g_1h^{-1}g_1^{-1})g_1 \\ &= g_1^{-1}(g_1gg_1^{-1})(g_1hg_1^{-1})(g_1gg_1^{-1})^{-1}(g_1hg_1^{-1})^{-1}g_1 = g_1^{-1}[g_1gg_1^{-1}, g_1hg_1^{-1}]g_1 \in g_1^{-1}G'g_1. \end{aligned}$$

zu (ii) „⇒“ Sei N ein Normalteiler von G mit $N \supseteq G'$. Wie oben bemerkt, gilt $[g,h]hg = gh$ für alle $g,h \in G$. Wegen $[g,h] \in N$ folgt daraus $N(hg) = N(gh)$, also $(gN)(hN) = (gh)N = N(gh) = N(hg) = (hg)N = (hN)(gN)$. Dies zeigt, dass G/N abelsch ist. „⇐“ Ist G/N abelsch, dann gilt $(gN)(hN) = (hN)(gN)$ für alle $g,h \in G$. Wie wir gerade gesehen haben, ist dies gleichbedeutend mit $N(hg) = N(gh)$, also $(gh)(hg)^{-1} = ghg^{-1}h^{-1} = [g,h] \in N$. Somit enthält N alle Kommutatoren, und es folgt $G' \subseteq N$. □

Die Bildung von Kommutatorgruppen lässt sich iterieren. Man bezeichnet mit G'' die Kommutatorgruppe von G', also $G'' = (G')'$. Allgemeiner definiert man rekursiv $G^{(0)} = G$ und $G^{(n+1)} = (G^{(n)})'$ für alle $n \in \mathbb{N}_0$. Die Untergruppen $G^{(n)}$ mit $n \geq 2$ werden die ***höheren Kommutatorgruppen*** von G genannt. Nach Satz 6.7 gilt $G^{(n+1)} \trianglelefteq G^{(n)}$ für alle $n \in \mathbb{N}_0$, und die Faktorgruppen $G^{(n)}/G^{(n+1)}$ sind abelsch.

Definition 6.8 Eine Gruppe G wird ***auflösbar*** genannt, wenn $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}_0$ gilt.

Offenbar sind abelsche Gruppen auflösbar, denn für jede abelsche Gruppe G gilt $G^{(1)} = \{e\}$, wie wir im Anschluss an Definition 6.6 gesehen haben.

Definition 6.9 Eine ***Subnormalreihe*** für eine Gruppe G ist eine Folge von Untergruppen der Form $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_r = \{e\}$ mit $r \in \mathbb{N}_0$, wobei für $0 \leq k < r$ jeweils $N_{k+1} \trianglelefteq N_k$ gilt. Die Faktorgruppen N_k/N_{k+1} bezeichnet man als ***Faktoren*** der Subnormalreihe. Sind alle Faktoren abelsch, dann spricht man von einer ***abelschen Subnormalreihe***.

Proposition 6.10 Jede endliche abelsche Gruppe besitzt eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Beweis: Sei G eine endliche abelsche Gruppe. Wir beweisen die Aussage durch vollständige Induktion über die Gruppenordnung $|G|$. Für $|G| = 1$ ist nichts zu zeigen, denn in diesem Fall können wir einfach $G_0 = G$ setzen. Sei nun $n = |G| > 1$, und setzen wir die Aussage für endliche, abelsche Gruppen von Ordnung $< n$ voraus. Nach Satz 5.10 ist G isomorph zu einem äußeren direkten Produkt $C_1 \times ... \times C_r$ zyklischer Faktoren C_i von Primzahlpotenzordnung; wir können o.B.d.A. voraussetzen, dass G mit einem solchen Produkt übereinstimmt. Sei $m = |C_r|$, p ein Primteiler von m und $g \in C_r$ ein Element der Ordnung m. Dann ist $\langle g^p \rangle$ eine Untergruppe der Ordnung $\frac{m}{p}$ von C_r. Setzen wir $G_1 = C_1 \times ... \times C_{r-1} \times \langle g^p \rangle$, dann ist G/G_1 zyklisch von Ordnung p. Nach Induktionsvoraussetzung besitzt G_1 eine Subnormalreihe mit zyklischen Faktoren, so dass wir insgesamt eine solche Reihe für G erhalten. □

Satz 6.11 Für eine endliche Gruppe G sind die folgenden Eigenschaften äquivalent.

(i) Die Gruppe G ist auflösbar.

(ii) Sie besitzt eine abelsche Subnormalreihe.

(iii) Sie hat eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Dabei ist die Äquivalenz „(i) $\Leftrightarrow$ (ii)“ auch für unendliche Gruppen gültig.

Beweis: Sei G zunächst ein beliebige, möglicherweise unendliche Gruppe. „(i) $\Rightarrow$ (ii)“ Nach Voraussetzung gilt $G^{(r)} = \{e\}$ für ein $r \in \mathbb{N}_0$. Setzen wir also $G_k = G^{(k)}$ für $0 \leq k \leq r$, dann gilt $G_0 = G$, $G_r = \{e\}$ und außerdem $G_k \supseteq G_{k+1}$ für $0 \leq k \leq r$ nach Definition der höheren Kommutorgruppen. Wie wir bereits im Anschluss an Satz 6.7 festgestellt haben, ist auch G_{k+1} für $0 \leq k < r$ jeweils ein Normalteiler von G_k, und die Faktorgruppen G_k/G_{k+1} sind abelsch. Also bilden die Untergruppen $G_0, ..., G_r$ eine Subnormalreihe mit abelschen Faktoren.

„(ii) $\Rightarrow$ (i)“ Sei $G_0, ..., G_r$ eine Subnormalreihe von G mit abelschen Faktoren. Wir beweisen durch vollständige Induktion über k, dass $G^{(k)} \subseteq G_k$ für $0 \leq k \leq r$ gilt. Für $k = 0$ ist dies erfüllt, denn nach Definition gilt $G_0 = G = G^{(0)}$. Sei nun $k \in \{1, ..., r\}$, und setzen wir $G^{(\ell)} \subseteq G_\ell$ für $0 \leq \ell < k$ voraus. Nach Voraussetzung ist G_{k-1}/G_k abelsch, somit gilt $G_k \supseteq (G_{k-1})'$ nach Satz 6.7 (ii), angewendet auf den Normalteiler $N = G_k$. Mit der Induktionsvoraussetzung folgt nun $G^{(k)} = (G^{(k-1)})' \subseteq (G_{k-1})' \subseteq G_k$. Aus $G^{(r)} \subseteq G_r$ und $G_r = \{e\}$ erhalten wir schließlich $G^{(r)} = \{e\}$. Somit ist G auflösbar.

Sei nun G eine endliche Gruppe. Die Implikation „(iii) $\Rightarrow$ (ii)“ ist offenbar gültig, da zyklische Gruppen stets abelsch sind (siehe § 2). Beweisen wir nun „(ii) $\Rightarrow$ (iii)“ und setzen dazu voraus, dass $G_0, ..., G_r$ eine Subnormalreihe von G mit abelschen Faktoren ist. Für jedes $k \in \{0, ..., r-1\}$ ist $\bar{G} = G_k/G_{k+1}$ also eine endliche, abelsche Gruppe, und nach Proposition 6.10 besitzt diese eine Subnormalreihe $\bar{U}_0, ..., \bar{U}_s$ mit zyklischen Faktoren $\bar{U}_\ell/\bar{U}_{\ell+1}$. Sei nun $U_\ell = \pi_{G_{k+1}}^{-1}(\bar{U}_\ell) \subseteq G_k$ für $0 \leq \ell \leq s$. Dann gilt insbesondere $U_0 = G_k$ und $U_s = G_{k+1}$. Nach Satz 4.31 (angewendet auf $G = U_\ell$, $U = U_{\ell+1}$ und $N = G_{k+1}$) folgt aus $\bar{U}_{\ell+1} \trianglelefteq \bar{U}_\ell$, dass $U_{\ell+1}$ ein Normalteiler von U_ℓ ist, für $0 \leq \ell < s$. Wegen Satz 4.32 gilt außerdem

$$U_\ell/U_{\ell+1} \quad \cong \quad \bar{U}_\ell/\bar{U}_{\ell+1} \quad ,$$

also sind die Faktorgruppen $U_\ell/U_{\ell+1}$ zyklisch von Primzahlordnung. Fügen wir zwischen G_k und G_{k+1} also die Gruppen $U_1, ..., U_{s-1}$ ein und führen diesen Schritt für jedes $k \in \{0, ..., r-1\}$ aus, so erhalten wir insgesamt eine Subnormalreihe für G mit zyklischen Faktoren von Primzahlordnung. □

Die symmetrischen Gruppen S_n und die alternierenden Gruppen A_n sind auflösbar für $n \leq 4$, aber nicht auflösbar für alle $n \geq 5$. Diese Beobachtung wird später in der Galoistheorie eine wichtige Rolle spielen. Im nächsten Kapitel werden wir zeigen, dass endliche Gruppen von Primzahlpotenzordnung stets auflösbar sind. Zum Abschluss schauen wir uns an, wie man von der Auflösbarkeit einer Gruppe auf andere Gruppen schließen kann.

Satz 6.12

(i) Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.

(ii) Sei G eine Gruppe und $N \trianglelefteq G$. Unter diesen Voraussetzungen ist G auflösbar genau dann, wenn N und G/N beide auflösbar sind.

Beweis: zu (i) Sei G eine auflösbare Gruppe und U eine Untergruppe. Jeder Kommutator von U ist auch ein Kommutator von G. Daraus folgt $U' \subseteq G'$, und durch vollständige Induktion erhält man $U^{(n)} \subseteq G^{(n)}$ für alle $n \in \mathbb{N}_0$. Gilt nun $G^{(n)} = \{e_G\}$ für ein $n \in \mathbb{N}$, dann folgt daraus $U^{(n)} = \{e_G\}$. Also ist auch U auflösbar.

zu (ii) „⇒“ Ist G auflösbar, dann folgt daraus, wie wir unter (i) gesehen haben, die Auflösbarkeit von N. Für die Auflösbarkeit von G/N beweisen wir zunächst die Gleichung $(G/N)' = \pi_N(G')$. Sei S die Menge der Kommutatoren von G und $\bar{S}$ die Menge der Kommutatoren von G/N. Für alle $g, h \in G$ gilt

$$[gN, hN] \quad = \quad (gN)(hN)(gN)^{-1}(hN)^{-1} \quad = \quad (ghg^{-1}h^{-1})N \quad = \quad [g,h]N \quad = \quad \pi_N([g,h]).$$

Jedes Element aus S wird also von π_N nach $\bar{S}$ abgebildet, und die Abbildung ist surjektiv, weil jedes Element aus $\bar{S}$ die Form $[gN, hN]$ mit $g, h \in G$ hat. Es gilt also $\pi_N(S) = \bar{S}$. Aus $\bar{S} \subseteq \pi_N(S) \subseteq \pi_N(G')$ und der Untergruppeneigenschaft von $\pi_N(G')$ folgt $(G/N)' = \langle \bar{S} \rangle \subseteq \pi_N(G')$. Aus $\pi_N(S) \subseteq \bar{S}$ folgt umgekehrt $S \subseteq \pi_N^{-1}(\bar{S}) \subseteq \pi_N^{-1}((G/N)')$. Weil $\pi_N^{-1}((G/N)')$ Untergruppe von G ist, erhalten wir $G' = \langle S \rangle \subseteq \pi_N^{-1}((G/N)')$ und somit $\pi_N(G') \subseteq (G/N)'$. Insgesamt ist damit $\pi_N(G') = (G/N)'$ bewiesen. Vollständige Induktion liefert $(G/N)^{(n)} = \pi_N(G^{(n)})$ für alle $n \in \mathbb{N}_0$. Gilt also $G^{(n)} = \{e_G\}$ für ein $n \in \mathbb{N}_0$, dann folgt daraus $(G/N)^{(n)} = \{e_{G/N}\}$.

„⇐“ Nach Voraussetzung gibt es ein $n \in \mathbb{N}_0$ mit $N^{(n)} = \{e_G\}$ und $(G/N)^{(n)} = \{e_{G/N}\}$. Wegen $\pi_N(G^{(n)}) = (G/N)^{(n)} = \{e_{G/N}\}$ gilt $G^{(n)} \subseteq N$. Daraus folgt $G^{(2n)} \subseteq (G^{(n)})^{(n)} \subseteq N^{(n)} = \{e_G\}$ und somit die Auflösbarkeit von G. □

Aus Satz 6.12 folgt unmittelbar: Ist G ein inneres semidirektes Produkt einer Untergruppe U und eines Normalteilers N, so ist G genau dann auflösbar, wenn N und $G/N = (UN)/N \cong U$ beide auflösbar sind. Wie in den Übungen gezeigt wird, kann auch jedes äußere (semi-)direkte Produkt der Form $N \rtimes_\phi U$ (bzw. $G = N \times U$) als inneres semidirektes von Gruppen aufgefasst werden, die zu N und U isomorph sind. Also ist auch $N \rtimes_\phi U$ genau dann auflösbar, wenn N und U auflösbar sind.

Zum Abschluss des Kapitels untersuchen wir die Auflösbarkeit der symmetrischen und alternierenden Gruppen.

Satz 6.13 Die Gruppen S_n und A_n sind auflösbar für $n \leq 4$, nicht auflösbar für $n \geq 5$.

Beweis: Die Gruppe A_2 ist trivial, also auflösbar, und A_3 ist als Gruppe von Primzahlordnung zyklisch, also abelsch und somit ebenfalls auflösbar. Für $n = 4$ betrachten wir die Untergruppenkette $\{\mathrm{id}\} \subseteq V_4 \subseteq A_4$, wobei

$$V_4 \quad = \quad \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

die Kleinsche Vierergruppe bezeichnet. Offenbar gilt $\mathrm{id} \trianglelefteq V_4$, und als Gruppe der Ordnung 4 ist die Faktorgruppe $V_4/\{\mathrm{id}\} \cong V_4$ abelsch. Darüber hinaus ist die Gruppe V_4 nicht nur ein Normalteiler von A_4, sondern sogar von S_4. Für den Nachweis seien $\sigma \in S_4$ und $\tau \in V_4$ vorgegeben. Im Fall $\tau = \mathrm{id}$ gilt offenbar $\sigma\tau\sigma^{-1} = \mathrm{id} \in V_4$. Ansonsten ist τ eine Doppeltransposition der Form $\tau = (i\ j)(k\ \ell)$, und die Gleichung

$$\sigma\tau\sigma^{-1} \quad = \quad (\sigma(i)\ \sigma(j))(\sigma(k)\ \sigma(\ell))$$

zeigt, dass $\sigma\tau\sigma^{-1}$ ebenfalls eine Doppeltransposition und somit in V_4 enthalten ist. Als Gruppe der Primzahlordnung 3 ist A_4/V_4 ebenfalls zyklisch und damit abelsch. Insgesamt ist damit nachgewiesen, dass auch A_4 eine auflösbare Gruppe ist.

Die Gruppe S_1 ist trivial und somit auflösbar. Für $n \geq 2$ ist S_n/A_n zyklisch von Ordnung 2, also abelsch und damit auflösbar. Dies zeigt, dass S_n genau dann auflösbar ist, wenn A_n auflösbar ist. Insbesondere ist S_n für $2 \leq n \leq 4$ auflösbar. Um den Beweis abzuschließen, genügt es nun zu zeigen, dass A_n für $n \geq 5$ nicht auflösbar ist. Dafür wiederum reicht es zu zeigen, dass der Kommutator A_n' von A_n mit A_n selbst übereinstimmt. Denn daraus folgt $A_n^{(m)} = A_n$ für alle höheren Kommutatoren, während eine auflösbare Gruppe $G^{(m)} = \{e_G\}$ für hinreichend großes m erfüllen muss.

Aus Satz 2.11 ist bekannt, dass A_n von der Menge der 3-Zykel in S_n erzeugt wird. Für die Gleichung $A_n' = A_n$ genügt es also nachzuweisen, dass A_n' für $n \geq 5$ alle 3-Zykel aus S_n enthält. Seien $k, \ell, m, n, p \in M_n$ paarweise verschieden, außerdem $\sigma = (k\ \ell\ m)$ und $\tau = (k\ n\ p)$. Dann gilt

$$[\sigma, \tau] \quad = \quad \sigma\tau\sigma^{-1}\tau^{-1} \quad = \quad (k\ \ell\ m)(k\ n\ p)(k\ m\ \ell)(k\ p\ n) \quad = \quad (k\ \ell\ n).$$

Da die drei Elemente k, ℓ, n in M_n beliebig gewählt werden können, zeigt die Rechnung, dass jeder 3-Zykel tatsächlichn in A_n' enthalten ist. □

§ 7. Gruppenoperationen und Klassengleichung

Zusammenfassung. Der Begriff der Gruppenoperation ermöglicht es, die Elemente einer Gruppe auf eine sehr allgemeine Weise als „Symmetrieoperationen“ zu interpretieren, wobei sich die Symmetrie auf die Strukturen der Geometrie (zum Beispiel Polytope, siehe § 1), auf Strukturen der Analysis (Funktionenräume) oder der Algebra beziehen kann. Dabei liefert der Aufbau der Gruppen Informationen über die jeweilige Struktur, und umgekehrt lässt der Aufbau der Struktur, auf der eine Gruppe operiert, häufig Rückschlüsse auf die Gruppe zu.

Nach der Einführung der wichtigsten Grundbegriffe und der Herleitung einiger elementarer Gesetzmäßigkeiten konzentrieren uns auf zwei spezielle Operationen einer Gruppe auf der Menge ihrer Elemente: der Operation durch Linkstranslation und der Operationen durch Konjugation. Mit Hilfe des ersten Typs beweisen wir den *Satz von Cayley*, der besagt, dass jede endliche Gruppe zu einer Untergruppe einer symmetrischen Gruppe isomorph ist. Der zweite Typ führt uns auf die sog. *Klassengleichung*, mit deren Hilfe wir zeigen, dass Gruppen von Primzahlquadratordnung abelsch und Gruppen von Primzahlpotenzordnung auflösbar sind. Außerdem studieren wir die Klassengleichung der symmetrischen und alternierenden Gruppen und beweisen die Einfachheit von A_n für $n \geq 5$.

Wichtige Grundbegriffe

- Operation einer Gruppe G auf einer Menge X
- Stabilisator G_x eines Elements $x \in X$
- Bahn $G(x)$ eines Elements $x \in X$, Fixpunkt
- Repräsentantensysteme der Bahnen
- Operation durch Linkstranslation
- Operation durch Konjugation
- Konjugationsklasse von Gruppenelementen
- Zentralisator eines Gruppenelements

Zentrale Sätze

- Untergruppeneigenschaft des Stabilisators G_x
- Zerlegung von X durch die Bahnen einer Operation
- Beziehung zwischen Bahnlänge und Stabilisator
- Korrespondenz zwischen Operationen von G auf X und Homomorphismen $G \to \mathrm{Per}(X)$
- Satz von Cayley
- Bahngleichung und Klassengleichung
- Auflösbarkeit von p-Gruppen
- Gruppen der Ordnung p^2 sind abelsch
- Einfachheit der A_n für $n \geq 5$

Definition 7.1 Sei G eine Gruppe und X eine Menge. Eine ***Gruppenoperation*** von G auf X ist eine Abbildung $\alpha : G \times X \longrightarrow X$ mit den Eigenschaften

$$\alpha(e_G, x) = x \qquad \text{und} \qquad \alpha(g, \alpha(h, x)) = \alpha(gh, x)$$

für alle $g, h \in G$ und $x \in X$, wobei e_G das Neutralelement der Gruppe bezeichnet.

An Stelle von $\alpha(g, x)$ verwendet man häufig auch die Infix-Schreibweise $g \cdot x$, wobei $\cdot$ das Symbol für die Gruppenoperation ist. Die definierenden Gleichungen der Gruppenoperation lassen sich dann sparsamer in der Form $e_G \cdot x = x$

und $g \cdot (h \cdot x) = (gh) \cdot x$ schreiben. Man darf allerdings das Symbol $\cdot$ nicht mit der Verknüpfungsabbildung der Gruppe verwechseln.

Wir betrachten einige Beispiele für Gruppenoperationen.

(i) Die symmetrische Gruppe S_n operiert auf der Menge $M_n = \{1, ..., n\}$ durch $\sigma \cdot x = \sigma(x)$ für alle $\sigma \in S_n$ und $x \in M_n$. Ist $n = 7$, dann gilt beispielsweise $(1\ 2\ 7) \cdot 2 = 7$ und $(1\ 2\ 7) \cdot 3 = 3$.

(ii) Sei K ein Körper und V ein K-Vektorraum. Dann operiert die Gruppe $G = \mathrm{GL}(V)$ der bijektiven linearen Abbildungen $V \to V$ auf V durch $\phi \cdot v = \phi(v)$ für alle $\phi \in G$ und $v \in V$.

Anhand der folgenden Merkmale kann eine Gruppenoperation genauer analysiert werden.

Definition 7.2 Sei G eine Gruppe, X eine Menge und $G \times X \to X$, $(g, x) \mapsto g \cdot x$ eine Gruppenoperation.

(i) Für jedes $x \in X$ nennt man $G(x) = \{g \cdot x \mid g \in G\}$ die ***Bahn*** von x.

(ii) Gibt es ein $x \in X$ mit $G(x) = X$, dann ist die Gruppenoperation ***transitiv***.

(iii) Die Elemente $x \in X$ mit $G(x) = \{x\}$ heißen ***Fixpunkte*** der Gruppenoperation.

(iv) Eine Teilmenge $Y \subseteq X$ wird als ***G-invariant*** bezeichnet, wenn für alle $g \in G$ und $y \in Y$ auch $g \cdot y \in Y$ gilt.

Die folgende Beobachtung ist für nachfolgende Theorie von zentraler Bedeutung, ähnlich wie beim Satz von Lagrange die Zerlegung einer Gruppe in Nebenklassen bezüglich einer Untergruppe.

Proposition 7.3 Sei G eine Gruppe, X eine Menge und $G \times X \to X$, $(g, x) \mapsto g \cdot x$ eine Gruppenoperation. Dann gilt

(i) Die Menge $\mathcal{B} = \{G(x) \mid x \in X\}$ der Bahnen ist eine Zerlegung von X.

(ii) Eine Teilmenge $Y \subseteq X$ ist genau dann G-invariant, wenn Y eine Vereinigung von Bahnen der Operation ist.

Beweis: zu (i) Wir überprüfen die in § 3 angegebenen Bedingungen für eine Zerlegung. Jedes $x \in X$ ist wegen $e_G \cdot x = x$ in $G(x)$ enthalten. Also ist jede Bahn nichtleer, und jedes $x \in X$ ist in mindestens einer Bahn enthalten. Wir zeigen nun, dass jedes Element in *genau* einer Bahn enthalten ist und beweisen dafür: Ist $x \in X$ und $y \in G(x)$, dann folgt $G(x) = G(y)$. Wegen $y \in G(x)$ gibt es ein Gruppenelement $g_0 \in G$ mit $g_0 \cdot x = y$ und

$$g_0^{-1} \cdot y \quad = \quad g_0^{-1} \cdot (g_0 \cdot x) \quad = \quad (g_0^{-1} g_0) \cdot x \quad = \quad e_G \cdot x \quad = \quad x.$$

Wir überprüfen nun die Inklusionen $G(x) \subseteq G(y)$ und $G(x) \supseteq G(y)$. „$\subseteq$“ Sei $z \in G(x)$. Dann gibt es ein $g \in G$ mit $g \cdot x = z$. Es folgt $(g g_0^{-1}) \cdot y = g \cdot (g_0^{-1} \cdot y) = g \cdot x = z$ und damit $z \in G(y)$. „$\supseteq$“ Sei $z \in G(y)$. Dann existiert nach Definition der Bahn $G(y)$ ein $g \in G$ mit $g \cdot y = z$. Wir erhalten damit $(g g_0) \cdot x = g \cdot (g_0 \cdot x) = g \cdot y = z$, also $z \in G(x)$.

zu (ii) „⇐“ Setzen wir voraus, dass Y eine Vereinigung von Bahnen der Operation ist. Seien $g \in G$ und $y \in Y$ vorgegeben. Auf Grund der Voraussetzung ist mit y die gesamte Bahn $G(y)$ in Y enthalten; es gilt also $g \cdot y \in Y$. „⇒“ Sei $y \in Y$. Da Y eine G-invariante Teilmenge ist, folgt $g \cdot y \in Y$ für alle $g \in G$, und damit $G(y) \subseteq Y$. Dies zeigt, dass Y eine Vereinigung von Bahnen der Gruppenoperation ist. □

Ist die Gruppenoperation transitiv, so gibt es nur eine Bahn in X. Diese Bedingung ist gleichbedeutend damit, dass je zwei Elemente $x, y \in X$ in derselben Bahn liegen, also jeweils ein $g \in G$ mit $g \cdot x = y$ existiert. Dies bedeutet auch, dass $G(x) = X$ für *alle* $x \in X$ erfüllt ist.

(i) Die Gruppe S_n operiert transitiv auf M_n. Sind nämlich $a, b \in M_n$ mit $a \neq b$ vorgegeben, dann gilt $\tau \cdot a = b$ für $\tau = (a\ b)$. Also liegen je zwei Elemente in derselben Bahn.

(ii) Sei nun $G = S_7$ und $U = \langle \sigma \rangle$ die vom Element $\sigma = (1\ 2\ 5)(3\ 4)(6\ 7)$ erzeugte, zyklische Untergruppe der Ordnung 6. Für jedes $n \in \mathbb{Z}$ gilt $\sigma^n(1) \in \{1, 2, 5\}$, wie man mit vollständiger Induktion leicht überprüft. Die Bahn von 1 ist also durch $U(1) = \{1, 2, 5\}$ gegeben. Zugleich ist dies auch die Bahn der Elemente 2 und 5. Ebenso sieht man $U(3) = U(4) = \{3, 4\}$ und $U(6) = U(7) = \{6, 7\}$.

Ist allgemein $\sigma \in S_n$ ein Produkt disjunkter Zykel, dann bilden die Träger der Zykel genau die Bahnen der Operation von $\langle \sigma \rangle$ auf M_n mit mehr als einem Element. Damit kann gezeigt werden, dass jedes Element $\sigma \in S_n$ eine bis auf Reihenfolge eindeutige Darstellung als Produkt disjunkter Zyklen besitzt.

Satz 7.4 Sei G eine Gruppe, die auf einer Menge X operiert, und $x \in X$. Dann ist die Teilmenge $G_x = \{g \in G \mid g \cdot x = x\}$ eine Untergruppe von G. Man nennt sie den ***Stabilisator*** von x.

Beweis: Wegen $e_G \cdot x = x$ gilt $e_G \in G_x$. Seien nun $g, h \in G_x$ vorgegeben. Dann gilt $g \cdot x = x$ und $h \cdot x = x$. Es folgt $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$. Dies zeigt $gh \in G_x$. Ferner gilt $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e_G \cdot x = x$ und somit also auch $g^{-1} \in G_x$. □

Wieder betrachten wir eine Reihe von Beispielen.

(i) Wir betrachten die Operation von $G = S_4$ auf $X = M_4$. Der Stabilisator G_4 des Elements $4 \in X$ besteht nach Definition aus allen $\sigma \in G$ mit $\sigma \cdot 4 = \sigma(4) = 4$, also allen Permutationen mit $4 \notin \mathrm{tr}(\sigma)$. Es gilt also

$$G_4 \quad = \quad \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

(ii) In der Untergruppe U von S_7 aus Beispiel (ii) von oben ist der Stabilisator von 3 durch die dreielementige Untergruppe $\langle \sigma^2 \rangle$ gegeben. Denn für jedes $m \in \mathbb{Z}$ gilt $\sigma^m(3) = 3$ genau dann, wenn m eine gerade Zahl ist. Der Stabilisator von 1 ist die Untergruppe $\langle \sigma^3 \rangle$ der Ordnung 2.

(iii) Sei $V = \mathbb{R}^2$, $G = \mathrm{GL}(V)$ und $X = V$. Ist $v = e_1$, dann besteht G_v genau aus den Matrizen der Form

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \qquad \text{mit} \quad a, b \in \mathbb{R}\,,\ b \neq 0 \quad ,$$

denn an der ersten Spalte der Matrix kann abgelesen werden, dass $e_1 = (1, 0)$ auf sich abgebildet wird. Für den Nullvektor gilt $G_{(0,0)} = G$.

Proposition 7.5 Sei $n \in \mathbb{N}$ mit $n \geq 2$. Wie wir bereits festgestellt haben, existiert eine natürliche Gruppenoperation der symmetrischen Gruppe S_n auf der Menge M_n. Der Stabilisator $(S_n)_n$ ist eine zu S_{n-1} isomorphe Untergruppe von S_n.

Beweis: Man überprüft leicht, dass durch die Zuordnung $\sigma \mapsto \sigma|_{M_{n-1}}$ eine Bijektion zwischen $(S_n)_n$ und S_{n-1} definiert ist. Denn jedes $\sigma \in (S_n)_n$ bildet n auf n und M_{n-1} bijektiv auf M_{n-1} ab, somit ist $\sigma|_{M_{n-1}}$ tatsächlich ein Element in S_{n-1}. Umgekehrt kann offenbar jedes $\tau \in S_{n-1}$ durch $\hat{\tau}(k) = \tau(k)$ für $1 \leq k \leq n-1$ und $\hat{\tau}(n) = n$ zu einem Element $\hat{\tau} \in (S_n)_n$ fortgesetzt werden. Die Zuordnungen $(S_n)_n \to S_{n-1}$, $\sigma \mapsto \sigma|_{M_{n-1}}$ und $S_{n-1} \to (S_n)_n$, $\tau \mapsto \hat{\tau}$ sind zueinander invers, also handelt es sich um Bijektionen. Außerdem ist die erste Zuordnung ein Gruppenhomomorphismus, denn für alle $\sigma, \rho \in (S_n)_n$ ist wegen $\rho(M_{n-1}) \subseteq M_{n-1}$ die Komposition $\sigma|_{M_{n-1}} \circ \rho|_{M_{n-1}}$ definiert (der Wertebereich von $\rho|_{M_{n-1}}$ ist im Definitionsbereich von $\sigma|_{M_{n-1}}$ enthalten), und es gilt $(\sigma \circ \rho)|_{M_{n-1}} = \sigma|_{M_{n-1}} \circ \rho|_{M_{n-1}}$. Insgesamt liegt also ein Isomorphismus $(S_n)_n \cong S_{n-1}$ vor. □

Ebenso kann man zeigen, dass der Stabilisator $(S_n)_k$ für $1 \leq k \leq n-1$ isomorph zu S_{n-1} ist. Insgesamt sind in S_n also n zu S_{n-1} isomorphe Untergruppen enthalten.

Satz 7.6 Sei G eine Gruppe, die auf einer Menge X operiert, und sei $x \in X$. Dann gibt es eine Bijektion $\phi_x : G/G_x \to G(x)$ mit $\phi_x(gG_x) = g \cdot x$ für alle $g \in G$. Ist insbesondere X endlich, dann ist auch der Index $(G : G_x)$ endlich, und es gilt $(G : G_x) = |G(x)|$.

Beweis: Für die Existenz der Abbildung ϕ_x genügt es nach Satz 4.25 zu überprüfen, dass für alle $g, h \in G$ aus der Bedingung $g \equiv_\ell h$ (gegeben durch $h \in gG_x$) jeweils $g \cdot x = h \cdot x$ folgt. Dies ist tatsächlich der Fall. Ist nämlich $h \in gG_x$, also $h = gg_1$ für ein $g_1 \in G_x$, dann folgt $h \cdot x = (gg_1) \cdot x = g \cdot (g_1 \cdot x) = g \cdot x$.

Die Abbildung ϕ_x ist surjektiv: Ist nämlich $y \in G(x)$ vorgegeben, dann existiert nach Definition der Bahn ein Element $g \in G$ mit $g \cdot x = y$, und wir erhalten $\bar{\phi}_x(gG_x) = y$. Nun beweisen wir noch die Injektivität. Seien $\bar{g}, \bar{h} \in G/G_x$ mit $\phi_x(\bar{g}) = \phi_x(\bar{h})$ vorgegeben. Außerdem seien $g, h \in G$ so gewählt, dass $\bar{g} = gG_x$ und $\bar{h} = hG_x$ gilt. Nach Definition der Abbildung ϕ_x gilt $g \cdot x = \phi_x(gG_x) = \phi_x(hG_x) = h \cdot x$, also

$$(g^{-1}h) \cdot x \quad = \quad g^{-1} \cdot (h \cdot x) \quad = \quad g^{-1} \cdot (g \cdot x) \quad = \quad x.$$

Es folgt $g^{-1}h \in G_x$, also $\bar{g} = gG_x = g(g^{-1}h)G_x = hG_x = \bar{h}$. □

In vielen Fällen ist es sinnvoll, eine Gruppe auf der Menge ihrer Elemente oder der Menge ihrer Untergruppen operieren zu lassen. Wir betrachten hierzu eine Reihe von Beispielen. Aus jeder dieser Operationen werden sich später wichtige Anwendungen ergeben.

Definition 7.7 Sei G eine Gruppe und $\mathcal{U}$ die Menge ihrer Untergruppen.

(i) Die Operation von G auf der Menge ihrer Elemente gegeben durch $g \cdot h = gh$ bezeichnet man als ***Operation durch Linkstranslation***. Bezüglich dieser Operation ist jeder Stabilisator trivial, d.h. es gilt $G_h = \{e\}$ für alle $h \in G$, und die Operation ist transitiv.

(ii) Die Operation von G auf der Menge ihrer Elemente gegeben durch $g \cdot h = ghg^{-1}$ wird ***Operation durch Konjugation*** genannt. Die Bahnen dieser Operation nennt man auch ***Konjugationsklassen***, und den Stabilisator eines Elements $h \in G$ nennt man auch den ***Zentralisator*** $C_G(h)$ von h in G.

(iii) Die Operation von G auf $\mathcal{U}$ gegeben durch $g \cdot U = gUg^{-1}$ wird ebenfalls als ***Operation durch Konjugation*** bezeichnet. Der Stabilisator eines Elements $U \in \mathcal{U}$ ist der ***Normalisator*** $N_G(U)$ von U in G (siehe § 4).

Wir überprüfen kurz die Angaben in der Definition. Bezeichnet $\cdot : G \times G \to G$ die Operation durch Linkstranslation, dann gilt für alle $g, g' \in G$ und $h \in G$ sowohl $e \cdot h = eh = h$ als auch $g \cdot (g' \cdot h) = g \cdot (g'h) = g(g'h) = (gg')h = (gg') \cdot h$, also liegt tatsächlich eine Gruppenoperation vor. Ist $g \in G_h$ ein Element des Stabilisators von h bezüglich dieser Operation, dann folgt $gh = g \cdot h = h$, und Multiplikation mit h^{-1} von rechts liefert $ghh^{-1} = hh^{-1}$, also $ge = e$ und $g = e$. Damit ist $G_h = \{e\}$ nachgewiesen. Die Bahn $G(e)$ des Neutralelements umfasst alle Elemente der Gruppe G, denn für alle $g \in G$ gilt $g = ge = g \cdot e \in G(e)$. Damit ist die gezeigt, dass es sich um eine transitive Gruppenoperation handelt.

Ebenso ist die Operation durch Konjugation von G auf der Menge G tatsächlich eine Gruppenoperation, denn für alle $g, g' \in G$ und $h \in G$ gilt sowohl $e \cdot h = ehe^{-1} = ehe = h$ als auch

$$g \cdot (g' \cdot h) \quad = \quad g \cdot (g'h(g')^{-1}) \quad = \quad g(g'h(g')^{-1})g^{-1} \quad = \quad (gg')h(gg')^{-1} \quad = \quad (gg') \cdot h.$$

Auch die Operation von G auf der Menge $\mathcal{U}$ ihrer Untergruppen ist eine Gruppenoperation, denn für alle $g, g' \in \mathcal{U}$ und $U \in \mathcal{U}$ gilt $e \cdot U = eUe^{-1} = eUe = U$ und

$$g \cdot (g' \cdot U) \quad = \quad g \cdot (g'U(g')^{-1}) \quad = \quad g(g'U(g')^{-1})g^{-1} \quad = \quad (gg')U(gg')^{-1} \quad = \quad (gg') \cdot U.$$

Wir kommen nun zu einer erste wichtigen Anwendung der Gruppenoperationen. Der ***Satz von Cayley*** besagt, dass jede endliche Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe S_n ist, unter der Voraussetzung, dass n groß genug gewählt wird. Dieses Ergebnis beruht auf dem folgenden allgemeinen Zusammenhang zwischen Gruppenoperationen und Homomorphismen.

Satz 7.8 Sei G eine Gruppe und X eine Menge.

(i) Ist $\alpha : G \times X \to X$ eine Gruppenoperation, dann kann jedem $g \in G$ durch $\tau_g(x) = \alpha(g,x)$ ein Element aus $\mathrm{Per}(X)$ zugeordnet werden. Die Abbildung $G \to \mathrm{Per}(X)$, $g \mapsto \tau_g$ ist ein Gruppenhomomorphismus.

(ii) Sei umgekehrt $\phi : G \to \mathrm{Per}(X)$ ein Gruppenhomomorphismus. Dann ist durch $\alpha : G \times X \to X$ mit $\alpha(g,x) = \phi(g)(x)$ eine Gruppenoperation gegeben.

Beweis: zu (i) Zunächst überprüfen wir, dass τ_g für jedes $g \in G$ eine bijektive Abbildung ist. Seien $x, y \in X$. Aus $\tau_g(x) = \tau_g(y)$ folgt $\alpha(g,x) = \alpha(g,y)$, und es gilt

$$\begin{aligned} x &= \alpha(e_G,x) = \alpha(g^{-1}g,x) = \alpha(g^{-1},\alpha(g,x)) = \alpha(g^{-1},\alpha(g,y)) \\ &= \alpha(g^{-1}g,y) = \alpha(e_G,y) = y. \end{aligned}$$

Also ist die Abbildung τ_g injektiv. Ist $y \in X$ vorgegeben, dann setzen wir $x = \alpha(g^{-1},x)$. Es gilt dann $\tau_g(x) = \alpha(g,x) = \alpha(g,\alpha(g^{-1},y)) = \alpha(gg^{-1},y) = \alpha(e_G,y) = y$. Dies beweist die Surjektivität von τ_g. Somit ist τ_g für jedes $g \in G$ ein Element von $\mathrm{Per}(X)$. Nun zeigen wir, dass durch $g \mapsto \tau_g$ ein Gruppenhomomorphismus gegeben ist. Seien dazu $g,h \in G$ vorgegeben. Für jedes $x \in X$ gilt

$$(\tau_g \circ \tau_h)(x) = \tau_g(\tau_h(x)) = \tau_g(\alpha(h,x)) = \alpha(g,\alpha(h,x)) = \alpha(gh,x) = \tau_{gh}(x).$$

Also ist die Abbildung $g \mapsto \tau_g$ verträglich mit den Verknüpfungen auf G und $\mathrm{Per}(X)$.

zu (ii) Seien $g,h \in G$ und $x \in X$ gegeben. Wir müssen die definierenden Gleichungen einer Gruppenoperation nachrechnen. Weil ϕ ein Gruppenhomomorphismus ist, wird e_G auf das Neutralelement id_X von $\mathrm{Per}(X)$ abgebildet. Es folgt $\alpha(e_G,x) = \phi(e_G)(x) = \mathrm{id}_X(x) = x$. Die Homomorphismus-Eigenschaft liefert außerdem $\phi(gh) = \phi(g) \circ \phi(h)$. Also gilt

$$\begin{aligned} \alpha(gh,x) &= \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = \\ &\alpha(g,\phi(h)(x)) = \alpha(g,\alpha(h,x)). \end{aligned}$$

□

Die Gruppenoperation im Beispiel (i) von oben kommt durch den identischen Homomorphismus auf $G = S_n$, die Operation im Beispiel (ii) durch die Inklusionsabbildung $\mathrm{GL}(V) \to \mathrm{Per}(V)$ zu Stande. Jedes Element aus $\mathrm{GL}(V)$ ist inbesondere eine bijektive Abbildung auf V.

Satz 7.9 *(Satz von Cayley)*

Sei G eine Gruppe der Ordnung n. Dann gibt es einen Monomorphismus $G \to S_n$. Mit anderen Worten, G ist isomorph zu einer Untergruppe von S_n.

Beweis: Wie wir in Definition 7.7 festgestellt haben, operiert G durch Linkstranslation auf sich selbst. Nach Satz 7.8 existiert ein Gruppenhomomorphismus $\Psi : G \to \mathrm{Per}(G)$, $g \mapsto \tau_g$, wobei $\tau_g \in \mathrm{Per}(G)$ jeweils durch $\tau_g(h) = g \cdot h = gh$ definiert ist. Dieser Homomorphismus ist injektiv. Sei nämlich $g \in \ker(\Psi)$ vorgegeben, also $\Psi(g) = \tau_g = \mathrm{id}_G$. Dann gilt insbesondere $g = ge_G = \tau_g(e_G) = \mathrm{id}_G(e_G) = e_G$. Damit ist die Injektivität von Ψ nachgewiesen.

Darüber hinaus gibt es wegen $|G| = n$ eine Bijektion $\phi : M_n \to G$, wobei $M_n = \{1, ..., n\}$ ist. Nach Satz 4.5 liefert diese Bijektion einen Isomorphismus $\hat{\phi}$ zwischen $S_n = \mathrm{Per}(M_n)$ und $\mathrm{Per}(G)$. Ingesamt ist $\hat{\phi}^{-1} \circ \Psi : G \to S_n$ also ein Monomorphismus, der einen Isomorphismus zwischen G und der Untergruppe $(\hat{\phi}^{-1} \circ \Psi)(G)$ von S_n definiert. □

Dem Beweis des Satzes von Cayley können wir folgende einfache Konsequenz aus Satz 7.8 entnehmen: Ist G eine Gruppe, die auf einer n-elementigen Menge operiert ($n \in \mathbb{N}$), so liefert diese Operation auf natürliche Weise einen Homomorphismus $G \to S_n$. Dies kann verwendet werden, um den Isomorphietyp der Symmetriegruppen der platonischen Körper, die wir in § 1 betrachtet haben, zu bestimmen.

(i) *Tetraedergruppe:* Es gilt $\mathbb{T}^+ \cong A_4$ und $\mathbb{T} \to S_4$.

Beweis: Die Operation von $\mathbb{T}$ auf der 4-elementigen Menge der Ecken des Tetraeders definiert einen Homomorphismus $\phi : \mathbb{T} \to S_4$. Ein Element der Tetraedergruppe, das alle Ecken festhält, muss mit $\mathrm{id}_{\mathbb{R}^3}$ übereinstimmen. Somit ist der Homomorphismus injektiv.

Nun enthält die Gruppe $\mathbb{T}^+$ enthält genau 12 Elemente. Neben $\mathrm{id}_{\mathbb{R}^3}$ sind dies 8 Drehungen (um 120° und 240°) um Achsen durch eine Ecke und eine gegenüberliegende Seite sowie 3 Drehungen (um 180°) um Achsen durch die Mitten gegenüberliegender Kanten. Der Homomorphiesatz, angewendet auf die Determinantenabbildung, liefert einen Isomorphismus $\mathbb{T}/\mathbb{T}^+ \cong \{\pm 1\}$. Es gilt also $(\mathbb{T} : \mathbb{T}^+) = 2$ und $|\mathbb{T}| = 2 \cdot |\mathbb{T}^+| = 2 \cdot 12 = 24$. Also ist $\mathbb{T}$ isomorph zu einer 24-elementigen Untergruppe von S_4, und wegen $|S_4| = 24$ folgt daraus $\mathbb{T} \cong S_4$. Identifiziert man die Ecken des Tetraeders mit $M_4 = \{1, 2, 3, 4\}$, dann entsprechen die Elemente von $\mathbb{T}^+$ neben id den 3-Zykeln und den Doppeltranspositionen in S_4. Damit erhält man $\mathbb{T}^+ \cong A_4$.

(ii) *Würfelgruppe:* Es gilt $\mathbb{W}^+ \cong S_4$ und $\mathbb{W} \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$.

Beweis: Die orientierungserhaltende Symmetriegruppe $\mathbb{W}^+$ des Würfels operiert auf der vierelementigen Menge der Diagonalen, die je zwei gegenüberliegende Ecken des Würfels verbinden. Dadurch erhält man einen Homomorphismus $\psi : \mathbb{W}^+ \to S_4$. Eine Drehung, die alle Diagonalen festhält, stimmt mit $\mathrm{id}_{\mathbb{R}^3}$ überein; deshalb ist ψ injektiv.

Die Gruppe $\mathbb{W}^+$ besteht aus 24 Elementen. Neben $\mathrm{id}_{\mathbb{R}^3}$ sind dies 8 Drehungen um diese Diagonalen, 6 Drehungen um Achsen durch die Mitten gegenüberliegender Kanten, und 9 Drehungen um Achsen gegenüberliegender Seiten. Daraus kann wie beim Tetraeder geschlossen werden, dass $\mathbb{W}^+$ isomorph zu S_4 ist. Die volle Symmetriegruppe $\mathbb{W}$ ist ein inneres direktes Produkt von $\mathbb{W}^+$ und der zweielementigen Gruppe erzeugt von der Punktspiegelung am Koordinatenursprung, gegeben durch das Negative $-E_3$ der Einheitsmatrix. Daraus ergibt sich ein Isomorphismus $\mathbb{W} \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$.

(iii) *Ikosaedergruppe:* Es gilt $\mathbb{I}^+ \cong A_5$ und $\mathbb{I} \cong A_5 \times \mathbb{Z}/2\mathbb{Z}$.

Beweis: Der Ikosaeder enthält fünf verschiedene zueinander kongruente regelmäßige Oktaeder, deren Ecken mit Ecken des Ikosaders übereinstimmen. Die Gruppe des Ikosaeders operiert auf diesen Oktaedern. Dies liefert einen Homomorphismus der orientierungserhaltenden Ikosaedergruppe $\mathbb{I}^+$ nach S_5. Die Gruppe $\mathbb{I}^+$ besteht aus 60 Elementen, und anhand der Klassengleichung (siehe unten) kann man zeigen, dass $\mathbb{I}^+$ eine einfache Gruppe ist. Daraus kann gefolgert werden, dass φ injektiv ist und das Bild mit der alternierenden Gruppe

A_5 übereinstimmt. Es gilt also $\mathbb{I}^+ \cong A_5$. Wie beim Würfel zeigt man, dass für die volle Symmetriegruppe $\mathbb{I} \cong A_5 \times \mathbb{Z}/2\mathbb{Z}$ gilt.

Wenden wir uns nun als nächstem Thema der Formulierung der Bahngleichung zu.

Definition 7.10 Sei G eine Gruppe, die auf einer Menge X operiert, $\mathcal{B}$ die Menge der Bahnen dieser Operation und $\mathcal{S} \subseteq \mathcal{B}$ eine Teilmenge. Eine Teilmenge $R \subseteq X$ wird ***Repräsentantensystem*** von $\mathcal{S}$ genannt, wenn $G(x) \in \mathcal{S}$ für alle $x \in R$ gilt und die Abbildung $R \to \mathcal{S}$, $x \mapsto G(x)$ bijektiv ist.

Damit erhalten wir im Fall einer endlichen Menge X

Satz 7.11 *(Bahngleichung)*
Sei G eine Gruppe, die auf einer endlichen Menge X operiert. Sei $F \subseteq X$ die Fixpunktmenge der Operation und $R \subseteq X$ ein Repräsentantensystem der Menge aller Bahnen $G(x)$ mit mindestens zwei Elementen. Dann gilt

$$|X| \quad = \quad |F| + \sum_{x \in R} (G : G_x)$$

und $(G : G_x) > 1$ für alle $x \in R$.

Beweis: Sei $\mathcal{B}$ die Menge aller Bahnen, $\mathcal{S} \subseteq \mathcal{B}$ die Teilmenge aller Bahnen der Länge > 1 und $R \subseteq X$ ein Repräsentantensystem von $\mathcal{S}$. Weil die einelementigen Bahnen genau die Mengen $\{x\}$ mit $x \in F$ sind, ist $F \cup R$ ein Repräsentantensystem von $\mathcal{B}$, und die Mengen R und F sind disjunkt. Weil X die disjunkte Vereinigung der Mengen aus $\mathcal{B}$ ist und nach Definition des Repräsentantensystems für jedes $B \in \mathcal{B}$ genau ein $x \in F \cup R$ mit $B = G(x)$ existiert, gilt

$$\begin{aligned} |X| \quad &= \quad \sum_{B \in \mathcal{B}} |B| \quad = \quad \sum_{x \in F \cup R} |G(x)| \quad = \quad \sum_{x \in F} |G(x)| + \sum_{x \in R} |G(x)| \\ &= \quad \sum_{x \in F} |\{x\}| + \sum_{x \in R} |G(x)| \quad = \quad |F| + \sum_{x \in R} |G(x)|. \end{aligned}$$

Durch Anwendung von Satz 7.6 erhalten wir $|X| = |F| + \sum_{x \in R} (G : G_x)$. Aus der Voraussetzung $|G(x)| > 1$ folgt außerdem jeweils $(G : G_x) > 1$, für alle $x \in R$. □

Mit Hilfe der Zerlegung einer Menge X, auf der eine Gruppe G operiert, in die Bahnen dieser Operation, aus der wir soeben die Bahngleichung hergeleitet haben, lässt auch die Darstellung von Permutationen in disjunkte Zykel begründen.

Satz 7.12 Sei $n \in \mathbb{N}$. Dann besitzt jedes $\sigma \in S_n$ eine Darstellung $\sigma = \tau_1 \circ \ldots \circ \tau_r$ als Produkt paarweise disjunkter Zykel τ_j, und diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig bestimmt.

Beweis: Wir betrachten die Operation der zyklischen Untergruppe $G = \langle\sigma\rangle$ auf M_n. Es seien $B_1, ..., B_r$ die Bahnen dieser Operation mit mehr als einem Element (wobei genau dann $r = 0$ gilt, wenn $\sigma = \mathrm{id}$ ist). Für $1 \le j \le r$ setzen wir $k_j = |B_j|$ und definieren $\tau_j : M_n \to M_n$ durch $\tau_j|_{B_j} = \sigma|_{B_j}$ und $\tau_j(k) = k$ für $k \in M_n \setminus B_j$. Weil B_j eine Bahn unter der Operation von G ist, gilt $\sigma(B_j) \subseteq B_j$, und $\sigma|_{B_j}$ ist eine Bijektion $B_j \to B_j$. Dies zeigt, dass auch τ_j jeweils bijektiv und somit in S_n enthalten ist. Wie man leicht überprüft, stimmen σ und das Produkt $\tau_1 \circ ... \circ \tau_r$ sowohl auf jeder Bahn B_j als auch auf der Menge $F = M_n \setminus (B_1 \cup ... \cup B_r)$ überein. Bei Letzterem handelt es sich um die Fixpunktmenge der Operation von G auf M_n.

Um die Form der Permutationen τ_j näher zu bestimmen, bemerken wir zunächst, dass für jedes $a \in B_j$ das kleinste $\ell \in \mathbb{N}$ mit $\sigma^\ell(a) = a$ jeweils durch $\ell = k_j$ gegeben ist; denn andernfalls würde die Bahn $B_j = G(a)$ aus weniger als k_j Elementen bestehen. Wählen wir nun für $1 \le j \le r$ jeweils ein Element $a_j \in B_j$ beliebig und setzen dann $a_{j\ell} = \sigma^\ell(a_j)$ für $0 \le \ell < k_j$, dann muss also $B_j = \{a_{j0}, a_{j1}, ..., a_{j,k_j-1}\}$ gelten. Außerdem gilt $\tau_j(a_{j\ell}) = \sigma(a_{j\ell}) = a_{j,\ell+1}$ für $0 \le \ell < k_j - 1$ und $\tau_j(a_{j,k_j-1}) = \sigma(a_{j,k_j-1}) = a_{j0}$, sowie $\tau_j(k) = k$ für $k \notin B_j$. Dies zeigt, dass τ_j mit dem k_j-Zykel $(a_{j0}\ a_{j1}\ ...\ a_{j,k_j-1})$ übereinstimmt. Damit ist gezeigt, dass σ tatsächlich als Produkt von paarweise disjunkten Zyklen dargestellt werden kann.

Zum Nachweis der Eindeutigkeit nehmen wir nun an, dass $\sigma = \sigma_1 \circ ... \circ \sigma_s$ eine beliebige solche Darstellung ist. Dann sind die Bahnen der Operation von $G = \langle\sigma\rangle$ mit mehr als einem Element offenbar gegeben durch $\langle\sigma_i\rangle(b_i)$ für $1 \le i \le s$, wobei b_i jeweils ein beliebiges Element im Träger von σ_i bezeichnet. Die Menge dieser Bahnen muss mit $\{B_1, ..., B_r\}$ übereinstimmen. Es muss also $r = s$ gelten, und nach Umnummerierung der Zykel σ_i können wir $B_j = \langle\sigma_j\rangle(b_j)$ annehmen. Wegen $\sigma_j|_{B_j} = \sigma|_{B_j} = \tau_j|_{B_j}$ und $\sigma_j(k) = k = \tau_j(k)$ für $k \notin B_j$ stimmen die k_j-Zykel σ_j und τ_j überein. Damit ist die Eindeutigkeit bis auf Reihenfolge der Faktoren nachgewiesen. □

Proposition 7.13 Der Stabilisator eines Elements $h \in G$ unter der Operation durch Konjugation ist gegeben durch $C_G(h) = \{g \in G \mid gh = hg\}$. Die Fixpunkte der Operation sind die Elemente der Menge $Z(G) = \{g \in G \mid gh = hg \ \forall\ h \in G\}$, dem sogenannten ***Zentrum***. Auch $Z(G)$ ist eine Untergruppe, darüber hinaus sogar ein Normalteiler von G.

Beweis: Wir haben bereits oben die Bezeichnung $C_G(h)$ für den Stabilisator von $h \in G$ eingeführt. Für alle $g \in G$ gilt die Äquivalenz

$$g \in C_G(h) \quad \Leftrightarrow \quad g \cdot h = h \quad \Leftrightarrow \quad ghg^{-1} = h \quad \Leftrightarrow \quad gh = hg.$$

Ein Element $h \in G$ ist genau dann ein Fixpunkt der Operation, wenn $g \cdot h = h \Leftrightarrow gh = hg$ für alle $g \in G$ erfüllt ist. Dies ist gleichbedeutend damit, dass h in $Z(G)$ liegt.

Wir überprüfen nun die Untergruppen-Eigenschaft von $Z(G)$. Wegen $e_G g = g e_G$ für alle $g \in G$ ist e_G im Zentrum enthalten. Sind $g, h \in Z(G)$, dann gilt für jedes $g' \in G$ die Gleichung $g'(gh) = gg'h = (gh)g'$. Also ist auch das Produkt gh in $Z(G)$ enthalten. Außerdem ist $g'g^{-1} = (gg'^{-1})^{-1} = (g'^{-1}g)^{-1} = g^{-1}g'$, also $g^{-1} \in Z(G)$. Ist $g \in Z(G)$ und $h \in G$ beliebig, dann gilt $hgh^{-1} = ghh^{-1} = g \in Z(G)$. Damit ist auch die Normalteiler-Eigenschaft von $Z(G)$ nachgewiesen. □

Ist G eine Gruppe und N ein Normalteiler, dann gilt $gng^{-1} \in N$ für alle $g \in G$ und $n \in N$. Durch $G \times N \to N$, $g \cdot n = gng^{-1}$ ist also auch eine Operation von G auf N definiert.

Satz 7.14 *(Klassengleichung)*

Sei G eine endliche Gruppe, die durch Konjugation auf sich selbst operiert. Sei R ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element. Dann gilt

$$|G| \quad = \quad |Z(G)| + \sum_{g \in R} (G : C_G(g)).$$

Beweis: Dies ist ein Spezialfall der Bahngleichung, wenn man die Beschreibung der Fixpunktmenge und der Stabilisatoren aus Proposition 7.13 berücksichtigt. □

Besonders gut lässt sich die Klassengleichung anhand der symmetrischen Gruppen S_n illustrieren, denn hier sind die einzelnen Konjugationsklassen durch die Zerlegungstypen der Elemente gegeben, die wir in § 1 definiert haben.

Proposition 7.15 Sei $n \in \mathbb{N}$, und seien $\sigma, \sigma' \in S_n$ zwei nicht-triviale Elemente. Genau dann sind σ, σ' zueinander konjugiert, wenn sie denselben Zerlegungstyp besitzen.

Beweis: „⇒“ Seien σ, σ' zueinander konjugiert. Dann gilt es ein $\tau \in S_n$ mit $\sigma' = \tau\sigma\tau^{-1}$. Sei $\sigma = \sigma_1 \circ ... \circ \sigma_r$ eine disjunkte Zerlegung von σ, wobei die Zykellängen k_i durch $k_1 \geq ... \geq k_r$ geordnet sind. Definieren wir $\sigma'_i = \tau\sigma_i\tau^{-1}$ für $1 \leq i \leq r$, dann gilt $\sigma' = \sigma'_1 \circ ... \circ \sigma'_r$. Wir zeigen, dass σ'_i jeweils ein k_i-Zykel ist, für $1 \leq i \leq r$. Sei dazu $\mathrm{supp}(\sigma_i) = \{x_1, ..., x_{k_i}\}$, wobei $\sigma_i(x_\ell) = x_{\ell+1}$ für $1 \leq \ell < k_i$ und $\sigma_i(x_{k_i}) = x_1$ gilt. Setzen wir $x'_\ell = \tau(x_\ell)$, dann gilt $\sigma'_i(x'_\ell) = \tau\sigma_i\tau^{-1}(\tau(x_\ell)) = \tau\sigma(x_\ell) = \tau(x_{\ell+1}) = x'_{\ell+1}$ für $1 \leq i < k_i$ und ebenso

$$\sigma'_i(x'_{k_i}) \quad = \quad \tau\sigma_i\tau^{-1}(\tau(x_{k_i})) \quad = \quad \tau\sigma_i(x_{k_i}) \quad = \quad \tau(x_1) \quad = \quad x'_1.$$

Für $y \notin \{x'_1, ..., x'_{k_i}\}$ gilt $\tau^{-1}(y) \notin \{x_1, ..., x_{k_i}\}$ und somit $\sigma'_i(y) = \tau\sigma_i\tau^{-1}(y) = \tau\sigma_i(\tau^{-1}(y)) = \tau\tau^{-1}(y) = y$. Also ist σ'_i tatsächlich ein k_i-Zykel. Ebenso ist klar, dass die Träger der Zykel $\sigma'_1, ..., \sigma'_r$ disjunkt sind.

„⇐“ Nach Voraussetzung existieren disjunkte Zykelzerlegungen $\sigma = \sigma_1 \circ ... \circ \sigma_r$ und $\sigma' = \sigma'_1 \circ ... \circ \sigma'_r$, wobei σ_i und σ'_i jeweils dieselbe Zykellänge k_i haben, mit $k_1 \geq ... \geq k_r$. Sei $B_i = \mathrm{supp}(\sigma_i)$ und $B'_i = \mathrm{supp}(\sigma'_i)$ für $1 \leq i \leq r$, außerdem

$$B_0 = M_n \setminus (B_1 \cup ... \cup B_r) \qquad \text{und} \qquad B'_0 = M_n \setminus (B'_1 \cup ... \cup B'_r).$$

Wir ordnen die Elemente von B_i jeweils so an, dass $B_i = \{x_1, ..., x_{k_i}\}$ mit $\sigma_i(x_\ell) = x_{\ell+1}$ für $1 \leq \ell < k_i$ und $\sigma(x_{k_i}) = x_1$ gilt. Ebenso seien die Elemente in $B'_i = \{x'_1, ..., x'_{k_i}\}$ so angeordnet, dass $\sigma'_i(x'_\ell) = x'_{\ell+1}$ für $1 \leq \ell < k_i$ und $\sigma_i(x'_{k_i}) = x'_1$ gilt. Wir definieren nun $\tau_i : B_i \to B'_i$ durch $\tau_i(x_\ell) = x'_\ell$ und wählen eine beliebige Bijektion $\tau_0 : B_0 \to B'_0$. Definieren wir die Abbildung $\tau : M_n \to M_n$ durch $\tau(x) = \tau_i(x)$ für $x \in B_i$ und $i \in \{0, ..., r\}$, dann ist τ bijektiv, weil die Einschränkungen $\tau|_{B_i} : B_i \to B'_i$ für $0 \leq i \leq r$ bijektiv sind. Außerdem gilt $\sigma' = \tau \circ \sigma \circ \tau^{-1}$. Ist nämlich $x \in B'_i$ für ein $i \in \{1, ..., r\}$, $x = x'_\ell$ in der Notation von oben mit $1 \leq \ell < k_i$, dann folgt $\tau^{-1}(x) \in B_i$ und

$$\begin{aligned} \tau\sigma\tau^{-1}(x'_\ell) \quad &= \quad \tau\sigma(\tau^{-1}(x'_\ell)) \quad = \quad \tau\sigma_i(\tau^{-1}(x'_\ell)) \quad = \quad \tau\sigma_i(x_\ell) \quad = \quad \tau(x_{\ell+1}) \\ &= \quad x'_{\ell+1} \quad = \quad \sigma'_i(x'_\ell) \quad = \quad \sigma'(x'_\ell). \end{aligned}$$

Ebenso behandelt man den Fall, dass $x = x'_{k_i}$ ist. Im Fall $x \in B'_0$ gilt $\sigma'(x) = x$, und wegen $\tau^{-1}(x) \in B_0$ gilt auch $\tau\sigma\tau^{-1}(x) = \tau\sigma(\tau^{-1}(x)) = \tau(\tau^{-1}(x)) = x$. Insgesamt gilt also $\tau\sigma\tau^{-1} = \sigma'$. □

Der Beweis der Proposition zeigt, wie sich die Konjugation mit einem Element $\tau \in S_n$ konkret auf ein Element σ mit gegebener Zykelzerlegung auswirkt. Ist beispielsweise $\sigma = (1\ 2\ 3)(4\ 5)$ und $\tau \in S_5$ beliebig vorgegeben, dann gilt

$$\tau\sigma\tau^{-1} \quad = \quad (\ \tau(1)\ \tau(2)\ \tau(3)\ )(\ \tau(4)\ \tau(5)\ ) \tag{7.1}$$

Die Gleichung lässt sich auch direkt nachrechnen, indem man sich ansieht, auf welche Elemente $\tau(1)$, $\tau(2)$, ... durch die Permutation $\tau\sigma\tau^{-1}$ abgebildet werden.

Die Konjugationsklassen in S_n sind also durch die verschiedenen Zerlegungstypen der Elemente in S_n gegeben. Als nächstes schauen wir uns an, wie man die *Anzahl* der Elemente in den einzelnen Konjugationsklassen bestimmt.

Lemma 7.16 Sei $n \in \mathbb{N}$ und $2 \leq k \leq n$. Ist $A \subseteq M_n$ eine k-elementige Teilmenge, so beträgt die Anzahl der k-Zykel σ mit $\mathrm{supp}(\sigma) = A$ genau $(k-1)!$.

Beweis: Sei $A = \{x_1, ..., x_k\}$. Dann kann jeder k-Zykel σ mit Träger A in der Form $(x_1 x_{\tau(2)} ... x_{\tau(k)})$ geschrieben werden, wobei τ die Permutationen der Menge $\{2, ..., k\}$ durchläuft. Umgekehrt lässt sich aus einem gegebenen k-Zykel σ die Permutation τ zurückgewinnen: Für jedes $i \in \{2, ..., k\}$ ist $\tau(i)$ bestimmt durch die Gleichung $\sigma^{i-1}(x_1) = x_{\tau(i)}$. Da es $(k-1)!$ Permutationen von $\{2, ..., k\}$ gibt, folgt aus der bijektiven Korrespondenz zwischen k-Zykeln mit Träger A und Permutationen von $\{2, ..., k\}$ die Behauptung. □

Folgerung 7.17 Für $n \in \mathbb{N}$ und $k \in \{2, ..., n\}$ gibt es jeweils genau $(k-1)!\binom{n}{k}$ k-Zykel.

Beweis: Für die Auswahl einer k-elementigen Teilmenge $A \subseteq M_n$ gibt es $\binom{n}{k}$ Möglichkeiten, und für jede solche Menge A gibt es auf Grund des Lemmas dann $(k-1)!$ verschiedene k-Zykel mit Träger A. □

Es ist nicht schwierig, daraus eine Formel abzuleiten, die die Anzahl der Elemente eines *beliebigen* Zerlegungstyps liefert.

(i) Sei $(k_1, ..., k_r)$ ein Zerlegungstyp von Elementen der S_n, wobei wir zunächst annehmen, dass die Zykellängen $k_1 > k_2 > ... > k_r \geq 2$ erfüllen, also keine Zykellänge mehrfach vorkommt. Für $1 \leq i \leq r$ sei $s_i = \sum_{j=1}^{i-1} k_j$. Dann ist die Anzahl der Elemente dieses Zerlegungstyps gegeben durch

$$\prod_{i=1}^{r} (k_i - 1)! \binom{n - s_i}{k_i}.$$

Dies kommt durch eine einfache kombinatorische Überlegung zu Stande: Um ein Element des angegebenen Typs zu bilden, hat man zunächst $\binom{n}{k_1}$ Möglichkeiten, den Träger des k_1-Zykels zu wählen. Für die Wahl des k_2-Zykels bleiben dann noch $\binom{n-k_1}{k_2}$ Möglichkeiten, für die des k_3-Zykels $\binom{n-k_1-k_2}{k_3}$ Möglichkeiten usw.

(ii) Sei nun $(k_1, ..., k_r)$ ein beliebiger Zerlegungstyp von Elementen der S_n, und für $1 \leq \ell \leq n$ sei a_ℓ jeweils die Anzahl der k_j mit $k_j = \ell$. Dann ist die Anzahl der Elemente des Zerlegungstyps gegeben durch

$$\prod_{\ell=1}^{n}(a_\ell!)^{-1} \cdot \prod_{i=1}^{r}(k_i-1)!\binom{n-s_i}{k_i}.$$

Diese Formel erhält man durch die folgende Überlegung: Wie im vorherigen Abschnitt sieht man, dass die Formel ohne den Vorfaktor $\prod_{\ell=1}^{n}(a_\ell!)^{-1}$ die Anzahl der Möglichkeiten liefert, zunächst den k_1-Zykel, dann den k_2-Zykel usw. zu wählen. Sei nun ℓ eine Zykellänge, die im Tupel $(k_1, ..., k_r)$ insgesamt a_l-mal auftritt. Dann wird durch diese Vorgehensweise dasselbe Produkt von a_ℓ Zykeln der Länge ℓ mehrmals, nämlich genau $a_\ell!$ mal gewählt, wobei zu berücksichtigen ist, dass die paarweise disjunkten ℓ-Zykel vertauschbar sind und somit die Reihenfolge der Faktoren keine Rolle spielt. Dieser Tatsache wird dadurch Rechnung getragen, dass wir das Produkt mit dem „Korrekturfaktor“ $(a_\ell!)^{-1}$ multiplizieren.

Wir haben bereits festgestellt, dass die Zerlegungstypen in $G = S_4$ neben der Identität durch Zykel der Länge 2, 3, 4 und Doppeltranspositionen der Form $(a\ b)(c\ d)$ gegeben sind. Für die 2-, 3- und 4-Zykel erhält man durch Einsetzen in die Formel 7.17 die Anzahlen 6, 8 und 6, und es ist leicht zu sehen, dass es genau drei Doppeltranspositionen gibt. Die Operation durch Konjugation liefert also eine Zerlegung der Gruppe in fünf Bahnen der Längen 1, 6, 8, 6, 3; insbesondere gibt es nur einen einzigen Fixpunkt. Das heißt also, dass S_4 ein triviales Zentrum besitzt. Ein Repräsentantensystem der Bahnen der Länge > 1 ist zum Beispiel durch

$$R \quad = \quad \{(1\ 2), (1\ 2\ 3), (1\ 2\ 3\ 4), (1\ 2)(3\ 4)\}$$

gegeben, und die Klassengleichung für $G = S_4$ hat die Form

$$24 \quad = \quad 1 + 6 + 8 + 6 + 3.$$

Nach demselben Schema kann die Klassengleichung von S_n für beliebiges $n \in \mathbb{N}$ aufgestellt werden. Wegen $S_1 = \{\mathrm{id}\}$ gibt es nur eine Konjugationsklasse in S_1. Wir geben nun die Konjugationsklassen von S_n sowie ihre Größen für $2 \leq n \leq 7$ an.

n = 2

Zerlegungstyp		(2)
Repräsentant	id	(1 2)
Anzahl	1	1

n = 3

Zerlegungstyp		(2)	(3)
Repräsentant	id	(1 2)	(1 2 3)
Anzahl	1	3	2

n = 4

Zerlegungstyp		(2)	(3)	(4)	(2, 2)
Repräsentant	id	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
Anzahl	1	6	8	6	3

n = 5

Zerlegungstyp		(2)	(3)	(4)	(5)	(2, 2)	(3, 2)
Repräsentant	id	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2)(3 4)	(1 2 3)(4 5)
Anzahl	1	10	20	30	24	15	20

n = 6

Zerlegungstyp		(2)	(3)	(4)	(5)	(6)
Repräsentant	id	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2 3 ... 6)
Anzahl	1	15	40	90	144	120
Zerlegungstyp	(6)	(2,2)	(3,2)	(3,3)	(2,2,2)	(4,2)
Repräsentant	(1 2 3 ... 6)	(1 2)(3 4)	(1 2 3)(4 5)	(1 2 3)(4 5 6)	(1 2)(3 4)(5 6)	(1 2 3 4)(5 6)
Anzahl	120	45	120	40	15	90

n = 7

Zerlegungstyp		(2)	(3)	(4)	(5)
Repräsentant	id	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 ... 5)
Anzahl	1	21	70	210	504
Zerlegungstyp	(6)	(7)	(2,2)	(3,2)	(3,3)
Repräsentant	(1 2 3 ... 6)	(1 2 3 ... 7)	(1 2)(3 4)	(1 2 3)(4 5)	(1 2 3 4 5 6)
Anzahl	840	720	105	420	280
Zerlegungstyp	(2,2,2)	(3,2,2)	(4,2)	(4,3)	(5,2)
Repräsentant	(1 2)(3 4)(5 6)	(1 2 3)(4 5)(6 7)	(1 2 3 4)(5 6)	(1 2 3 4)(5 6 7)	(1 2 3 4 5)(6 7)
Anzahl	105	210	630	420	504

Nun beschäftigen wir uns noch mit der Klassengleichung der alternierenden Gruppen A_n. Zunächst einmal ist auf Grund der Rechenregeln für das Signum klar, dass das Signum jedes Elements in S_n nur von seiner Konjugationsklasse abhängt. Außerdem ist offenbar jede A_n-Konjugationsklasse $A_n(\sigma)$ in der entsprechenden S_n-Konjugationsklasse $S_n(\sigma)$ enthalten. Es stellt sich aber die Frage, ob $A_n(\sigma)$ eine echte Teilmenge von $S_n(\sigma)$ ist, oder ob die Konjugationsklassen übereinstimmen. Das folgende Lemma zeigt wegen $(S_n : A_n) = 2$, dass jede Konjugationsklasse $S_n(\sigma)$ entweder auch eine A_n-Konjugationsklasse ist oder in genau zwei A_n-Konjugationsklassen zerfällt.

> **Lemma 7.18** Sei G eine endliche Gruppe, die auf einer endlichen Menge X operiert, und sei U eine Untergruppe vom Index $n = (G : U)$. Sei R ein Repräsentantensystem von $U\backslash G$. Dann gilt für jedes $x \in X$ jeweils $G(x) = \bigcup_{a\in R} U(a \cdot x)$, und alle Mengen $U(a \cdot x)$ auf der rechten Seite der Gleichung sind gleichmächtig.

Beweis: Die Inklusion „$\supseteq$“ ist nach Definition erfüllt. Für den Nachweis von „$\subseteq$“ sei $y \in G(x)$ vorgegeben. Dann gilt $y = g \cdot x$ für ein $x \in X$. Weil R ein Repräsentantensystem von $U\backslash G$ ist, existiert ein $a \in R$ mit $g \in Ua$. Schreiben wir $g = ua$ mit einem geeigneten $u \in U$, dann folgt $y = g \cdot x = (ua) \cdot x = u \cdot (a \cdot x) \in U(a \cdot x)$.

Nun zeigen wir für vorgegebenes $a \in R$, dass die Mengen $U(x)$ und $U(a \cdot x)$ gleichmächtig sind. Dazu beweisen wir die Gleichung $U_{a\cdot x} = aU_x a^{-1}$. Ist $h \in U_{a\cdot x}$, dann gilt $h \cdot (a \cdot x) = a \cdot x$. Daraus folgt

$$(a^{-1}ha) \cdot x \quad = \quad a^{-1} \cdot (h \cdot (a \cdot x)) \quad = \quad a^{-1} \cdot (a \cdot x) \quad = \quad (a^{-1}a) \cdot x \quad = \quad e \cdot x \quad = \quad x.$$

Also liegt $u = a^{-1}ha$ in U_x, und es folgt $h = aua^{-1} \in aU_x a^{-1}$. Sei nun umgekehrt $h \in aU_x a^{-1}$ vorgegeben , also $h = aua^{-1}$ mit einem Element $u \in U_x$. Dann folgt

$$h \cdot (a \cdot x) \quad = \quad (aua^{-1}) \cdot (a \cdot x) \quad = \quad (au) \cdot (a^{-1} \cdot (a \cdot x)) \quad = \quad (au) \cdot ((a^{-1}a) \cdot x) \quad =$$
$$(au) \cdot (e \cdot x) \quad = \quad (au) \cdot x \quad = \quad a \cdot (u \cdot x) \quad = \quad a \cdot x$$

und somit $h \in U_{a\cdot x}$. Damit ist die Gleichung bewiesen. Da durch $u \mapsto aua^{-1}$ eine Bijektion zwischen U_x und aU_xa^{-1} gegeben ist (mit $u \mapsto a^{-1}ua$ als Umkehrabbildung), folgt daraus $|U_x| = |aU_xa^{-1}| = |U_{a\cdot x}|$. Der Zusammenhang zwischen Bahnlänge und Index des Stabilisators, Satz 7.6, liefert nun

$$|U(x)| \quad = \quad (G : U_x) \quad = \quad \frac{|G|}{|U_x|} \quad = \quad \frac{|G|}{|U_{a\cdot x}|} \quad = \quad (G : U_{a\cdot x}) \quad = \quad |U(a \cdot x)|. \qquad \square$$

Die folgende Proposition gibt Auskunft darüber, welcher der beiden Fälle für jede Konjugationsklasse $S_n(\sigma)$ mit $\sigma \in A_n$ jeweils vorliegt.

> **Proposition 7.19** Sei $n \in \mathbb{N}$ mit $n \geq 2$, und sei $\sigma \in A_n$ ein Element ungleich dem Neutralelement mit Zerlegungstyp $(k_1, ..., k_r)$. Sind alle k_i ungerade und voneinander verschieden, also $k_1 > k_2 > ... > k_r$, und hat σ höchstens einen Fixpunkt, dann zerfällt $S_n(\sigma)$ in zwei verschiedene A_n-Konjugationsklassen. Andernfalls gilt $S_n(\sigma) = A_n(\sigma)$.

Beweis: Setzen wir zunächst voraus, dass $k_1 > ... > k_r \geq 3$ gilt und alle Werte k_i ungerade sind. Sei $\sigma_1 = (i_1\ i_2\ ...\ i_{k_1})$ der Zykel der Länge k_1 in der disjunkten Zykelzerlegung von σ, und sei $\tau = (i_1\ i_2)$. Wir zeigen, dass σ und $\sigma' = \tau\sigma\tau^{-1}$ in A_n nicht zueinander konjugiert, die Konjugationsklassen $A_n(\sigma)$ und $A_n(\sigma')$ also verschieden sind. Da σ und σ' in S_n zueinander konjugiert sind, hat auch σ' den Zerlegungstyp $(k_1, ..., k_r)$. Nehmen wir nun an, dass ein $\rho \in A_n$ mit $\sigma' = \rho\sigma\rho^{-1}$ existiert, und seien $\sigma_1, \sigma_2, ..., \sigma_r$ die Elemente in der disjunkten Zykelzerlegung von σ. Wegen $\rho\sigma\rho^{-1} = \sigma' = \tau\sigma\tau^{-1}$ und der Eindeutigkeit der disjunkte Zykelzerlegung muss dann $\rho\sigma_j\rho^{-1} = \sigma_j$ für $2 \leq j \leq r$ und $\rho\sigma_1\rho^{-1} = \tau\sigma_1\tau^{-1}$. Außerdem muss der einzige Fixpunkt von σ, sofern er existiert, von ρ auf sich selbst abgebildet werden.

Die Gleichung $\rho\sigma_j\rho^{-1} = \sigma_j$ für $2 \leq j \leq r$ zeigt, dass $\rho_j = \rho|_{\mathrm{supp}(\sigma_j)}$ entweder die Identität ist oder die Elemente von $\mathrm{supp}(\sigma_j)$ in der Reihenfolge, in der sie in σ_j auftreten, zyklisch vertauscht. Ist nämlich $\sigma_j = (m_1\ m_2\ ...\ m_{k_j})$, so gilt $\rho\sigma_j\rho^{-1} = \sigma_j$ genau dann, wenn ρ_j mit der Identität oder einem der folgenden Elemente übereinstimmt.

$$\begin{pmatrix} m_1 & m_2 & m_3 & \cdots & m_{k_j} \\ m_2 & m_3 & m_4 & \cdots & m_1 \end{pmatrix} \quad , \quad \begin{pmatrix} m_1 & m_2 & m_3 & \cdots & m_{k_j} \\ m_3 & m_4 & m_5 & \cdots & m_2 \end{pmatrix} \quad , ..., \quad \begin{pmatrix} m_1 & m_2 & m_3 & \cdots & m_{k_j} \\ m_{k_j} & m_1 & m_2 & \cdots & m_{k_j-1} \end{pmatrix}.$$

Dies zeigt, dass ρ_j eine Potenz eines k_j-Zykels (nämlich eine Potenz des zuerst angezeigten Elements) ist. Da k_j ungerade ist, ist das Signum von ρ_j positiv. Aus demselben Grund folgt aus $\rho\sigma_1\rho^{-1} = \tau\sigma_1\tau^{-1}$, dass $\rho_1 = \rho|_{\mathrm{supp}(\sigma_1)} = \rho|_{\{i_1,...,i_{k_1}\}}$ ein Produkt von τ und einer Potenz des Zykels $(i_1\ i_2\ ...\ i_{k_1})$ ist und somit negatives Signum besitzt. Wegen $\rho = \rho_1 \circ ... \circ \rho_r$ gilt insgesamt $\mathrm{sgn}(\rho) = -1$, im Widerspruch zur Annahme $\rho \in A_n$. Dies zeigt, dass tatsächlich $A_n(\sigma) \neq A_n(\sigma')$ gilt.

Betrachten wir nun den Fall, dass in der disjunkten Zykelzerlegung von σ zwei Zykel $(i_1\ ...\ i_r)$ und $(j_1\ ...\ j_r)$ derselben ungeraden Länge vorkommen, wobei wir auch den Fall $r = 1$ zulassen. Wir definieren das Element $\tau \in S_n$ durch $\tau = (i_1\ j_1) \circ ... \circ (i_r\ j_r)$. Konjugiert man nun σ mit dem Element τ, dann werden in der disjunkten Zykelzerlegung die beiden angegebenen r-Zykel vertauscht, während die übrigen Zykel unverändert bleiben. Es gilt also $\tau\sigma\tau^{-1} = \sigma$. Weil r ungerade ist, gilt $\mathrm{sgn}(\tau) = -1$. Daraus folgt nun $S_n(\sigma) = A_n(\sigma)$, die S_n-Konjugationsklasse von σ zerfällt also nicht in zwei A_n-Konjugationsklassen. Sei nämlich $\rho \in S_n(\sigma)$ vorgegeben. Dann gibt es ein $\tau_1 \in S_n$ mit $\rho = \tau_1\sigma\tau_1^{-1}$. Gilt $\tau_1 \in A_n$, dann folgt unmittelbar daraus $\rho \in A_n(\sigma)$. Andernfalls gilt $\mathrm{sgn}(\tau_1\tau) = (-1)(-1) = 1$ und somit ebenfalls $\rho = \tau_1\sigma\tau_1^{-1} = \tau_1\tau\sigma\tau^{-1}\tau_1^{-1} = (\tau_1\tau)\sigma(\tau_1\tau)^{-1} \in A_n(\sigma)$.

Nehmen wir nun an, dass in der disjunkten Zykelzerlegung von σ ein Zykel $\sigma_1 = (i_1 \dots i_r)$ gerader Länge r vorkommt. Konjugieren wir diesen Zykel mit sich selbst, dann ergibt sich wegen $\sigma_1\sigma_1\sigma_1^{-1} = \sigma_1$ keine Änderung. Konjugation der übrigen Zykel in der disjunkten Zykelzerlegung mit σ führt ebenfalls zu keiner Änderung, da der Träger $\{i_1, \dots, i_r\}$ von σ_1 zum Träger jedes anderen Zykels disjunkt ist. Insgesamt gilt also $\sigma_1\sigma\sigma_1^{-1} = \sigma$. Weil r gerade ist, ist das Signum von σ_1 negativ. Wie im vorherigen Absatz kann daraus nun geschlossen werden, dass $S_n(\sigma) = A_n(\sigma)$ gilt. □

Wir gehen nun mit Hilfe von Proposition 7.19 die Fälle $n \leq 2 \leq 7$ durch, um die Klassengleichung von A_n für diese Fälle explizit anzugeben.

- Im Fall $n = 2$ ist A_n trivial, die Klassengleichung also die triviale Gleichung $1 = 1$.
- Im Fall $n = 3$ liegt neben $\{\mathrm{id}\}$ nur eine Konjugationsklasse von S_3 auch in A_3, nämlich die Klasse der 3-Zykel. Auf Grund der Proposition zerfällt diese 2-elementige S_3-Klasse in zwei A_3-Klassen mit jeweils einem Element. Die Klassengleichung lautet also $3 = 1 + 1 + 1$.
- Im Fall $n = 4$ sind neben $\{\mathrm{id}\}$ die S_4-Konjugationsklasse der 3-Zykel und die S_4-Konjugationsklasse der Doppeltranspositionen in A_4 enthalten. Lediglich die 8-elementige Konjugationsklasse der 3-Zykel zerfällt in zwei A_4-Konjugationsklassen. Die Klassengleichung lautet also $12 = 1 + 4 + 4 + 3$.
- Im Fall $n = 5$ liegen neben $\{\mathrm{id}\}$ die 3-Zykel, die 5-Zykel und die Doppeltranspositionen in A_5. Nur die 24-elementige Klasse der 5-Zykel zerfällt. Wir erhalten die Klassengleichung $60 = 1 + 20 + 12 + 12 + 15$.
- Im Fall $n = 6$ liegen neben $\{\mathrm{id}\}$ die 3-Zykel, die 5-Zykel, die Doppeltranspositionen und die Elemente der Zerlegungstypen $(3,3)$ und $(4,2)$ in A_6. Nur die Klasse der 5-Zykel zerfällt. Daraus ergibt sich die Klassengleichung $360 = 1 + 40 + 72 + 72 + 45 + 40 + 90$.
- Im Fall $n = 7$ liegen neben $\{\mathrm{id}\}$ die 3-, 5- und 7-Zykel, die Doppeltranspositionen und die Elemente der Zerlegungstypen $(3,3)$, $(3,2,2)$ und $(4,2)$ in A_7. Hier zerfällt nur die Klasse der 7-Zykel. Wir erhalten die Klassengleichung $2520 = 1 + 70 + 504 + 360 + 360 + 105 + 280 + 210 + 630$.

Im folgenden Abschnitt dieses Kapitels verwenden wir die Klassengleichung zur Untersuchung endlicher Gruppen mit Primzahlpotenzordnung.

Definition 7.20 Sei p eine Primzahl. Eine endliche Gruppe G wird als p-***Gruppe*** bezeichnet, wenn sie von p-Potenzordnung ist, also $|G| = p^e$ für ein $e \in \mathbb{N}_0$ erfüllt ist.

Wir werden nun mit Hilfe der Klassengleichung einige wichtige Eigenschaften der p-Gruppen herleiten.

Satz 7.21 Sei G eine nichttriviale p-Gruppe. Dann ist das Zentrum $Z(G)$ von G ebenfalls nichttrivial, besteht also aus mindestens p Elementen.

Beweis: Sei $r \in \mathbb{N}$ mit $|G| = p^r$. Wir stellen für die Gruppe G die Klassengleichung auf. Sei R ein Repräsentantensystem der Konjugationsklassen von G, die aus mehr als einem Element bestehen. Nach Satz 7.14 gilt dann

$$|G| \quad = \quad |Z(G)| + \sum_{g \in R} (G : C_G(g)).$$

Die Zahl $|G|$ ist nach Voraussetzung durch p teilbar. Die Indizes $(G : C_G(g))$ sind Teiler > 1 von p^r und wegen $(G : C_G(g)) > 1$ somit ebenfalls Vielfache von p. Damit muss auch $|Z(G)|$ durch p teilbar sein. Wegen $e_G \in Z(G)$ ist $|Z(G)| > 0$, und das kleinste positive Vielfache von p ist die Zahl p selbst. □

Lemma 7.22 Ist G eine Gruppe mit der Eigenschaft, dass die Faktorgruppe $G/Z(G)$ zyklisch ist, dann ist G selbst abelsch.

Beweis: Sei $N = Z(G)$ und $g \in G$ so gewählt, dass $\bar{g} = gN$ die Faktorgruppe G/N erzeugt. Seien außerdem $g_1, g_2 \in G$ beliebig vorgegeben. Zu zeigen ist die Gleichung $g_1 g_2 = g_2 g_1$. Wegen $G/N = \langle \bar{g} \rangle$ gibt es $m, n \in \mathbb{Z}$ mit $g_1 N = \bar{g}^m$, $g_2 N = \bar{g}^n$. Insbesondere gilt $g_1 \in g^m N$, $g_2 \in g^n N$, also gibt es Elemente $a, b \in N$ mit $g_1 = g^m a$ und $g_2 = g^n b$. Weil a und b als Elemente des Zentrums mit jedem Gruppenelement vertauschbar sind, erhalten wir

$$g_1 g_2 \quad = \quad g^m a g^n b \quad = \quad g^m g^n a b \quad = \quad g^{m+n} a b \quad = \quad g^n g^m a b \quad = \quad g^n b g^m a \quad = \quad g_2 g_1. \qquad \square$$

Satz 7.23 Sei p eine Primzahl. Dann ist jede Gruppe der Ordnung p^2 abelsch. Bis auf Isomorphie sind also $\mathbb{Z}/p^2\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ die einzigen Gruppen der Ordnung p^2.

Beweis: Sei G eine Gruppe mit $|G| = p^2$. Als p-Gruppe besitzt G nach Satz 7.21 ein nichttriviales Zentrum $Z(G)$. Da $|Z(G)|$ ein Teiler von p^2 ist, kann somit nur $|Z(G)| = p$ oder $|Z(G)| = p^2$ gelten. Im Fall $|Z(G)| = p^2$ gilt $Z(G) = G$. Jedes Element aus G ist dann mit jedem anderen vertauschbar, also ist G abelsch. Im Fall $|Z(G)| = p$ ist $|G/Z(G)| = \frac{p^2}{p} = p$ von Primzahlordnung, die Faktorgruppe $G/Z(G)$ also zyklisch und G nach Lemma 7.22 abelsch. □

Satz 7.24 Jede p-Gruppe ist auflösbar.

Beweis: Sei G eine p-Gruppe, $|G| = p^n$ für ein $n \in \mathbb{N}_0$. Wir beweisen die Aussage durch vollständige Induktion über n. Für $n \leq 2$ ist G nach Satz 7.8 abelsch und somit auflösbar. Sei nun $n \geq 3$, und setzen wir die Aussage für Werte kleiner als n voraus. Nach Satz 7.21 ist $Z(G)$ eine nichttrivale Untergruppe von G, wegen Proposition 7.13 darüber hinaus ein Normalteiler von G. Ist $G = Z(G)$, dann ist G wiederum abelsch und damit auflösbar. Ansonsten sind durch $Z(G)$ und $G/Z(G)$ zwei p-Gruppen kleinerer Ordnung als G gegeben, so dass wir die Induktionsvoraussetzung anwenden können. Also sind $Z(G)$ und $G/Z(G)$ auflösbar. Nach Satz 6.12 (ii) folgt daraus auch die Auflösbarkeit von G. □

Als weitere Anwendung der Klassengleichung leiten wir die Einfachheit der alternierenden Gruppen ab.

Satz 7.25 Die Gruppe A_n ist nicht einfach für $n = 4$, für alle übrigen $n \geq 2$ einfach.

Beweis: Die Gruppe A_4 ist nicht einfach, denn wie wir bereits im Beweis von Satz 6.13 gesehen haben, ist die Kleinsche Vierergruppe $V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ ein nichttrivialer Normalteiler von A_4. Die Gruppe A_2 besteht nur aus dem Element id und ist somit einfach. Die Gruppe A_3 hat die Primzahlordnung 3. Aus dem Satz von Lagrange folgt, dass A_3 nur Untergruppen der Ordnung 1 und 3 in A_3 gibt. Also sind $\{\mathrm{id}\}$ und A_3 die einzigen Untergruppen von A_3, somit erst recht die einzigen Normalteiler, und folglich ist A_3 einfach.

Der eigentlich interessante Teil des Beweises ist der Nachweis der Einfachheit von A_n für $n \geq 5$. Betrachten wir zunächst den Fall $n = 5$. Wir haben in Abschnitt (4) gesehen, dass die Klassengleichung von A_5 durch

$$60 \quad = \quad 1 + 20 + 12 + 12 + 15$$

gegeben ist. Nehmen wir nun an, dass N ein nichttrivialer Normalteiler von G ist. Ist C eine Konjugationsklasse, dann gilt entweder $C \cap N = \emptyset$ oder $C \subseteq N$. Ist nämlich $n \in C \cap N$, dann gilt $gng^{-1} \in N$. Dies zeigt, dass die gesamte Konjugationsklasse $[n] = \{gng^{-1} \mid g \in G\}$ von n in N enthalten ist. Dies bedeutet, dass N als disjunkte Vereinigung von A_5-Konjugationsklassen dargestellt werden kann, wobei $\{\mathrm{id}\}$ wegen $\mathrm{id} \in N$ eine dieser Klassen sein muss. Da jede Konjugationsklasse außer $\{\mathrm{id}\}$ mindestens 12 Elemente enthält, muss $|N| \geq 13$ gelten. Andererseits muss die Ordnung $|N|$ ein Teiler von 60 ungleich $1, 60$ sein. Dies lässt als einzige Möglichkeiten $|N| \in \{15, 20, 30\}$ zu.

Auf Grund der Zerlegung von N in A_5-Konjugationsklassen müsste es nun möglich sein, $|N|$ als Summe der Form $1 + d_1 + \ldots + d_r$ darzustellen, wobei $r \in \mathbb{N}$ und $d_1, \ldots, d_r \in \{12, 15, 20\}$ gilt, wobei 12 in der Summe zweimal, 15 und 20 höchstens einmal vorkommen. Wegen $d_i \geq 12$ genügt es, Summen mit $r \geq 2$ zu betrachten, denn im Fall $r \geq 3$ wäre bereits $1 + d_1 + \ldots + d_r \geq 1 + 12 + 12 + 15 = 40 > 30$. Wie man sich leicht überzeugt, stimmt aber keine der Zahlen

$$1 + 12 \quad , \quad 1 + 15 \quad , \quad 1 + 20 \quad , \quad 1 + 12 + 12 \quad , \quad 1 + 12 + 15 \quad , \quad 1 + 12 + 20 \quad , \quad 1 + 15 + 20$$

mit 15, 20 oder 30 überein. Also kann es in A_5 keinen Normalteiler $N \neq \{\mathrm{id}\}, A_5$ geben, und die Gruppe A_5 ist einfach.

Nun beweisen wir die Einfachheit von A_n für alle $n \geq 5$ durch vollständige Induktion, wobei der Induktionsanfang bereits erledigt ist. Wir setzen die Aussage nun für ein solche n voraus und beweisen sie für $n + 1$. Nehmen wir an, dass N ein nichttrivialer Normalteiler von A_{n+1} ist. Für $1 \leq i \leq n + 1$ sei $G_i = \{\sigma \in S_{n+1} \mid \sigma(i) = i\}$, der Stabilisator von i in S_n. Wie wir am Anfang des Kapitels (bei der Definition der Stabilisatorgruppen) bemerkt haben, gilt $G_i \cong S_n$ für jedes i, und dieser Isomorphismus ändert das Signum der Permutationen nicht, da lediglich ein Fixpunkt aus dem Definitionsbereich entfernt wird und somit der Zerlegungstyp gleich bleibt. Durch Einschränkung des Isomorphismus auf $H_i = G_i \cap A_n$ erhält man somit einen Isomorphismus $\phi_i : H_i \to A_n$.

Wegen $N \trianglelefteq A_n$ gilt $N \cap H_i \trianglelefteq H_i$ für $1 \leq i \leq n+1$. Sind nämlich $n \in N \cap H_i$ und $h \in H_i$ vorgegeben, dann gilt $hnh^{-1} \in N$ auf Grund der Normalteiler-Eigenschaft und $hnh^{-1} \in H_i$ auf Grund der Untergruppen-Eigenschaft von H_i, insgesamt also $hnh^{-1} \in N \cap H_i$. Wegen $H_i \cong A_n$ ist auch H_i einfach, es sind also $\{\mathrm{id}\}$ und H_i die einzigen Normalteiler. Somit gilt für $1 \leq i \leq n + 1$ jeweils $N \cap H_i = \{\mathrm{id}\}$ oder $N \cap H_i = H_i$.

Nehmen wir zunächst an, es gilt $N \cap H_j = H_j$ für ein j. Wie man sich leicht überzeugt, ist H_j in A_{n+1} zu jeder der Gruppen $H_1, ..., H_{n+1}$ konjugiert; bezeichnet $\sigma_i \in A_{n+1}$ ein beliebiges Element mit $\sigma_i(j) = i$, dann gilt $H_i = \sigma_i H_j \sigma_i^{-1}$. Auf Grund der Normalteilereigenschaft gilt

$$N \cap H_i \quad = \quad N \cap \sigma_i H_j \sigma_i^{-1} \quad = \quad \sigma_i N \sigma_i^{-1} \cap \sigma_i H_j \sigma_i^{-1} \quad = \quad \sigma_i (N \cap H_j) \sigma_i^{-1} \quad = \quad \sigma_i H_j \sigma_i^{-1} \quad = \quad H_i.$$

Aus $N \cap H_i = H_i$ folgt $N \supseteq H_i$, für $1 \leq i \leq n+1$. Jeder 3-Zykel aus A_{n+1} ist in einer der Untergruppen H_i enthalten. Also enthält N alle 3-Zykel. Weil Mit Satz 2.11 (ii) folgt daraus $N = A_{n+1}$, im Widerspruch zur Annahme von oben. Also muss $N \cap H_i = \{\mathrm{id}\}$ für $1 \leq i \leq n+1$ gelten. Es gibt in N also kein nichttriviales Element ohne Fixpunkt. Daraus folgt auch, dass es in N keine zwei verschiedenen Elemente gibt, die auf einem $i \in M_{n+1}$ denselben Wert haben. Denn wäre $\sigma(i) = \tau(i)$ für $\sigma, \tau \in N$, dann würde daraus $(\tau^{-1}\sigma)(i) = i$ folgen.

Sei nun $\sigma \in N$ ein nichttriviales Element, und sei $(k_1, ..., k_r)$ der Zerlegungstyp von σ. Nehmen wir an, dass in der disjunkten Zykelzerlegung von σ ein r-Zykel σ_1 mit $r \geq 3$ vorkommt, also $k_1 \geq 3$ gilt. Sei $\sigma_1 = (i_1\ i_2\ \cdots\ i_r)$. Sei $\tau = (i_3\ j\ k)$ mit $j, k \neq \{i_1, i_2, i_3\}$; ein solches Element existiert wegen $n+1 \geq 6$. Setzen wir $\sigma' = \tau\sigma\tau^{-1}$, dann ist σ' wegen $\tau \in A_{n+1}$ und $N \trianglelefteq A_{n+1}$ ebenfalls in N enthalten. Die disjunkte Zykelzerlegung von σ' enthält dann den k-Zykel $\sigma_1' = (i_1\ i_2\ j\ \cdots\ i_r)$. Wegen $\sigma(i_2) = i_3$ und $\sigma'(i_2) = j \neq i_3$ gilt dann $\sigma \neq \sigma'$, andererseits aber $\sigma(i_1) = i_2 = \sigma'(i_1)$. Aber das zwei verschiedene Elemente aus N an einer Stelle das gleiche Bild haben, wurde oben ausgeschlossen.

Als einzige Möglichkeit bleibt somit, dass jedes nichttriviale Element aus N ein Produkt von disjunkten Transpositionen ist. Sei $\sigma \in N \setminus \{\mathrm{id}\}$ und $\sigma = \sigma_1 ... \sigma_r$ eine solche Zerlegung. Sei $\sigma_1 = (i\ j)$ und $\sigma_2 = (k\ \ell)$, außerdem $\tau = (\ell\ p\ q)$, wobei $p, q \in M_{n+1}$ so gewählt sind, dass $p \neq q$ und $p, q \notin \{i, j, k, \ell\}$. Solche Elemente existieren wiederum wegen $n+1 \geq 6$. Setzen wir $\sigma' = \tau\sigma\tau^{-1}$, dann sind die Transpositionen $(i\ j)$ und $(k\ p)$ in der disjunkten Zykelzerlegung von σ' enthalten. Wegen $\sigma(k) = \ell$ und $\sigma'(k) = p \neq \ell$ sind σ und σ' zwei verschiedene Elemente aus N. Andererseits gilt $\sigma(i) = j = \sigma'(i)$, was erneut unserer Feststellung von oben widerspricht. Also existieren in N kein nichttrivialen Elemente. Aber den Fall $N = \{\mathrm{id}\}$ haben wir ebenfalls oben ausgeschlossen. Insgesamt hat also die Annahme, dass A_{n+1} einen nichttrivialen Normalteiler N besitzt, zu einem Widerspruch geführt. □

Folgerung 7.26 Für $n \geq 5$ ist A_n der einzige nichttriviale Normalteiler von S_n.

Beweis: Dass A_n als Kern der Signums-Abbildung ein Normalteiler von S_n ist, wissen wir bereits, und wegen $|A_n| = \frac{1}{2}n!$ muss dies für $n \geq 5$ (sogar für $n \geq 3$) ein nichttrivialer Normalteiler sein. Sei nun umgekehrt N ein nichtrivialer Normalteiler von S_n. Gilt $N \subseteq A_n$, dann gilt auch $N \trianglelefteq A_n$. Weil A_n einfach ist, bleibt in diesem Fall $N = A_n$ als einzige Möglichkeit.

Betrachten wir nun den Fall, dass $N \not\subseteq A_n$ gilt, und definieren wir $N_1 = N \cap A_n$. Durch Einschränkung der Signumsfunktion auf N erhalten wir einen Gruppenhomomorphismus $\phi : N \to \{\pm 1\}$, dessen Kern genau N_1 ist. Wegen $N \not\subseteq A_n$ gibt es in N Elemente σ mit $\phi(\sigma) = -1$, der Homomorphismus ist also surjektiv. Wir können den Homomorphiesatz anwenden und erhalten einen Isomorphismus $N/N_1 \cong \{\pm 1\}$. Es folgt $\frac{|N|}{|N_1|} = |N/N_1| = |\{\pm 1\}| = 2$ und $|N| = 2|N_1|$.

Nun ist N_1 als Durchschnitt zweier Normalteiler von S_n ebenfalls ein Normalteiler von S_n, und wegen $N_1 \subseteq A_n$ somit auch ein Normalteiler von A_n. Außerdem gilt $N_1 \subsetneq A_n$. Denn andernfalls wäre $N \cap A_n = N_1 = A_n$, also $N \supseteq A_n$. Wegen $N \not\subseteq A_n$ würde daraus $N \supsetneq A_n$ folgen, und dies wiederum würde dann $(S_n : N) < (S_n : A_n) = 2$ bedeuten, also $(S_n : N) = 1$ und $N = S_n$. Dies aber steht im Widerspruch zur Annahme, dass N ein *nichttrivialer* Normalteiler von S_n

ist. Aus $N_1 \trianglelefteq A_n$ und $N_1 \subsetneq A_n$ sowie der Einfachheit von A_n folgt $N_1 = \{\mathrm{id}\}$. Dies wiederum bedeutet $|N| = 2|N_1| = 2 \cdot 1 = 2$. Sei σ das einzige nichttriviale Element in N. Wegen $\mathrm{ord}(\sigma) = |N| = 2$ handelt es sich um ein Produkt r disjunkter Transpositionen, wobei $r \geq 1$ ist.

Weil N ein Normalteiler von S_n ist, liegt jedes zu σ in S_n konjugierte Element, also jedes Element vom selben Zerlegungstyp, ebenfalls in N. Dies führt zu einem Widerspruch, sobald wir gezeigt haben, dass es in S_n mehr als zwei Elemente vom selben Zerlegungstyp wie σ gibt. Für Transpositionen ist dies unmittelbar klar, wie man z.B. anhand der Elemente (1 2) und (1 3) sieht. Für $r \geq 2$ seien $\tau, \tau' \in S_n$ Produkte von r disjunkten Transpositionen, wobei in der Zykelzerlegung von τ die Transpositionen (1 2) und (3 4), in der von τ' die Transpositionen (1 3) und (2 4) vorkommen. Offenbar sind τ und τ' verschieden, denn es gilt $\tau(1) = 2$ und $\tau'(1) = 3$. Ingesamt ist damit bewiesen, dass in S_n kein nichttrivialer Normalteiler N mit $N \subsetneq A_n$ existiert. □

Aus der Klassengleichung ergibt sich auch eine interessante Anwendung für die Gruppe A_4.

Satz 7.27 Die Gruppe A_4 hat keine Untergruppe der Ordnung 6.

Beweis: Auch diese Aussage lässt sich mit Hilfe der Klassengleichung beweisen. Für A_4 lautet sie $12 = 1+4+4+3$, wie wir oben nachgerechnet haben. Nehmen wir nun an, N ist eine Untergruppe der Ordnung 6 von A_4. Wegen $(A_4 : N) = \frac{|A_4|}{|N|} = \frac{12}{6} = 2$ ist N auch ein Normalteiler. Wie im Beweis von Satz 7.25 begründet man, dass N eine disjunkte Vereinigung von A_4-Konjugiertenklassen sein muss, wobei eine dieser Klassen gleich $\{\mathrm{id}\}$ ist. Betrachtet man die Mächtigkeit dieser Klassen, so folgt daraus, dass $|N| = 6$ als Summe der Zahlen 1, 3 und 4 darstellbar sein muss, wobei die Zahl 1 genau einmal, die Zahl 3 höchstens einmal und die Zahl 4 höchstens zweimal in der Darstellung vorkommen muss (letzteres, weil es zwei A_4-Konjugiertenklassen mit vier Elementen gibt). Wie man sich leicht überzeugt, existiert eine solche Darstellung nicht, denn es ist $1+3 = 4$, $1+4 = 5$, und alle andere anderen Summen dieser Form sind ≥ 8. Also existiert in A_4 keine Untergruppe der Ordnung 6. □

Wir geben noch einen weiteren Beweis an, der mit der Hilfe der Sylowsätze funktioniert, die wir im folgenden Kapitel behandeln. Nehmen wir an, dass V eine Untergruppe von $G = A_4$ der Ordnung 6 ist. Auf Grund des 0-ten Sylowsatzes enthält V eine Untergruppe U der Ordnung 3. Wegen $(V : U) = 2$ ist U ein Normalteiler von V. Es folgt daraus $V \subseteq N_G(U)$, und daraus wiederum ergibt sich

$$(G : N_G(U)) \quad \leq \quad (G : V) \quad = \quad \frac{|G|}{|V|} \quad = \quad \frac{12}{6} \quad = \quad 2.$$

Nun sind die Sylowgruppen von G wegen $|G| = 2^2 \cdot 3$ genau die Untergruppen der Ordnung 3. Da G nach dem Zweiten Sylowsatz auf der Menge $\mathcal{U}$ dieser Untergruppen transitiv operiert und $N_G(U)$ der Stabilisator von $U \in \mathcal{U}$ ist, gilt $|\mathcal{U}| = |G(U)| = (G : N_G(U))$; dies ist ein Spezialfall der Formel $(G : G_x) = |G(x)|$ aus Satz 7.6. Auf Grund der Ungleichung $(G : N_G(U)) \leq 2$ von oben würde dies bedeuten, dass G nur zwei Untergruppen der Ordnung 3 besitzt. Tatsächlich aber gibt es in G genau acht Elemente der Ordnung drei (die 3-Zykel). Jede Untergruppe der Ordnung 3 enthält genau zwei dieser Elemente. Es gibt also genau vier Untergruppen der Ordnung 3 in G. Der Widerspruch zu $|\mathcal{U}| = 2$ zeigt, dass die Annahme bezüglich der Existenz von V falsch war.

§ 8. *Die Sylowsätze*

Zusammenfassung. In diesem Abschnitt leiten wir als besondere Anwendung aus der Theorie der Gruppenoperationen die bekannten Sylowsätze her. Diese ermöglichen weitreichende Aussagen über die sog. *p-Sylowgruppen* einer endlichen Gruppe; dabei handelt es sich um die Untergruppen maximaler p-Potenzordnung. In einigen Fällen lassen sich auf diese Weise sogar alle Gruppen einer festen Ordnung bis auf Isomorphie klassifizieren, was wir am Ende des Kapitels anhand zweier konkreter Beispiele demonstrieren.

Die wesentliche Idee beim Beweis der Sylowsätze besteht darin, die endliche Gruppe auf der Menge ihrer p-Sylowgruppen operieren zu lassen, wobei nicht nur die Operation der gesamten Gruppen, sondern auch die Operation der p-Untergruppen dieser Menge berücksichtigt wird. Die im letzten Abschnitt entwickelten Grundlagen zum Thema Gruppenoperationen, inbesondere die Bahngleichung, spielen beim Beweis die entscheidende Rolle. Die gewünschten Ergebnisse erhalten wir durch die detaillierte Untersuchung der Stabilisatoren dieser Gruppenoperation.

Wichtige Grundbegriffe

- Operation einer Gruppe auf der Menge ihrer Untergruppen (Normalisatoren als Stabilisatoren dieser Operation)
- p-Untergruppen und Sylowgruppen einer endlichen Gruppe

Zentrale Sätze

- Satz über die Existenz von p-Untergruppen („Nullter Sylowsatz“)
- Erster, Zweiter und Dritter Sylowsatz
- Anwendungen der Sylowsätze:
  Klassifikation der Gruppen der Ordnung 15 und der Gruppen der Ordnung $2p$ für eine beliebige Primzahlen p

Wir beginnen diesen Abschnitt mit einer weiteren Anwendung der Bahngleichung.

Satz 8.1 *(„Nullter Sylowsatz“)*
Sei G eine endliche Gruppe, p eine Primzahl und $k \in \mathbb{N}_0$ derart, dass p^k ein Teiler der Gruppenordnung $|G|$ ist. Dann gibt es in G eine Untergruppe der Ordnung p^k.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über $n = |G|$. Für $n = 1$ ist 1 die einzige Primzahlpotenz, die n teilt, und daher braucht nichts gezeigt werden. Sei nun $n > 1$, und setzen wir die Aussage für alle kleineren Gruppenordnungen als gültig voraus. Sei G eine Gruppe der Ordnung n und p^k eine Primzahlpotenz, die n teilt, wobei wir $k > 0$ annehmen können. Wir unterscheiden nun zwei Fälle.

1. Fall: Es gibt eine Untergruppe $H \subsetneq G$ mit $p \nmid (G : H)$.
Dann ist p^k wegen $|G| = (G : H)|H|$ auch ein Teiler von $|H|$. Nach Induktionsvoraussetzung gibt es in H eine Untergruppe U der Ordnung p^k, und natürlich ist U auch eine Untergruppe von G.

2. Fall: Für jede Untergruppe $H \subsetneq G$ ist p ein Teiler von $(G : H)$.
In diesem Fall stellen wir die Klassengleichung für G auf. Bezeichnet R ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element, dann gilt

$$|G| \quad = \quad |Z(G)| + \sum_{g \in R} (G : C_G(g)) \quad ,$$

Auf Grund unserer Voraussetzung sind die Zahlen $(G : C_G(g))$ ebenso wie $|G|$ alle durch p teilbar, somit ist auch $|Z(G)|$ ein Vielfaches von p. Daraus folgt, dass $Z(G)$ ein Element der Ordnung p enthält. Denn nach Satz 5.10 ist isomorph zu einem äußeren direkten Produkt zyklischer Gruppen $C_1, ..., C_r$; darunter muss zumindest eine mit $p \mid |C_i|$ sein. Ist $h \in C_i$ ein Erzeuger, dann ist $g = h^{|C_i|/p}$ nach Satz 3.9 ein Element der Ordnung p. Damit ist $N = \langle g \rangle$ eine Untergruppe der Ordnung p.

Wegen $N \subseteq Z(G)$ ist N ein Normalteiler von G. Sind nämlich $n \in N$ und $g \in G$ beliebig vorgegeben, dann gilt $gng^{-1} = gg^{-1}n = n \in N$. Wir bilden nun die Faktorgruppe $\bar{G} = G/N$. Wegen $|\bar{G}| < |G|$ können wir die Induktionsvoraussetzung anwenden und erhalten eine Untergruppe $\bar{U}$ von $\bar{G}$ der Ordnung p^{k-1}. Sei $U = \pi^{-1}(\bar{U})$ das Urbild von $\bar{U}$ unter dem kanonischen Epimorphismus $\pi : G \to G/N$. Wegen $\bar{U} = U/N$ und nach dem Satz von Lagrange gilt $|U| = |\bar{U}| \cdot |N| = p^{k-1}p = p^k$. □

In endlichen abelschen Gruppen kann man sogar für *jeden* Teiler d der Gruppenordnung eine Untergruppe der Ordnung d finden. Dies kann aus Satz 5.10 abgeleitet werden, wenn man noch berücksichtigt, dass nach Satz 3.11 eine endliche zyklische Gruppe zu jedem Teiler ihrer Gruppenordnung eine (eindeutig bestimmte) Untergruppe dieser Ordnung besitzt. Für nicht-abelsche Gruppen ist die Aussage für beliebige Teiler aber falsch. Beispielsweise haben wir in den Übungen gezeigt, dass die alternierende Gruppe A_4 keine Untergruppe der Ordnung 6 besitzt, obwohl 6 ein Teiler von $|A_4| = 12$ ist.

Folgerung 8.2 *(Satz von Cauchy)*
Ist G eine endliche Gruppe und p ein Primteiler von $|G|$, dann existiert in G ein Element der Ordnung p.

Beweis: Nach Satz 8.1 gibt es in G eine Untergruppe U der Ordnung p. Als Gruppe von Primzahlordnung ist U nach Folgerung 2.22 (ii) zyklisch, es gibt also ein $g \in U$ mit $U = \langle g \rangle$. Nach Definition der Elementordnung gilt $\text{ord}(g) = |\langle g \rangle| = |U| = p$. □

Nun kommen wir zur letzten wichtigen Anwendung der Bahngleichung in diesem Kapitel, den Sylowsätzen.

Definition 8.3 Sei p eine Primzahl und G eine endliche Gruppe der Ordnung $n = p^r m$, wobei m und p teilerfremd sind. Eine ***p*-Untergruppe** von G ist eine Untergruppe der Ordnung p^s mit $0 \leq s \leq r$. Ist $r = s$, dann sprechen wir von einer ***p*-Sylowgruppe**.

Um die Sylowsätze zu beweisen, betrachten wir die bereits in Definition 7.7 eingeführte Operation einer Gruppe G auf der Menge ihrer Untergruppen. Den Stabilisator eines Elements dieser Menge unter der Operation hatten wir dort als *Normalisator* der Untergruppe bezeichnet. Diese Bezeichnung ist durch folgende Eigenschaft gerechtfertigt.

Proposition 8.4 Sei G eine Gruppe und U eine Untergruppe. Dann ist $N_G(U)$ die größte Untergruppe H von G mit der Eigenschaft, dass U Normalteiler von H ist.

Beweis: Als Stabilisator bezüglich einer Gruppenoperation ist $N_G(U)$ jedenfalls eine Untergruppe von G. Aus Proposition 6.1 folgt insbesondere, dass für jede Gruppe durch die Konjugation mit einem Gruppenelement jeweils ein Automorphismus der Gruppe definiert ist. (Man bezeichnet diese Automorphismen als ***innere Automorphismen*** der Gruppe.) Daraus folgt, dass $uUu^{-1} = U$ für alle $u \in U$ gilt, und U somit in $N_G(U)$ enthalten ist. Also ist U auch eine Untergruppe von $N_G(U)$. Für jedes $g \in N_G(U)$ gilt $gUg^{-1} = U$ nach Definition von $N_G(U)$. Dies zeigt, dass U sogar ein Normalteiler von $N_G(U)$ ist. Sei nun H eine beliebige Untergruppe von G mit der Eigenschaft $U \trianglelefteq H$. Für jedes $h \in H$ gilt dann $hUh^{-1} = U$ und somit $h \in N_G(U)$. Also ist H tatsächlich in $N_G(U)$ enthalten. □

Lemma 8.5 Sei G eine Gruppe mit Untergruppen S, H, und es gelte $hSh^{-1} = S$ für alle $h \in H$. Dann ist das Komplexprodukt HS eine Untergruppe von G, und es gilt $S \trianglelefteq HS$.

Beweis: Wir zeigen zunächst, dass aus der Voraussetzung $hSh^{-1} = S$ für alle $h \in H$ die Gleichung $HS = SH$ folgt. Sei $a \in HS$ vorgegeben. Dann gibt es Elemente $h \in H$ und $s \in S$ mit $hs = a$. Auf Grund der Voraussetzung liegt hsh^{-1} in S und somit $hs = (hsh^{-1})h$ in SH. Dies beweist die Inklusion $HS \subseteq SH$. Sei nun umgekehrt $b \in SH$ vorgegeben, $b = sh$ mit $s \in S$ und $h \in H$. Dann liegt $h^{-1}sh$ in $h^{-1}Sh = S$, und es folgt $sh = h(h^{-1}sh) \in HS$.

Wir können nun Lemma 4.20 über Komplexprodukte anwenden. Demzufolge ist HS eine Untergruppe von G. Zum Beweis von $S \trianglelefteq HS$ bestimmen wir den Normalisator von S in HS. Wegen $hSh^{-1} = S$ für alle $h \in H$ gilt $H \subseteq N_{HS}(S)$, und wegen $sSs^{-1} \subseteq S$ für alle $s \in S$ ist auch S in $N_{HS}(S)$ enthalten. Jede Untergruppe von HS, die S und H enthält, stimmt offenbar mit HS überein. Es gilt also $N_{HS}(S) = HS$, und aus der Eigenschaft $S \trianglelefteq N_{HS}(S)$ des Normalisators, siehe Proposition 8.4, folgt $S \trianglelefteq HS$. □

Wir können nun unser Hauptresultat formulieren und beweisen.

Satz 8.6 Sei G eine Gruppe der Ordnung n, p eine Primzahl und $n = mp^r$ mit $p \nmid m$.

(i) *Erster Sylowsatz:* Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.

(ii) *Zweiter Sylowsatz:* Je zwei p-Sylowgruppen sind zueinander konjugiert.

(iii) *Dritter Sylowsatz:* Für die Anzahl ν_p der p-Sylowgruppen gilt $\nu_p \equiv 1 \bmod p$ und $\nu_p \mid m$.

Beweis: Zunächst definieren wir uns eine geeignete Gruppenoperation und betrachten dazu die Operation durch Konjugation von G auf der Menge $\mathcal{V}$ der Untergruppen von G. Nach Satz 8.1 gibt es mindestens eine p-Sylowgruppe $P \in \mathcal{V}$. Die Bahn $\mathcal{U} = G(P)$ eine G-invariante Teilmenge. Für jedes $Q \in G(P)$ gilt $Q = g \cdot P = gPg^{-1}$ für ein $g \in G$. Weil nach Proposition 6.1 die Konjugation mit g ein Automorphismus von G ist, sind die Gruppen P und Q isomorph, und somit besteht $\mathcal{U}$ ausschließlich aus p-Sylowgruppen.

Wir zeigen nun, dass p teilerfremd zu $|\mathcal{U}|$ ist. Auf Grund des allgemeinen Zusammenhangs aus Satz 7.6 zwischen Bahnlänge und Index des Stabilisators gilt zunächst $|\mathcal{U}| = |G(P)| = (G : N_G(P))$. Wegen $P \subseteq N_G(P)$ und auf Grund der Gleichung aus dem Satz 2.20 von Lagrange gegeben durch $|N_G(P)| = |P| \cdot (N_G(P) : P)$ erhalten wir

$$(G : P) \quad = \quad \frac{|G|}{|P|} \quad = \quad \frac{|G|}{|N_G(P)|} \cdot \frac{|N_G(P)|}{|P|} \quad = \quad (G : N_G(P))(N_G(P) : P).$$

Somit ist $|\mathcal{U}| = (G : N_G(P))$ ein Teiler von $m = (G : P)$. Da m teilerfremd zu p ist, gilt dies auch für $|\mathcal{U}|$.

zu (i) Sei H eine beliebige p-Untergruppe. Wir betrachten die Operation von H auf $\mathcal{U}$ durch Konjugation und zeigen, dass mindestens ein Fixpunkt existiert. Darüber hinaus zeigen wir, dass jede Untergruppe S, die als Fixpunkt der Operation auftritt, die Untergruppe H enthält.

Die Menge $\mathcal{U}$ zerfällt unter der Operation von H disjunkt in eine gewisse Anzahl von Bahnen. Ist $\mathcal{B}$ eine solche Bahn, dann ist $|\mathcal{B}|$ ein Teiler von $|H|$ und somit eine p-Potenz. Sei F die Menge der Fixpunkte und $\mathcal{R}$ ein Repräsentantensystem der Bahnen mit Länge > 1. Weil $|\mathcal{U}|$ teilerfremd zu p ist, muss es auf Grund der Bahngleichung

$$|\mathcal{U}| \quad = \quad |F| + \sum_{U \in \mathcal{R}} (H : H_U)$$

aus Satz 7.11 mindestens einen Fixpunkt $S \in \mathcal{B}$ unter dieser der Operation geben.

Wir beweisen nun die Inklusion $H \subseteq S$. Die Fixpunkt-Eigenschaft bedeutet gerade $hSh^{-1} = S$ für alle $h \in H$. Nach Lemma 8.5 ist das Komplexprodukt HS jedenfalls eine Untergruppe von G und S ein Normalteiler von HS. Nach dem Isomorphiesatz, Satz 4.32, gilt $H/(H \cap S) \cong HS/S$ und somit

$$\frac{|H|}{|H \cap S|} = \frac{|HS|}{|S|} \quad \Leftrightarrow \quad |HS| = \frac{|H||S|}{|H \cap S|}.$$

Mit $|S|$ und $|H|$ ist also auch $|HS|$ eine p-Potenz. Aus $HS \supseteq S$ und der p-Sylowgruppen-Eigenschaft von S folgt, dass $HS = S$ und somit $H \subseteq S$ gilt.

zu (ii) Sei P' eine beliebige p-Sylowgruppe in G. Wie wir in (i) gezeigt haben, gibt es ein Element $P'' \in \mathcal{U}$ mit $P' \subseteq P''$. Weil P' und P'' dieselbe Ordung haben, gilt $P' = P''$. Weil P'' in derselben Bahn wie P liegt, gibt es ein $g \in G$ mit $P' = P'' = gPg^{-1}$.

zu (iii) Aus (ii) folgt, dass $\mathcal{U} = G(P)$ bereits die Menge *aller* p-Sylowgruppen von G ist und somit $\nu_p = |\mathcal{U}| = (G : N_G(P))$ gilt. Bereits am Anfang des Beweises wurde gezeigt, dass dies ein Teiler von $m = (G : P)$ ist. Zum Beweis der Kongruenz betrachten wir die Operation von P auf $\mathcal{U}$. Nach Teil (i) ist P in jeder p-Sylowgruppe enthalten, die unter dieser Operation fest bleibt. Da P auf Grund seiner Ordnung in keiner anderen p-Sylowgruppe als P selbst liegen kann, ist P der einzige Fixpunkt dieser Operation, und der Rest von $\mathcal{U}$ zerfällt in Bahnen von p-Potenzlänge > 1. Bezeichnen wir mit R ein Repräsentantensystem dieser Bahnen, dann gilt auf Grund der Bahngleichung

$$\nu_p \quad = \quad |\mathcal{U}| \quad = \quad |\{P\}| + \sum_{U \in R} (P : P_U).$$

Wegen $|\{P\}| = 1$, und weil es sich bei den Bahnlängen $(P : P_U) = |P(U)|$ um p-Potenzen > 1 handelt, ist die rechte Seite der Gleichung kongruent zu 1 modulo p. □

Folgerung 8.7 Sei G eine Gruppe und p eine Primzahl. Eine p-Sylowgruppe P ist genau dann ein Normalteiler von G, wenn die Anzahl ν_p der p-Sylowgruppen von G gleich 1 ist.

Beweis: „⇒“ Ist P' eine weitere p-Sylowgruppe, dann ist P' nach Teil (ii) der Sylowsätze zu P konjugiert. Es gibt also ein $g \in G$ mit $P' = gPg^{-1}$. Weil P ein Normalteiler von G ist, folgt $P' = gPg^{-1} = P$ und somit $\nu_p = 1$. „⇐“ Sei

$g \in G$. Nach Proposition 6.1 ist die Untergruppe gPg^{-1} isomorph zu P. Insbesondere hat gPg^{-1} dieselbe Ordnung wie P und ist somit eine p-Sylowgruppe. Wegen $\nu_p = 1$ muss $gPg^{-1} = P$ gelten. Weil g beliebig gewählt war, folgt daraus die Normalteiler-Eigenschaft von P. □

Als erstes Anwendungsbeispiel für die Sylowsätze beweisen wir

Lemma 8.8 Jede Gruppe der Ordnung 15 besitzt einen Normalteiler der Ordnung 3 und einen Normalteiler der Ordnung 5.

Beweis: Sei G eine Gruppe mit $|G| = 15$, und für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Wegen Teil (iii) der Sylowsätze ist ν_3 ein Teiler von 5, also $\nu_3 \in \{1, 5\}$, und es gilt $\nu_3 \equiv 1 \bmod 3$. Da $5 \not\equiv 1 \bmod 3$ ist, bleibt als einzige Möglichkeit $\nu_3 = 1$. Die einzige 3-Sylowgruppe ist nach Folgerung 8.7 ein Normalteiler von G. Wenden wir Teil (iii) der Sylowsätze auf die Anzahl der 5-Sylowgruppen an, dann erhalten wir $\nu_5 | 3$, also $\nu_5 \in \{1, 3\}$, und $\mu_5 \equiv 1 \bmod 5$. Wegen $3 \not\equiv 1 \bmod 5$ muss $\nu_5 = 1$ sein, und die einzige 5-Sylowgruppe ist wiederum ein Normalteiler von G. □

Folgerung 8.9 Jede Gruppe der Ordnung 15 ist zyklisch.

Beweis: Sei G eine Gruppe mit $|G| = 15$. Nach Lemma 8.8 besitzt G Normalteiler N und U der Ordnungen 3 bzw. 5. Weil $|N|$ und $|U|$ teilerfremd sind, gilt $N \cap U = \{e\}$. Die Untergruppe NU enthält U und N, also ist $|NU|$ ein Vielfaches von 3 und zugleich ein Vielfaches von 5. Also ist $|NU|$ insgesamt ein Vielfaches von 15. Wegen $NU \subseteq G$ und $|G| = 15$ folgt $G = NU$. Insgesamt haben wir damit gezeigt, dass G ein direktes Produkt von N und U ist. Nach Proposition 4.24 folgt daraus $G \cong N \times U$. Als Gruppen von Primzahlordnung sind N und U nach Folgerung 2.22 zyklisch, es gilt also $N \cong \mathbb{Z}/3\mathbb{Z}$ und $U \cong \mathbb{Z}/5\mathbb{Z}$. Mit dem Chinesischen Restsatz, Satz 5.8, erhalten wir

$$G \quad \cong \quad N \times U \quad \cong \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \quad \cong \quad \mathbb{Z}/15\mathbb{Z}.$$

Insbesondere ist G zyklisch. □

Proposition 8.10 Sei $n \in \mathbb{N}$ mit $n \geq 3$, G eine Gruppe und $\{g, h\}$ ein Erzeugendensystem von G, wobei $\mathrm{ord}(g) = n$, $\mathrm{ord}(h) = 2$ und $ghgh = e_G$ gilt. Dann ist G isomorph zur Diedergruppe D_n.

Beweis: Aus früheren Kapitel ist bekannt, dass die Diedergruppe D_n ein zweielementiges Erzeugendensystem $\{\rho_n, \tau\}$ besitzt mit den Eigenschaften $\mathrm{ord}(\rho_n) = n$, $\mathrm{ord}(\tau) = 2$ und $\rho_n \tau \rho_n \tau = \mathrm{id}_{\mathbb{R}^2}$. Aus den Gleichungen hatten wir gefolgert, dass D_n eine Gruppe der Ordnung D_n ist, dessen Elemente durch

$$D_n \quad = \quad NU \quad = \quad \{\rho_n^a \tau^b \mid 0 \leq a < n, b \in \{0, 1\}\}$$

gegeben sind. Genauso kann man aus den hier angegebenen Voraussetzungen ableiten, dass $|G| = 2n$ gilt, und dass die Elemente von G durch

$$G \quad = \quad \langle g \rangle \langle h \rangle \quad = \quad \{g^a h^b \mid 0 \leq a < n, b \in \{0, 1\}\}$$

gegeben sind. Offenbar ist die Abbildung $\psi : D_n \to G$ definiert durch $\psi(\rho_n^a \tau^b) = g^a h^b$ eine Bijektion. Die Gleichung ist nicht nur für $0 \leq a < n$ und $b \in \{0, 1\}$, sondern für beliebige $a, b \in \mathbb{Z}$ gültig. Sind nämlich a, b beliebige ganze

Zahlen und a_1, b_1 die Reste nach Division durch n bzw. 2, dann erhält man wegen $\mathrm{ord}(\rho_n) = \mathrm{ord}(g) = n$ und $\mathrm{ord}(\tau) = \mathrm{ord}(h) = 2$ die Gleichung

$$\psi(\rho_n^a \tau^b) \quad = \quad \psi(\rho_n^{a_1} \tau^{b_1}) \quad = \quad g^{a_1} h^{b_1} \quad = \quad g^a h^b.$$

Darüber hinaus handelt es sich bei der Abbildung ψ einen Isomorphismus. Seien nämlich $a, c \in \{0, ..., n-1\}$ und $b, d \in \{0, 1\}$. Im Fall $b = 0$ gilt

$$\begin{aligned} \psi(\rho_n^a \tau^b \circ \rho_n^c \tau^d) \quad &= \quad \psi(\rho_n^a \circ \rho_n^c \tau^d) \quad = \quad \psi(\rho_n^{a+c} \tau^d) \quad = \quad g^{a+c} h^d \quad = \quad g^a \cdot g^c h^d \\ &= \quad g^a h^b \cdot g^c h^d \quad = \quad \psi(\rho_n^a \tau^b) \cdot \psi(\rho_n^c \tau^d). \end{aligned}$$

Im Fall $b = 1$ verwenden wir die Tatsache, dass aus der Gleichung $\tau \rho_n = \rho_n^{-1} \tau$ durch vollständige Induktion die Gleichung $\tau \rho_n^c = \rho_n^{-c} \tau$ folgt, und dass man ebenso aus $hg = g^{-1} h$ die Gleichung $hg^c = g^{-c} h$ erhält. Daraus ergibt sich auch in diesem Fall

$$\begin{aligned} \psi(\rho_n^a \tau^b \circ \rho_n^c \tau^d) \quad &= \quad \psi(\rho_n^a \circ \tau \circ \rho_n^c \circ \tau^d) \quad = \quad \psi(\rho_n^a \circ \rho_n^{-c} \circ \tau \circ \tau^d) \quad = \quad \psi(\rho_n^{a-c} \circ \tau^{d+1}) \\ = \quad g^{a-c} \cdot h^{d+1} \quad &= \quad g^a \cdot g^{-c} \cdot h \cdot h^d \quad = \quad g^a \cdot h \cdot g^c \cdot h^d \quad = \quad g^a h^b \cdot g^c h^d \quad = \quad \psi(\rho_n^a \tau^b) \cdot \psi(\rho_n^c \tau^d). \end{aligned}$$

Damit ist die Homomorphismus-Eigenschaft der Abbildung ψ nachgewiesen. □

Satz 8.11 Sei p eine ungerade Primzahl und G eine nicht-abelsche Gruppe der Ordnung $2p$. Dann ist G isomorph zur Diedergruppe D_p.

Beweis: In Proposition 8.10 wurde eine Charakterisierung der Diedergruppen bis auf Isomorphie gegeben. Demnach gilt $G \cong D_p$, wenn Elemente $g, h \in G$ existieren, so dass die Bedingungen $G = \langle g, h \rangle$, $\mathrm{ord}(g) = p$, $\mathrm{ord}(h) = 2$ und $ghgh = e_G$ erfüllt sind. Wir werden dies nun mit Hilfe der Sylowsätze beweisen. Sei ν_p die Anzahl der p-Sylowgruppen von G. Nach Teil (iii) der Sylowsätze ist ν_p ein Teiler von 2, es ist also nur $\nu_p \in \{1, 2\}$ möglich. Darüber hinaus gilt $\nu_p \equiv 1 \bmod p$. Daraus folgt $\nu_p = 1$. Sei N die einzige p-Sylowgruppe von G, und sei $g \in N$ ein erzeugendes Element dieser Untergruppe. Außerdem sei H eine beliebige 2-Sylowgruppe von G und $h \in H$ ein erzeugendes Element von H. Dann gilt $\mathrm{ord}(g) = p$ und $\mathrm{ord}(h) = 2$. Darüber hinaus ist auch $G = \langle g, h \rangle$ erfüllt. Denn $U = \langle g, h \rangle$ ist eine Untergruppe von G, deren Ordnung von $\mathrm{ord}(g) = p$ und $\mathrm{ord}(h) = 2$ geteilt wird. Wegen $\mathrm{ggT}(2, p) = 1$ ist insgesamt $2p$ ein Teiler von $|U|$, was wegen $|G| = 2p$ nur den Schluss $U = G$ zulässt.

Wegen $N \trianglelefteq G$ gilt $hNh = N$. Das Element hgh liegt also in N, und folglich existiert ein $b \in \mathbb{Z}$ mit $hgh = g^b$. Aus $g^{b^2} = (g^b)^b = (hgh)^b = hg^b h = h^2 g h^2 = e_G g e_G = g$ und $\mathrm{ord}(g) = p$ folgt $b^2 \equiv 1 \bmod p$. Wie wir in der Zahlentheorie-Vorlesung zeigen werden, hat die Gleichung $x^2 = \bar{1}$ im Ring $\mathbb{Z}/p\mathbb{Z}$ nur zwei Lösungen, nämlich $\pm\bar{1}$. Daraus folgt $b \equiv \pm 1 \bmod p$.

Betrachten wir zunächst den Fall $b \equiv 1 \bmod p$. Wir zeigen, dass in diesem Fall nicht nur N, sondern auch H ein Normalteiler von G ist. Es gilt $hgh = g$, was zu $hg = gh^{-1} = gh$ und $ghg^{-1} = h$ umgeformt werden kann. Der Normalisator $N_G(H)$ von $H = \langle h \rangle$ in G enthält damit außer h also auch das Element g. Daraus ergibt sich $G = \langle g, h \rangle \subseteq N_G(H)$. Folglich ist in dieser Situation neben N auch die Untergruppe H nach Proposition 8.4 ein Normalteiler von G. Auf Grund der Teilerfremdheit von $|H| = 2$ und $|N| = p$ gilt $H \cap N = \{e_G\}$. Auf Grund der Normalteiler-Eigenschaft

von H (oder N) ist NH eine Untergruppe von G. Diese enthält g und h, also auch $G = \langle g, h \rangle$, woraus $G = NH$ folgt. Insgesamt ist damit nachgewiesen, dass G ein inneres direktes Produkt von N und H ist. Nach Proposition 4.24 gilt also $G \cong N \times H$. Als äußeres direktes Produkt zweier abelscher Gruppen ist $N \times H$ abelsch. Weil aber G nicht-abelsch ist, haben wir damit gezeigt, dass der Fall $b \equiv 1 \bmod p$ ausgeschlossen ist.

Somit bleibt $b \equiv -1 \bmod p$ als einzige Möglichkeit. Es folgt $hgh = g^b = g^{-1}$, was zu $ghgh = e_G$ umgeformt werden kann. Damit sind die charakteristischen Eigenschaften der Diedergruppe nachgewiesen, und wir erhalten $G \cong D_p$ wie gewünscht. □

§ 9. Grundlagen der Ringtheorie

Zusammenfassung. Wie bereits aus der Linearen Algebra bekannt, ist ein *Ring* eine algebraische Struktur, in der die arithmetischen Operationen Addition, Subtraktion und Multiplikation zur Verfügung stehen, im Allgemeinen aber keine Division. Die Definition basiert auf den Begriffen der *Gruppe* und des *Monoids*, die wir im ersten Kapitel studiert haben. Das Standardbeispiel ist der Ring $\mathbb{Z}$ der ganzen Zahlen.

Wichtige spezielle Elementen in Ringen sind *Einheiten* und *Nullteiler*. Ein Ring R mit $R^\times = R \setminus \{0_R\}$ bezeichnet man als *Körper*. Darunter fallen die bekannten Zahlbereiche $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$, aber wir wissen bereits aus der Linearen Algebra, dass es außerdem für jede Primzahl p einen Körper $\mathbb{F}_p$ mit p Elementen gibt. In vielen Ringen (beispielsweise in $\mathbb{Z}$ und den Körpern) ist das Nullelement der einzige Nullteiler; solche Ringe bezeichnet man als *Integritätsbereiche*. Die *Charakteristik* eines Rings R ist die Ordnung des Elements 1_R in der Gruppe $(R, +)$, sofern diese endlich ist; ansonsten ordnet man ihr den Wert null zu.

Das Analogon der Untergruppe in der Ringtheorie ist der Begriff des *Teilrings*. Im Gegensatz zur Gruppentheorie steht aber hier der Aspekt der *Erweiterung* im Vordergrund. Beispielsweise leisten die Ringe der Form $\mathbb{Z}[\sqrt{d}]$, die dadurch entstehen, dass man den Ring $\mathbb{Z}$ um eine reelle oder imaginäre Quadratwurzel erweitert, wichtige Beiträge zur Lösung von Problemen der Elementaren Zahlentheorie.

Wichtige Grundbegriffe

- Ringe und Ringhomomorphismen
- Einheiten und Nullteiler
- Nullringe, Integritätsbereiche, Körper
- Charakteristik eines Rings
- Teilring eines Rings R, Erweiterungsring

Zentrale Sätze

- Existenz und Eindeutigkeit von Ringhomomorphismen $\mathbb{Z} \to R$ (wobei R beliebiger Ring)
- Existenz und Eindeutigkeit des erzeugten Erweiterungsrings $R[A]$
- Primzahlcharakteristik von Integritätsbereichen
- Injektivität von Körperhomomorphismen
- Gestalt der quadratischen Zahlringe

Definition 9.1 Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, genannt ***Addition*** und ***Multiplikation***, so dass die folgenden Bedingungen erfüllt sind:

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein kommutatives Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Das Neutralelement der Gruppe $(R, +)$ bezeichnet man mit 0_R und nennt es das ***Nullelement*** des Rings. Ist $a \in R$, dann schreibt man $-a$ für das Inverse von a in der Gruppe $(R, +)$ und nennt es das ***Negative*** von a. Das Neutralelement

von $(R,\cdot)$ wird ***Einselement*** von R genannt und mit 1_R bezeichnet. An Stelle von $a+(-b)$ schreiben wir auch kürzer $a-b$. Die Rechenregeln für Inverse aus der Algebra-Vorlesung sind natürlich auch in der Gruppe $(R,+)$ gültig, es gilt also $-(a+b)=(-a)+(-b)$ und $-(-a)=a$ für alle $a,b\in R$. Darüber hinaus gilt auch

$$0_R\cdot a=0_R \quad , \quad (-a)b=a(-b)=-(ab) \quad \text{und} \quad (-a)(-b)=ab \quad \text{für alle} \quad a,b\in R.$$

Ähnliche Rechenregeln wurden in der Linearen Algebra für die Elemente eines Vektorraums bewiesen. Die erste Gleichung erhält man, indem man in der Gleichung $0_R\cdot a=(0_R+0_R)\cdot a=0_R\cdot a+0_R\cdot a$ auf beiden Seiten das Element $-(0_R\cdot a)$ addiert. Die Gleichung $(-a)b+ab=((-a)+a)b=0_R\cdot b=0_R$ zeigt, dass $(-a)b$ das additive Inverse von ab ist, also $(-a)b=-(ab)$ gilt, und genauso zeigt man $a(-b)=-(ab)$. Die letzte Gleichung kann schließlich durch $(-a)(-b)=-(a(-b))=-(-ab)=ab$ auf die bereits bekannten Regeln zurückgeführt werden.

Die Zahlbereiche $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ bilden mit ihrer herkömmlichen Addition und Multiplikation jeweils Ringe. Außerdem kennen wir bereits die Restklassenringe $R[x]$ und die Polynomringe $\mathbb{Z}/n\mathbb{Z}$. Dagegen ist der Zahlbereich $\mathbb{N}_0$ mit der gewöhnlichen Addition und Multiplikation *kein* Ring, weil $(\mathbb{N}_0,+)$ keine Gruppe ist. Beispielsweise besitzt das Element 1 in $(\mathbb{N}_0,+)$ kein Inverses. Ein solches Inverses $a\in\mathbb{N}_0$ von 1 müsste nämlich die Gleichung $a+1=0$ erfüllen, aber durch Addition von -1 auf beiden Seiten erhält man $a=-1$, im Widerspruch zu $a\in\mathbb{N}_0$.

Man beachte, dass Null- und Einselement eines Rings R auch zusammenfallen können, also $0_R=1_R$ gelten kann. Allerdings kann dies nur passieren, wenn der gesamte Ring nur aus einem einzigen Element besteht, also $R=\{0_R\}=\{1_R\}$ gilt. Ist nämlich R ein Ring mit $0_R=1_R$ und $a\in R$ beliebig, dann erhält man $a=a\cdot 1_R=a\cdot 0_R=0_R$. Ringe mit nur einem Element bezeichnet man als ***Nullringe***.

Wie in der Kategorie der Gruppen lassen sich aus gegebenen Ringen neue Ringe konstruieren. Sind $(R,+_R,\cdot_R)$ und $(S,+_S,\cdot_S)$ zwei vorgegebene Ringe, und definiert man auf dem kartesischen Produkt $R\times S$ eine Addition und eine Multiplikation durch

$$(r_1,s_1)+(r_2,s_2)=(r_1+_R r_2,s_1+_S s_2) \qquad \text{und} \qquad (r_1,s_1)\cdot(r_2,s_2)=(r_1\cdot_R r_2,s_1\cdot_S s_2) \quad ,$$

so ist $(R\times S,+,\cdot)$ ein Ring. Denn wie in der Algebra-Vorlesung gezeigt wurde, ist $(R\times S,+)$ als äußeres direktes Produkt der abelschen Gruppen $(R,+)$ und $(S,+)$ selbst eine abelsche Gruppe, und wie dort zeigt man, dass $(R\times S,\cdot)$ ein abelsches Monoid ist. Auch das Distributivgesetz kann auf die Distributivgesetze in $(R,+_R,\cdot_R)$ und $(S,+_S,\cdot_S)$ zurückgeführt werden, denn für beliebig vorgegebene Elemente $(r_1,s_1),(r_2,s_2),(r_3,s_3)\in R\times S$ gilt

$$\begin{aligned}(r_1,s_1)\cdot((r_2,s_2)+(r_3,s_3)) &= (r_1,s_1)\cdot(r_2+_R r_3,s_2+_S s_3) = (r_1\cdot_R(r_2+_R r_3),s_1\cdot_S(s_2+_S s_3))\\ &= (r_1\cdot_R r_2+_R r_1\cdot_R r_3,s_1\cdot_S s_2+_S s_1\cdot_S s_3) = (r_1\cdot_R r_2,s_1\cdot_S s_2)+(r_1\cdot_R r_3,s_1\cdot_S s_3)\\ &= (r_1,s_1)\cdot(r_2,s_2)+(r_1,s_1)\cdot(r_3,s_3).\end{aligned}$$

Man bezeichnet $R\times S$ als ***direktes Produkt*** der Ringe R und S.

Definition 9.2 Seien $(R,+_R,\cdot_R)$ und $(S,+_S,\cdot_S)$ Ringe. Eine Abbildung $\phi:R\to S$ heißt ***Ringhomomorphismus*** von $(R,+_R,\cdot_R)$ nach $(S,+_S,\cdot_S)$, wenn die Gleichung $\phi(1_R)=1_S$ gilt und außerdem

$$\phi(a+_R b) = \phi(a)+_S\phi(b) \qquad \text{und} \qquad \phi(a\cdot_R b) = \phi(a)\cdot_S\phi(b)$$

für alle $a,b\in R$ erfüllt ist.

Sind beispielsweise R und S Ringe, und betrachten wir den oben konstruierten Ring $R \times S$, dann sind die Abbildungen $\pi_1 : R \times S \to R$, $(r,s) \mapsto r$ und $\pi_2 : R \times S \to S$, $(r,s) \mapsto s$ beides Ringhomomorphismen. Dies rechnet man durch Einsetzen unmittelbar nach.

Man beachte, dass die Bedingung $\phi(1_R) = 1_S$ für Ringhomomorphismen im Allgemeinen ***nicht redundant*** ist, sie ergibt sich also nicht automatisch aus den beiden anderen Eigenschaften der Abbildung ϕ. Beispielsweise erfüllt der Homomorphismus

$$\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \quad , \quad a \mapsto (a, 0)$$

die beiden Bedingungen $\phi(a+b) = \phi(a) + \phi(b)$ und $\phi(ab) = \phi(a)\phi(b)$ für alle $a, b \in \mathbb{Z}$. Es gilt aber nicht $\phi(1) = 1_{\mathbb{Z}\times\mathbb{Z}}$, denn das Einselement von $\mathbb{Z} \times \mathbb{Z}$ ist $(1,1)$ und nicht $(1,0)$.

Aus der Definition folgt unmittelbar, dass ein Ringhomomorphismus $\phi : R \to S$ ein ***Gruppenhomomorphismus*** $(R, +_R) \to (S, +_S)$ ist. Also gelten alle Rechenregeln, die wir in der Algebra für diese Homomorphismen bewiesen haben, insbesondere $\phi(0_R) = 0_S$ und $\phi(-a) = -\phi(a)$ für alle $a \in R$.

Die Begriffe Mono-, Epi-, Iso-, Endo- und Automorphismus von Ringen sind wie in der Kategorie der Gruppen definiert. (Ein Monomorphismus von Ringen ist also ein injektiver Ringhomomorphismus usw.) Wie dort zeigt man auch hier, dass die Komposition zweier Ringhomomorphismen ein Ringhomomorphismus und die Umkehrabbildung eines Isomorphismus von Ringen wiederum ein Isomorphismus ist.

In der Gruppentheorie wurde für jedes $n \in \mathbb{N}_0$ die n-te Potenz eines Monoidelements g definiert. Diese wurde in additiver Schreibweise mit $n \cdot g$ und in multiplikativer Schreibweise g^n bezeichnet. Bei invertierbaren Elementen wurde die Definition sogar auf alle $n \in \mathbb{Z}$ ausgedehnt. Wir behalten diese Notation für die Gruppe $(R, +)$ und das Monoid $(R, \cdot)$ bei, falls $(R, +, \cdot)$ einen Ring bezeichnet. Für jedes $n \in \mathbb{N}$ und jedes $a \in R$ gilt also

$$n \cdot a \quad = \quad \underbrace{a + \ldots + a}_{n\text{-mal}} \qquad \text{und} \qquad a^n \quad = \quad \underbrace{a \cdot \ldots \cdot a}_{n\text{-mal}}.$$

Außerdem gilt $0 \cdot a = 0_R$, $a^0 = 1_R$ sowie $(-n) \cdot a = -n \cdot a$ und $a^{-n} = (a^n)^{-1}$ für alle $n \in \mathbb{N}$.

Der folgende Satz zeigt, dass der Ring $\mathbb{Z}$ der ganzen Zahlen in der Ringtheorie eine besondere Rolle spielt.

Satz 9.3 Für jeden Ring R existiert ein eindeutig bestimmter Ringhomomorphismus $\mathbb{Z} \to R$.

Beweis: Zum Nachweis der *Existenz* bemerken wir zunächst, dass nach Proposition 4.12 ein eindeutig bestimmter Homomorphismus ϕ von der zyklischen Gruppe $(\mathbb{Z}, +)$ in die Gruppe $(R, +)$ mit $\phi(1) = 1_R$ existiert. Auf Grund der Homomorphismus-Eigenschaft erfüllt dieser die Gleichung $\phi(n) = \phi(n \cdot 1) = n \cdot \phi(1) = n \cdot 1_R$ für alle $n \in Z$. Um zu sehen, dass ϕ auch ein Ringhomomorphismus ist, muss noch $\phi(mn) = \phi(m)\phi(n)$ für alle $m, n \in \mathbb{Z}$ überprüft werden. Wir beweisen die Gleichung zunächst für $m \in \mathbb{Z}$ und $n \in \mathbb{N}_0$, durch vollständige Induktion über n. Für $n = 0$ ist die Gleichung wegen

$$\phi(m \cdot 0) \quad = \quad \phi(0) \quad = \quad 0_R \quad = \quad 0 \cdot 1_R \quad = \quad (m \cdot 1_R) \cdot (0 \cdot 1_R) \quad = \quad \phi(m)\phi(0)$$

erfüllt. Setzen wir die Gleichnung nun für n voraus, dann erhalten wir

$$\begin{aligned} \phi(m(n+1)) \quad = \quad \phi(mn+m) \quad = \quad \phi(mn) + \phi(m) \quad = \quad \phi(m)\phi(n) + \phi(m) \cdot 1_R \quad = \\ \phi(m)\phi(n) + \phi(m)\phi(1) \quad = \quad \phi(m)(\phi(n) + \phi(1)) \quad = \quad \phi(m)\phi(n+1). \end{aligned}$$

Schließlich gilt noch $\phi(m(-n)) = \phi(-mn) = -\phi(mn) = -\phi(m)\phi(n) = \phi(m)(-\phi(n)) = \phi(m)\phi(-n)$ für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$, so dass die Gleichung $\phi(mn) = \phi(m)\phi(n)$ damit für alle $m, n \in \mathbb{Z}$ bewiesen ist. Die *Eindeutigkeit* von ϕ folgt direkt aus der Eindeutigkeitsaussage in Proposition 4.12 und der Tatsache, dass jeder Ringhomomorphismus $\mathbb{Z} \to R$ die Zahl $1 \in \mathbb{Z}$ auf das Einselement 1_R abbildet. □

Definition 9.4 Sei R ein Ring.

(i) Ein Element $a \in R$ heißt ***Einheit***, wenn ein $b \in R$ mit $ab = 1_R$ existiert. Die Menge der Einheiten von R bezeichnen wir mit $R^\times$.

(ii) Man nennt es ***Nullteiler***, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten sind genau die invertierbaren Elemente im Monoid $(R, \cdot)$. Das multiplikative Inverse eines Elements $a \in R^\times$ wird auch der ***Kehrwert*** von a genannt und mit a^{-1} bezeichnet. Auch hier gelten die bekannten Rechenregeln für Inverse, also $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ und $(a^{-1})^{-1} = a$ für alle $a, b \in R^\times$. Nach Satz 1.15 bilden die invertierbaren Elemente in einem Monoid eine Gruppe. Damit ist auch $R^\times$ eine Gruppe, die sogenannte ***Einheitengruppe***.

Definition 9.5 Ein Ring R mit 0_R als einzigem Nullteiler heißt ***Integritätsbereich***. Gilt $R^\times = R \setminus \{0_R\}$, dann ist R ein ***Körper***.

Die Zahlbereiche $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper, denn jedes Element ungleich Null in diesen Bereichen besitzt ein multiplikatives Inverses. Im Ring $\mathbb{Z}$ sind die Elemente ± 1 die einzigen beiden Einheiten. Es gibt also außer der Null weitere Nicht-Einheiten, und damit ist $\mathbb{Z}$ kein Körper. Man überprüft aber leicht, dass $\mathbb{Z}$ ein Integritätsbereich ist. Denn das Element 0 ist ein Nullteiler, denn es gilt $1 \neq 0$ und $0 \cdot 1 = 0$. Andererseits ist 0 der einzige Nullteiler. Sind nämlich $a, b \neq 0$, dann ist auch das Produkt ab ungleich Null. Wäre $ab = 0$, dann würden wir durch $b = a^{-1}ab = a^{-1}0 = 0$ einen Widerspruch zur Voraussetzung erhalten. Mit demselben Argument kann gezeigt werden, dass jeder Teilring (s.u.) eines Körpers ein Integritätsbereich ist.

Im Ring $\mathbb{Z} \times \mathbb{Z}$ gibt es vier Einheiten, die Elemente $(\pm 1, \pm 1)$. Es ist aber kein Integritätsbereich, denn das Element $(1, 0)$ ist wegen $(1, 0)(0, 1) = (0, 0)$ und $(0, 1) \neq (0, 0)$ ein Nullteiler des Rings. Nullringe der Form $R = \{0_R\}$ sind generell keine Integritätsbereiche, weil das Nullelement 0_R nach Definition kein Nullteiler ist.

Lemma 9.6

(i) Ein Element a in einem Ring R kann nicht zugleich Nullteiler und Einheit sein.

(ii) Jeder Körper ist ein Integritätsbereich.

(iii) In jedem Integritätsbereich R gilt die ***Kürzungsregel***: Sind $a, b, c \in R$ mit $c \neq 0_R$, dann folgt aus $ac = bc$ die Gleichung $a = b$.

Beweis: zu (i) Angenommen, a ist zugleich Nullteiler und Einheit. Dann gibt es ein Element $b \neq 0_R$ mit $ab = 0_R$ und ein $c \in R$ mit $ca = 1_R$. Wir erhalten den Widerspruch $b = 1_R \cdot b = (ca)b = c(ab) = c0_R = 0_R$.

zu (ii) Nehmen wir an, dass R ein Körper, aber kein Integritätsbereich ist. Dann ist 0_R kein Nullteiler in R, oder es gibt einen Nullteiler $a \neq 0_R$. Die erste Möglichkeit ist ausgeschlossen, denn 1_R ist in jedem Ring stets eine Einheit, und aus $R^\times = R \setminus \{0_R\}$ folgt $1_R \neq 0_R$. Die Gleichung $1_R \cdot 0_R = 0_R$ zeigt also, dass 0_R ein Nullteiler ist. Aber auch die zweite Möglichkeit kann nicht eintreten, denn wegen $R^\times = R \setminus \{0_R\}$ wäre a zugleich Nullteiler und Einheit, was zu (i) im Widerspruch steht.

zu (iii) Aus $ac = bc$ folgt $(a-b)c = ac - bc = 0_R$. Wäre $a - b \neq 0_R$, dann wäre das Element ein Nullteiler ungleich 0_R. Weil R aber ein Integritätsbereich ist, muss $a - b = 0_R$ gelten. □

Einen Ringhomomorphismus zwischen Körpern bezeichnet man als ***Körperhomomorphismus***. Wir bemerken

Proposition 9.7 Ein Körperhomomorphismus $\phi : K \to L$ ist stets injektiv.

Beweis: Sei $a \in K$ ein Element im Kern, also ein Element mit $\phi(a) = 0_L$, und nehmen wir an, dass $a \neq 0_K$ ist. Dann folgt $1_L = \phi(1_K) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = 0_L\phi(a^{-1}) = 0_L$. Aber dies ist unmöglich, da L kein Nullring ist. □

Definition 9.8 Sei R ein Ring. Die ***Charakteristik*** eines Rings R ist definiert durch

$$\operatorname{char}(R) \quad = \quad \begin{cases} n & \text{falls } n \in \mathbb{N} \text{ minimal mit } n \cdot 1_R = 0_R \text{ ist,} \\ 0 & \text{falls } n \cdot 1_R \neq 0_R \text{ für alle } n \in \mathbb{N} \text{ gilt.} \end{cases}$$

Bei positiver Charakteristik ist $\operatorname{char}(R)$ also die Ordnung des Elements 1_R in der Gruppe $(R, +)$. Die Charakteristik kann auch den Wert 1 annehmen. Dies ist genau dann der Fall, wenn Null- und Einselement von R zusammenfallen, also $0_R = 1_R$ gilt. Wir untersuchen nun die Charakteristik von Integritätsbereichen. Wie allgemein üblich, bezeichnen wir eine natürliche Zahl n als ***Primzahl***, wenn $n > 1$ ist und keine Zahlen $r, s \in \mathbb{N}$ mit $1 < r, s < n$ und $n = rs$ existieren.

Proposition 9.9 Sei R ein Integritätsbereich. Dann ist die Charakteristik $\operatorname{char}(R)$ entweder gleich Null oder eine Primzahl.

Beweis: Wäre $\operatorname{char}(R) = 1$, dann wäre der Ring R (wie oben gezeigt) ein Nullring und damit kein Integritätsbereich. Nehmen wir nun an, dass $n = \operatorname{char}(R) > 1$, aber keine Primzahl ist. Dann gibt es natürliche Zahlen r, s mit $1 < r, s < n$ und $n = rs$. Nach Definition der Charakteristik gilt $r \cdot 1_R, s \cdot 1_R \neq 0_R$, aber $n \cdot 1_R = 0_R$. Die Gleichung $(r \cdot 1_R)(s \cdot 1_R) = (rs) \cdot 1_R = n \cdot 1_R = 0_R$ zeigt dann, dass die Elemente r_R und s_R des Rings R Nullteiler ungleich Null sind. Aber dies widerspricht der Voraussetzung, dass es sich bei R um einen Integritätsbereich handelt. □

Nach Proposition 9.9 ist also insbesondere $\operatorname{char}(K)$ für einen Körper gleich Null oder eine Primzahl. Es gibt beispielsweise keinen Körper der Charakteristik 4; inbesondere ist der Restklassenring $\mathbb{Z}/4\mathbb{Z}$ kein Körper, noch nicht einmal ein Integritätsbereich.

In der Gruppentheorie haben wir die Untergruppen einer Gruppe G als Teilmengen von G definiert, auf denen in natürlicher Weise wiederum eine Gruppenstruktur existiert. Nun führen wir einen entsprechenden Begriff für die Kategorie der Ringe ein.

Definition 9.10 Sei R ein Ring. Eine Teilmenge $S \subseteq R$ wird ***Teilring*** von R genannt, wenn $1_R \in S$ gilt und mit $a, b \in S$ jeweils auch die Elemente $a - b$ und ab in S liegen.

Umgekehrt bezeichnet man einen Ring R als ***Erweiterungsring*** eines anderen Rings S, wenn S ein Teilring von R ist. Das Paar (S, R) bezeichnet man in diesem Fall als ***Ringerweiterung***. Allgemein wird die Schreibweise $R|S$ verwendet, um ausdrücken, dass durch (S, R) eine Ringerweiterung gegeben ist.

Satz 9.11 Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$ ein Teilring. Dann ist die Menge S unter den Verknüpfungen $+$ und $\cdot$ abgeschlossen. Bezeichnen wir mit $+_S$ und $\cdot_S$ die auf S eingeschränkten Verknüpfungen, dann ist $(S, +_S, \cdot_S)$ ein Ring.

Beweis: Als erstes beweisen wir die Abgeschlossenheit. Aus $1_R \in S$ folgt zunächst $0_R = 1_R - 1_R \in S$, denn auf Grund der Teilring-Eigenschaft liegt Differenz zweier Elemente aus S wieder in S. Wegen $-a = 0_R - a$ ist mit jedem $a \in S$ auch das Negative $-a$ in S enthalten. Seien nun $a, b \in S$ vorgegeben. Dann gilt $-b \in S$ und somit $a + b = a - (-b) \in S$. Aus der Teilring-Eigenschaft folgt auch $ab \in S$. Also ist S tatsächlich unter $+$ und $\cdot$ abgeschlossen.

Nun überprüfen wir die Ringeigenschaften von $(S, +_S, \cdot_S)$. Wie bereits gezeigt wurde, gilt $0_R \in S$, und mit $a, b \in S$ liegen auch die Elemente $a + b$ und $-a$ in S. Also ist S eine Untergruppe von $(R, +)$, und wie in der Algebra-Vorlesung gezeigt wurde, ist $(S, +_S)$ damit eine Gruppe. Wegen

$$a +_S b \quad = \quad a + b \quad = \quad b + a \quad = \quad b +_S a \quad \text{für alle} \quad a, b \in S$$

ist diese auch kommutativ. Ebenso kann das Assoziativ- und Kommutativitätsgesetz von $\cdot_S$ auf die Assoziativität und Kommutativität von $\cdot$ zurückgeführt werden. Wegen $a \cdot_S 1_R = a \cdot 1_R = a$ und $1_R \cdot_S a = 1_R \cdot a = a$ ist 1_R das Neutralelement von $(S, \cdot_S)$. Schließlich leitet man auch das Distributivgesetz für $+_S$ und $\cdot_S$ aus dem entsprechenden Gesetz für $+_R$ und $\cdot_R$ ab. □

Beispielsweise ist $\mathbb{Z}$ ein Teilring von $\mathbb{Q}$, $\mathbb{Q}$ ein Teilring von $\mathbb{R}$ und $\mathbb{R}$ ein Teilring von $\mathbb{C}$. Die Menge $\mathbb{Z} \times \{0\}$ ist mit den Verknüpfungen $(a, 0) + (b, 0) = (a + b, 0)$ und $(a, 0) \cdot (b, 0) = (ab, 0)$ zwar ein Ring, aber *kein* Teilring von $\mathbb{Z} \times \mathbb{Z}$, denn das Einselement $1_{\mathbb{Z}\times\mathbb{Z}} = (1, 1)$ ist nicht in $\mathbb{Z} \times \{0\}$ enthalten.

Der soeben durchgeführte Beweis zeigt, dass für die Teilring-Eigenschaft $a - b \in S$ für $a, b \in S$ gefordert werden muss, um die Existenz von Negativen in S sicherzustellen. Würde man statt dessen $a + b \in S$ fordern, dann wäre die Unterstruktur S im allgemeinen kein Ring. Die Teilmenge $\mathbb{N} \subseteq \mathbb{Z}$ genügt beispielsweise den Bedingungen $1 \in \mathbb{N}$ und $a, b \in \mathbb{N} \Rightarrow a + b, ab \in \mathbb{N}$, ohne dass $(\mathbb{N}, +, \cdot)$ selbst ein Ring ist.

Lemma 9.12 Sei $(R,+,\cdot)$ ein Ring, und sei $(S_i)_{i\in I}$ eine Familie von Teilringen. Dann ist auch $S=\bigcap_{i\in I} S_i$ ein Teilring von R.

Beweis: Weil S_i für jedes $i\in I$ ein Teilring von R ist, gilt $1_R\in S_i$ für alle $i\in I$ und damit $1_R\in S$. Seien nun $a,b\in S$ vorgegeben. Dann folgt $a,b\in S_i$ für alle $i\in I$. Weil jedes S_i ein Teilring von R ist, gilt damit auch $a-b\in S_i$ iund $ab\in S_i$ für alle $i\in I$. Dies wiederum bedeutet $a-b\in S$ und $ab\in S$. Damit ist der Nachweis der Teilring-Eigenschaft von S abgeschlossen. □

Das Analogon zum Teilring in der Kategorie der Körper ist durch folgende Definition gegeben.

Definition 9.13 Sei K ein Körper. Eine Teilmenge $F\subseteq K$ wird ***Teilkörper*** von K genannt, wenn $1_K\in F$ gilt, für alle $a,b\in F$ auch die Elemente $a-b$ und ab in F liegen und für jedes $a\in F$, $a\neq 0_K$ auch $a^{-1}\in F$ gilt.

Wir haben in Lemma 9.11 gesehen, dass man durch Einschränkung von Addition und Multiplikation von K auf die Teilmenge F einen Ring erhält. Durch Bedingung, dass für jedes $a\in F\setminus\{0_K\}$ auch a^{-1} in F liegt, wird F darüber hinaus zu einem Körper. Die Begriffe „***Erweiterungskörper***“ und „***Körpererweiterung***“ sind in genauer Analogie zu den Ringen definiert.

Lemma 9.14 Sei K ein Körper und $(F_i)_{i\in I}$ eine beliebige Familie von Teilkörpern. Dann ist auch $F=\bigcap_{i\in I} F_i$ ein Teilkörper von K.

Beweis: Nach Lemma 9.12 ist F jedenfalls ein Teilring von K. Ist außerdem $a\in F^\times$, dann liegt a auch in $F_i^\times$ für jedes $i\in I$, und somit liegt auch a^{-1} jeweils in F_i. Daraus wiederum folgt $a^{-1}\in F$. Damit ist die Teilkörper-Eigenschaft von F nachgewiesen. □

Folgerung 9.15 Ist K ein Körper und ist $(F_i)_{i\in I}$ die Familie *aller* Teilkörper von K, dann nennt man $P=\bigcap_{i\in I} F_i$ den ***Primkörper*** von K. Es handelt sich um den bezüglich Inklusion kleinsten Teilkörper von K.

Beispielsweise ist $\mathbb{Q}$ der gemeinsame Primkörper von $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$, und für jede Primzahl ist $\mathbb{F}_p$ sein eigener Primkörper. Im Körpertheorie-Teil der Vorlesung werden wir sehen, dass der Primkörper jedes Körpers isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p$ für eine Primzahl p ist.

Satz 9.16 Sei $\tilde{R}|R$ eine Ringerweiterung und $A\subseteq\tilde{R}$ eine beliebige Teilmenge. Dann gibt es einen eindeutig bestimmten Teilring $R[A]$ von $\tilde{R}$ mit den folgenden beiden Eigenschaften.

(i) Es gilt $R[A]\supseteq R\cup A$.

(ii) Ist R' ein weiterer Teilring von $\tilde{R}$ mit $R'\supseteq R\cup A$, dann folgt $R'\supseteq R[A]$.

Damit ist $R[A]$ also der ***kleinste*** Teilring von $\tilde{R}$, der $R\cup A$ enthält. Man nennt ihn den von A über R ***erzeugten*** Teilring.

Beweis: *Existenz:* Sei $(S_i)_{i\in I}$ die Menge *aller* Teilringe von $\tilde{R}$ mit $S_i \supseteq R \cup A$. Nach Lemma 9.12 ist $R[A] = \bigcap_{i\in I} S_i$ ein Teilring von $\tilde{R}$. Wegen $R \cup A \subseteq S_i$ für alle $i \in I$ gilt auch $R \cup A \subseteq R[A]$. Ist nun R' ein beliebiger Teilring von $\tilde{R}$ mit $R' \supseteq R \cup A$, dann gilt $R' = S_i$ für ein $i \in I$ nach Definition der Familie $(S_i)_{i\in I}$. Weil $R[A]$ nach Definition der Durchschnitt aller Ringe in der Familie $(S_i)_{i\in I}$ ist, gilt $R[A] \subseteq R_i = R'$.

Eindeutigkeit: Sei S ein weiterer Teilring mit den Eigenschaften (i) und (ii). Dann ist S jedenfalls *ein* Teilring von $\tilde{R}$ mit $S \supseteq R \cup A$, und $R[A]$ ist der *kleinste* Teilring mit dieser Eigenschaft. Daraus folgt $R[A] \subseteq S$. Umgekehrt ist auch $R[A]$ ein Teilring von $\tilde{R}$ mit $R[A] \supseteq R \cup A$, und S ist der kleinste Teilring mit dieser Eigenschaft. Somit gilt auch $S \subseteq R[A]$, insgesamt $R[A] = S$. □

Ist $S = \{s\}$ einelementig, dann schreibt man an Stelle von $R[\{s\}]$ auch einfach $R[s]$ für den erzeugten Teilring. Auch bei mehreren Elementen werden die Mengenklammern oft weggelassen, man schreibt also statt $R[\{s_1, s_2\}]$ den Ausdruck $R[s_1, s_2]$ usw.

Als wichtiges Beispiel für erzeugte Teilringe sehen wir uns die ***quadratischen Zahlringe*** an. Dazu verabreden wir für die Bezeichnung von Quadratwurzeln reeller Zahlen die folgende Konvention. Ist $d \in \mathbb{R}$ positiv, dann sei $\sqrt{d}$ ein eindeutig bestimmte positive Quadratwurzel von d. Im Fall $d < 0$ sei $d \in \mathbb{C}$ die eindeutig bestimmte komplexe Quadratwurzel mit positivem Imaginärteil, also $\sqrt{d} = i\sqrt{|d|}$. Zu beachten ist, dass bei dieser Schreibweise die Gleichung

$$\sqrt{ab} \quad = \quad \sqrt{a} \cdot \sqrt{b}$$

im allgemeinen nicht erfüllt ist, nämlich dann nicht, wenn a und b beide negativ sind. Zum Beispiel ist $\sqrt{(-3)(-5)} \neq \sqrt{-3}\sqrt{-5}$, denn es gilt $\sqrt{-3}\sqrt{-5} = (i\sqrt{3})(i\sqrt{5}) = i^2\sqrt{15} = -\sqrt{15} \neq \sqrt{15} = \sqrt{(-3)(-5)}$.

Außerdem verwenden wir im Folgenden die ***Kongruenzschreibweise***. Sind $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$, so bedeutet der Ausdruck $a \equiv b \bmod n$, dass n ein Teiler von $b - a$ ist. Man sagt „Die Zahlen a und b sind kongruent modulo n." Ausführlicher werden wir uns mit den Kongruenzen in § 5 beschäftigen. Als konkrete Anwendung von Satz 9.16 zeigen wir nun

Satz 9.17 Sei $d \in \mathbb{Z}$ und $\sqrt{d} \in \mathbb{C}$ wie oben definiert.

(i) Es gilt $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

(ii) Ist $d \equiv 1 \bmod 4$, dann gilt $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})] = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{d} \mid a, b \in \mathbb{Z}, a \equiv b \bmod 2\}$.

Die Ringe dieser Form bezeichnen wir als ***quadratische Zahlringe***.

Beweis: zu (i) Sei M die Teilmenge auf der rechten Seite der Gleichung. Wir überprüfen, dass M ein Teilring von $\mathbb{C}$ ist. Wegen $1 = 1 + 0\sqrt{d}$ gilt $1 \in M$. Seien nun $\alpha, \beta \in M$ vorgegeben. Dann gibt es $r, s, t, u \in \mathbb{Z}$ mit $\alpha = r + s\sqrt{d}$ und $\beta = t + u\sqrt{d}$. Es folgt $\alpha - \beta = (r - t) + (s - u)\sqrt{d} \in M$ und

$$\alpha\beta \quad = \quad \left(r + s\sqrt{d}\right)\left(t + u\sqrt{d}\right) \quad = \quad (rt + sud) + (ru + st)\sqrt{d} \quad \in M.$$

Außerdem gilt $M \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$, denn für jedes $a \in \mathbb{Z}$ gilt $a = a + 0 \cdot \sqrt{d} \in M$ und $\sqrt{d} = 0 + 1 \cdot \sqrt{d} \in M$.

Sei nun R' ein beliebiger Teilring von $\mathbb{C}$ mit $R' \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$. Zu zeigen ist $R' \supseteq M$. Sei dazu $\alpha \in M$ vorgeben, $\alpha = r + s\sqrt{d}$ mit $r, s \in \mathbb{Z}$. Aus $r, s \in \mathbb{Z}$ folgt $r, s \in R'$. Ebenso ist $\sqrt{d}$ nach Voraussetzung in R' enthalten. Da es sich bei R' um einen Teilring von $\mathbb{C}$ handelt, der als solcher unter Addition und Multiplikation abgeschlossen ist, folgt daraus zunächst $s\sqrt{d} \in R'$ und dann $r + s\sqrt{d} \in R'$.

zu (ii) Zunächst überprüfen wir wieder, dass die Menge M auf der rechten Seite ein Teilring von $\mathbb{C}$ ist. Es gilt $1 = \frac{1}{2} \cdot 2 + \frac{1}{2} \cdot 0 \cdot \sqrt{d}$ in M, denn es gilt $2 \equiv 0 \bmod 2$. Seien nun $\alpha, \beta \in M$ vorgegeben. Dann gibt es $r, s, t, u \in \mathbb{Z}$ mit $\alpha = \frac{1}{2}r + \frac{1}{2}s\sqrt{d}$, $\beta = \frac{1}{2}t + \frac{1}{2}u\sqrt{d}$, wobei $r \equiv s \bmod 2$ und $t \equiv u \bmod 2$ gilt. Das Element

$$\alpha - \beta \quad = \quad \left(\tfrac{1}{2}r + \tfrac{1}{2}s\sqrt{d}\right) - \left(\tfrac{1}{2}t + \tfrac{1}{2}u\sqrt{d}\right) \quad = \quad \tfrac{1}{2}(r-t) + \tfrac{1}{2}(s-u)\sqrt{d}$$

liegt ebenfalls in M, denn aus $r \equiv s \bmod 2$ und $t \equiv u \bmod 2$ folgt $r - t \equiv s - u \bmod 2$. Um zu sehen, dass auch das Element

$$\alpha\beta \quad = \quad \left(\tfrac{1}{2}r + \tfrac{1}{2}s\sqrt{d}\right)\left(\tfrac{1}{2}t + \tfrac{1}{2}u\sqrt{d}\right) \quad = \quad \tfrac{1}{4}(rt + dsu) + \tfrac{1}{4}(st + ru)\sqrt{d} \quad = \quad \tfrac{1}{2}v + \tfrac{1}{2}w\sqrt{d}$$

mit $v = \frac{1}{2}(rt + dsu)$ und $w = \frac{1}{2}(st + ru)\sqrt{d}$ in M enthalten ist, müssen wir überprüfen, dass $2v + 2w = rt + dsu + st + ru$ durch 4 teilbar ist. Denn daraus folgt, dass $v + w$ gerade ist, was wiederum äquivalent dazu ist dass v und w beide gerade oder ungerade sind, also $v \equiv w \bmod 2$ erfüllen. Auf Grund der Voraussetzung $d \equiv 1 \bmod 4$ gilt $rt + dsu + st + ru \equiv rt + su + st + ru \equiv (r+s)(t+u) \bmod 4$, und die Zahl $(r+s)(t+u)$ ist durch 4 teilbar, weil $r+s$ und $t+u$ gerade sind. Insgesamt ist M also tatsächlich ein Teilring von $\mathbb{C}$. Außerdem gilt $M \supseteq \mathbb{Z} \cup \{\frac{1}{2}(1+\sqrt{d})\}$. Denn jedes $a \in \mathbb{Z}$ ist wegen $a = \frac{1}{2}(2a) + \frac{1}{2} \cdot 0\sqrt{d}$ und $2a \equiv 0 \bmod 2$ in M enthalten, und ebenso gilt $\frac{1}{2}(1+\sqrt{d}) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 \cdot \sqrt{d} \in M$ wegen $1 \equiv 1 \bmod 2$.

Sei nun R' ein weiterer Teilring von $\mathbb{C}$ mit $R' \supseteq \mathbb{Z} \cup \{\frac{1}{2}(1 + \sqrt{d})\}$. Zu zeigen ist $R' \supseteq M$. Sei dazu $\alpha \in M$ vorgegeben, $\alpha = \frac{1}{2}r + \frac{1}{2}s\sqrt{d}$ mit $r, s \in \mathbb{Z}$, $r \equiv s \bmod 2$. Dann gilt $\alpha - s \cdot \frac{1}{2}(1 + \sqrt{d}) = \frac{1}{2}(r - s)$. Wegen $\frac{1}{2}(r-s) \in \mathbb{Z}$ und $\mathbb{Z} \subseteq R'$ folgt $\frac{1}{2}(r-s) \in R'$. Aus $\frac{1}{2}(1 + \sqrt{d}) \in R'$ folgt ebenso $s \cdot \frac{1}{2}(1 + \sqrt{d}) \in R'$. Da R' unter Addition abgeschlossen ist, liegt damit auch α in R'. □

Zwei Zahlringe spielen in der Zahlentheorie eine besonders wichtige Rolle: der Ring $\mathbb{Z}[i]$ der ***Gauß'schen Zahlen*** und der Ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ der ***Eisenstein-Zahlen***.

Wir betrachten nun allgemeine Ringerweiterungen, die von nur einem Element erzeugt werden. Bereits in der Linearen Algebra haben wir den Polynomring $R[x]$ über einem Ring R eingeführt. Im nächsten Kapitel werden wir sehen, wie man diese Ringe konstruiert. Mit Hilfe der Polynome können wir Ringerweiterungen, die von einem einzigen Element erzeugt werden, explizit beschreiben.

Proposition 9.18 Sei $\tilde{R} \mid R$ eine Ringerweiterung und $c \in \tilde{R}$. Dann gilt $R[c] = \left\{ f(c) \;\middle|\; f \in R[x] \right\}$.

Beweis: Sei S die Teilmenge auf der rechten Seite der Gleichung. Wir zeigen, dass S ein Teilring von $\tilde{R}$ ist. Das Einselement $1_{\tilde{R}} = 1_R$ von $\tilde{R}$ ist in $R[c]$ enthalten, denn betrachten wir 1_R als konstantes Polynom, also als Element von $R[x]$, dann gilt $1_R = 1_R(c) \in S$. Seien nun $\alpha, \beta \in S$ vorgegeben. Dann gibt es Polynome $f, g \in R[x]$ mit $\alpha = f(c)$ und $\beta = g(c)$. Es folgt $\alpha - \beta = f(c) - g(c) = (f - g)(c) \in S$ und $\alpha\beta = f(c)g(c) = (fg)(c) \in S$. Dies zeigt, dass S tatsächlich ein Teilring von $\tilde{R}$ ist.

Um zu zeigen, dass S mit $R[c]$ übereinstimmt, müssen wir noch überprüfen, dass S in jedem Teilring R' von $\tilde{R}$ mit $R' \supseteq R \cup \{c\}$ enthalten ist. Sei also R' ein solcher Teilring und $\alpha \in S$. Zu zeigen ist $\alpha \in R'$. Nach Definition von S gibt es ein $f \in R[x]$ mit $\alpha = f(c)$. Schreiben wir $f = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}_0$ und $a_0, ..., a_n \in R$, dann gilt $\alpha = \sum_{k=0}^{n} a_k c^k$. Weil die Elemente $a_0, ..., a_n, c$ nach Voraussetzung in R' liegen, gilt auch $a_k c^k \in R'$ für $0 \leq k \leq n$, auf Grund der Abgeschlossenheit von R' unter der Multiplikation von $\tilde{R}$. Aus der Abgeschlossenheit von R' unter Addition (und vollständiger Induktion über n) folgt dann auch, dass $\alpha = \sum_{k=0}^{n} a_k c^k$ in R' liegt. □

§ 10. Ideale

Zusammenfassung. Ideale sind Teilmengen von Ringen, mit denen in gewissen Grenzen auf ähnliche Weise gerechnet werden kann wie mit Ringelementen. Ursprünglich eingeführt wurden sie in Mathematik, um einen Ersatz für die eindeutige Primfaktorzerlegung zu erhalten, die in vielen Ringen, wie sie z.B. in der Zahlentheorie und der Algebraischen Geometrie vorkommen, nicht mehr gültig ist. Auch in anderen Bereichen der Mathematik haben sich die Ideale als nützliches Konzept erwiesen, beispielsweise in Funktionanalysis.

Nach der Definition der Ideale eines Rings, und der Definition der Hauptideale als wichtigen Spezialfall, beschäftigen wir uns zunächst mit der Beziehung der Ideale zur Teilerrelation. Wie wir es bereits bei den Untergruppen und den Ringerweiterungen gesehen haben, lassen sich auch Ideale durch die Angabe von Erzeugendensystemen definieren. Mit der Summe und dem Produkt von lernen wir die zwei zentrale Rechenoperationen der Idealtheorie kennen. Als besonders wichtige Idealtypen werden die ***Primideale*** und die ***maximalen Ideale*** eingeführt. Im nächsten Kapitel werden wir sehen, dass die Ideale das natürliche Analogon der Normalteiler in der Gruppentheorie sind, weil auch sie zur Definition von Faktorstrukturen genutzt werden können. In diesem Kontext werden die beiden genannten Idealtypen eine wichtige Rolle spielen.

Wichtige Grundbegriffe

- Ideale, Hauptideal, erzeugtes Ideal
- Teilbarkeitsrelation, ggT und kgV
- Rechenoperationen für Ideale (Summen, Produkte)
- Primideale und maximale Ideale

Zentrale Sätze

- Interpretation der Teilbarkeitsrelation durch Ideale
- Existenz und Eindeutigkeit des von einer Teilmenge erzeugten Ideals
- Rechenregeln für Ideale und Erzeugendensysteme
- Charakterisierung der Primideale
- Verhalten der Ideale unter Ringhomomorphismen

Definition 10.1 Sei R ein Ring. Ein ***Ideal*** in R ist eine Teilmenge $I \subseteq R$ mit den Eigenschaften

(i) $0_R \in I$

(ii) Für alle $a, b \in I$ und $r \in R$ gilt $a + b \in I$ und $ra \in I$.

Eine wichtige Rolle spielen die Ideale der folgenden Form.

Proposition 10.2 Ist R ein Ring und $b \in R$, dann ist die Menge der Vielfachen $\{ab \mid a \in R\}$ von b ein Ideal in R. Man nennt ein solches Ideal ein ***Hauptideal*** und bezeichnet es mit (b). Ein ***Hauptidealring*** ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist. In jedem Ring R ist das ***Nullideal*** $(0_R) = \{0_R\}$ das kleinste und das ***Einheitsideal*** $(1_R) = R$ das bezüglich Inklusion größte Ideal.

Beweis: Sei $b \in R$. Wir überprüfen, dass die Teilmenge (b) von R die in Definition 10.1 genannten Eigenschaften hat. Wegen $0_R = 0_R \cdot b$ ist 0_R in (b) enthalten. Seien nun $c, d \in (b)$ und $r \in R$ vorgegeben. Wegen $c, d \in (b)$ gibt es $a_1, a_2 \in R$ mit $c = a_1 b$ und $d = a_2 b$. Es folgt $c + d = (a_1 + a_2)b \in (b)$. Ebenso gilt $rc = r(a_1 b) = (ra_1)b \in (b)$. Also ist (b) tatsächlich ein Ideal.

Für alle $a \in R$ gilt $a \cdot 0_R = 0_R$. Dies zeigt, dass das Nullideal (0_R) tatsächlich als einziges Element 0_R enthält und damit das bezüglich Inklusion kleinste Ideal ist. Wegen $a \cdot 1_R = a$ für alle $a \in R$ enthält das Einheitsideal (1_R) alle Ringelemente und ist damit das bezüglich Inklusion größte Ideal. □

Ähnlich wie für Untergruppen, Normalteiler und Teilringe gilt auch für die Ideale

Proposition 10.3 Sei R ein Ring und $(I_j)_{j \in A}$ eine Familie von Idealen in R. Dann ist $I = \bigcap_{j \in A} I_j$ ein Ideal in R.

Beweis: Weil jedes I_j ein Ideal ist, gilt $0_R \in I_j$ für alle $j \in A$ und somit $0_R \in I$. Seien nun $a, b \in I$ und $r \in R$ vorgegeben. Dann gilt $a, b \in I_j$ für alle $j \in A$. Aus der Idealeigenschaft folgt $a + b \in I_j$ und $ra \in I_j$ für alle $j \in A$. Dies wiederum bedeutet $a + b \in I$ und $ra \in I$. □

Das Konzept der Erzeugendensysteme ist uns bereits aus der Linearen Algebra und der Gruppentheorie bekannt. Auch Teilringe, die von einer Menge erzeugt werden, haben wir bereits definiert, siehe dazu Satz 9.16.

Definition 10.4 Sei R ein Ring und $S \subseteq R$ eine Teilmenge. Man sagt, ein Ideal I in R wird von S ***erzeugt*** und schreibt $I = (S)$, wenn folgende Bedingungen erfüllt sind.

(i) $I \supseteq S$

(ii) Ist J ein Ideal in R mit $J \supseteq S$, dann folgt $J \supseteq I$.

Insgesamt ist I also das *kleinste* Ideal mit der Eigenschaft $I \supseteq S$.

Existenz und Eindeutigkeit des Ideals (S) beweist man wie bei den Teilringen. Für die Existenz bildet man die Familie $(I_j)_{j \in A}$ aller Ideale in R, die S enthalten und überprüft dann, dass

$$I \quad = \quad \bigcap_{j \in A} I_j$$

die Bedingungen (i) und (ii) aus Definition 10.4 erfüllt. Nehmen wir nun an, dass J ein weiteres Ideal ist, dass diese Bedingungen erfüllt. Dann liefert die Anwendung von (ii) sowohl $J \supseteq I$ als auch $I \supseteq J$, insgesamt also $I = J$. Ist S endlich, $S = \{a_1, ..., a_n\}$, dann verwendet man an Stelle von (S) auch die Schreibweise $(a_1, ..., a_n)$ für das erzeugte Ideal. Der folgende Satz gibt an, wie die Elemente eines solchen Ideals konkret aussehen.

Proposition 10.5 Sei R ein Ring, und seien $a_1, ..., a_n \in R$. Dann gilt

$$(a_1, ..., a_n) \quad = \quad \left\{ \sum_{i=1}^{n} r_i a_i \;\middle|\; r_1, ..., r_n \in R \right\}.$$

Beweis: Sei I die Menge auf der rechten Seite der Gleichung. Wir überprüfen, dass I die definierenden Eigenschaften des von $\{a_1, ..., a_n\}$ erzeugten Ideals besitzt. Zunächst zeigen wir, dass I ein Ideal ist. Das Element 0_R ist in I enthalten, denn es gilt $0_R = 0_R a_1 + ... + 0_R a_n$. Seien nun $a, b \in I$ und $r \in R$ vorgegeben. Dann existieren nach Definition von I Elemente $r_1, ..., r_n, r'_1, ..., r'_n \in R$, so dass

$$a = \sum_{i=1}^{n} r_i a_i \qquad \text{und} \qquad b = \sum_{i=1}^{n} r'_i a_i$$

gilt. Wir erhalten

$$a + b = \sum_{i=1}^{n} (r_i + r'_i) a_i \in I \qquad \text{und} \qquad ra = \sum_{i=1}^{n} (r r_i) a_i \in I.$$

Damit ist die Idealeigenschaft von I bewiesen. Außerdem enthält I die Menge S. Ist nämlich $j \in \{1, ..., n\}$, dann gilt $a_j = \sum_{i=1}^{n} \delta_{ij} a_i \in I$, wobei $\delta_{ij} \in \{0_R, 1_R\}$ jeweils das Kronecker-Delta bezeichnet. Sei nun J ein weiteres Ideal mit $J \supseteq I$. Sind $r_1, ..., r_n \in R$ beliebig gewählt, dann enthält J auf Grund der Idealeigenschaft die Elemente $r_1 a_1, ..., r_n a_n$, und durch einen einfachen Induktionsbeweis zeigt man, dass auch die Summe $\sum_{i=1}^{n} r_i a_i$ in J enthalten ist. Damit ist die Inklusion $J \supseteq I$ nachgewiesen. □

Die folgende Regel wird häufig beim Rechnen mit Idealen verwendet, die durch Erzeugendensysteme definiert sind.

Lemma 10.6 Sei R ein Ring, und seien $S, T \subseteq R$ beliebige Teilmengen. Gilt für die erzeugten Ideale $S \subseteq (T)$ und $T \subseteq (S)$, dann folgt $(S) = (T)$.

Beweis: Nach Definition ist (S) das *kleinste* Ideal, das S als Teilmenge enthält, und wegen $S \subseteq (T)$ ist (T) jedenfalls *ein* Ideal mit dieser Eigenschaft. Daraus folgt $(S) \subseteq (T)$, und ebenso erhält man $(T) \subseteq (S)$. □

Die Ideale stehen in einer engen Beziehung zur *Teilerrelation* auf den Elementen eines Rings.

Definition 10.7 Seien R ein Ring und $a, b \in R$. Wir sagen, dass a ein ***Teiler*** von b ist und schreiben $a|b$, wenn ein $c \in R$ mit $b = ac$ existiert. Gilt sowohl $a|b$ als auch $b|a$, dann sagt man, die Elemente a und b sind ***assoziiert*** zueinander.

Es ist leicht zu sehen, dass es sich bei der Relation „assoziiert“ um eine Äquivalenzrelation handelt. In Integritätsbereichen lässt sich die Relation auch folgendermaßen beschreiben.

Lemma 10.8 Ist R ein Integritätsbereich, so sind $a, b \in R$ genau dann zueinander assoziiert, wenn ein $\varepsilon \in R^\times$ mit $b = \varepsilon a$ existiert.

Beweis: „⇐“ Aus $b = \varepsilon a$ folgt $a|b$, und wegen $a = \varepsilon^{-1} b$ gilt auch $b|a$.

„⇒“ Nach Voraussetzung gilt $a|b$ und $b|a$, es gibt also Elemente $c, d \in R$ mit $b = ac$ und $a = bd$. Es folgt $a = acd$. Ist $a = 0$, dann gibt dasselbe für b, und die Gleichung $b = \varepsilon a$ ist mit der Einheit $\varepsilon = 1$ erfüllt. Ansonsten können wir auf $a \cdot 1 = acd$ die Kürzungsregel anwenden und erhalten $cd = 1$. Dies zeigt, dass $\varepsilon = c$ ein Einheit ist, also ist auch hier $b = \varepsilon a$ für ein geeignetes Element $\varepsilon \in R^\times$ erfüllt. □

Definition 10.9 Sei R ein Ring mit $a_1, ..., a_n \in R$. Wir sagen, ein Element $d \in R$ ist ein ***größter gemeinsamer Teiler*** (kurz ggT) von $a_1, ..., a_n$, wenn gilt

(i) $d|a_i$ für $1 \leq i \leq n$

(ii) Ist $b \in R$ mit $b|a_i$ für $1 \leq i \leq n$, dann folgt $b|d$.

Wir nennen die Elemente $a_1, ..., a_n$ ***teilerfremd***, wenn 1_R ein ggT der Elemente ist.

Definition 10.10 Sei R ein Ring mit $a_1, ..., a_n \in R$. Ein Element $e \in R$ heißt ***kleinstes gemeinsames Vielfaches*** (kurz kgV) von $a_1, ..., a_n$, wenn gilt

(i) $a_i|e$ für $1 \leq i \leq n$

(ii) Ist $b \in R$ mit $a_i|b$ für $1 \leq i \leq n$, dann folgt $e|b$.

Häufig schreibt man der Einfachheit halber $d = \text{ggT}(a_1, ..., a_n)$, um auszudrücken, dass d ein ggT von $a_1, ..., a_n$ ist. Dabei handelt es sich aber um keine Gleichung im herkömmlichen Sinn, weil der ggT im Allgemeinen nicht eindeutig bestimmt ist. Statt dessen gilt

Lemma 10.11 Sei R ein Ring und $d \in R$ ein größter gemeinsamer Teiler der Ringelemente $a_1, ..., a_n$. Ein weiteres Element $d' \in R$ ist genau dann ein ggT von $a_1, ..., a_n$, wenn d und d' zueinander assoziiert sind. Dieselbe Aussage gilt auch für das kleinste gemeinsame Vielfache.

Beweis: Sei d' ein weiterer ggT von $a_1, ..., a_n$. Nach Voraussetzung gilt $d'|a_i$ für $1 \leq i \leq n$. Weil nach Voraussetzung $d = \text{ggT}(a_1, ..., a_n)$ ist, folgt daraus $d'|d$. Genauso zeigt man $d|d'$, also sind d und d' assoziiert.

Sind umgekehrt d, d' zueinander assoziierte Elemente und ist $d = \text{ggT}(a_1, ..., a_n)$, dann folgt aus $d'|d$ und $d|a_i$ jeweils $d'|a_i$ für $1 \leq i \leq n$. Ist $b \in R$ ein Element mit $b|a_i$ für alle i, dann gilt $b|d$ auf Grund der ggT-Eigenschaft von d. Aus $b|d$ und $d|d'$ folgt $b|d'$. Damit ist insgesamt bewiesen, dass es sich bei d' um einen ggT der Elemente $a_1, ..., a_n$ handelt. Für das kleinste gemeinsame Vielfache verläuft der Beweis völlig analog. □

Wir haben oben die Hauptideale der Form (b) für ein Element b eines Rings R definiert. Es ist leicht zu überprüfen, dass für beliebige $b, c \in R$ auch Teilmengen der Form $(b, c) = \{ub + vc \mid u, v \in R\}$ jeweils ein Ideal in R bilden. Es handelt sich dabei um ein *endlich erzeugtes* Ideal. Diese werden weiter unten in Proposition 10.5 in allgemeiner Form betrachtet.

Satz 10.12 Sei R ein Ring, und seien $a, b \in R$.

(i) Es gilt $(a) \subseteq (b)$ genau dann, wenn b ein Teiler von a ist.

(ii) Ist $d \in R$ mit $(d) = (a, b)$, dann ist d ein ggT von a und b.

(iii) Ist $e \in R$ mit $(e) = (a) \cap (b)$, dann ist e ein kgV von a und b.

Ist R ein Hauptidealring, dann gilt auch von (ii) und (iii) die Umkehrung.

Beweis: zu (i) „⇒“ Aus $(a) \subseteq (b)$ folgt insbesondere $a \in (b)$. Da das Hauptideal (b) aus den Vielfachen von b besteht, bedeutet dies, dass ein $r \in R$ mit $a = rb$ existiert. Daraus folgt $b \mid a$. „⇐“ Nach Voraussetzung gibt es ein $r \in R$ mit $a = rb$, also gilt $a \in (b)$. Also ist (b) ein Ideal, dass a enthält, und nach Definition des von a erzeugten Ideals folgt $(a) \subseteq (b)$.

zu (ii) Aus $(d) = (a, b)$ folgt insbesondere $a \in (d)$ und $b \in (d)$. Es gibt also $r, s \in R$ mit $a = rd$ und $b = sd$. Dies zeigt, dass d ein gemeinsamer Teiler von a und b ist. Sei nun d' ein weiteres Ringelement mit $d' \mid a$ und $d' \mid b$. Dann gibt es $r', s' \in R$ mit $a = r'd'$ und $b = s'd'$. Also enthält das Hauptideal (d') die zweielementige Menge $\{a, b\}$. Nach Definition des erzeugten Ideals folgt $(a, b) \subseteq (d')$ und somit $(d) \subseteq (d')$. Nach Teil (i) ist d' damit ein Teiler von d. Insgesamt haben wir damit die ggT-Eigenschaft von d nachgerechnet.

zu (iii) Aus $(e) = (a) \cap (b)$ folgt $e \in (a)$ und $e \in (b)$. Es gibt also Ringelemente $r, s \in R$ mit $e = ra$ und $e = sb$. Damit ist e ein gemeinsames Vielfaches von a und b. Sei nun $e' \in R$ ein weiteres gemeinsames Vielfaches von a und b. Dann gibt es $r', s' \in R$ mit $e' = r'a$ und $e' = s'b$, und wir erhalten $e' \in (a) \cap (b)$. Es folgt $(e') \subseteq (a) \cap (b) = (e)$ und somit $e' \in (e)$. Dies zeigt, dass e' ein Vielfaches von e ist. Insgesamt ist e also ein kgV von a und b.

Setzen wir nun voraus, dass R ein Hauptidealring ist, und beweisen wir die Umkehrung von (ii). Sei d ein ggT der Elemente a und b. Das Ideal (a, b) ist ein Hauptideal, es gibt also ein $d' \in R$ mit $(a, b) = (d')$. Auf Grund von Teil (ii) ist d' ebenfalls ein ggT von a und b, also sind d und d' assoziiert. Aus $d \mid d'$ und $d' \mid d$ folgt nach Teil (i), dass $(d) = (d') = (a, b)$ gilt.

Zum Schluss beweisen wir die Umkehrung von (iii) unter der Voraussetzung, dass R ein Hauptidealring ist. Sei e ein kgV der Elemente a und b. Weil $(a) \cap (b)$ ein Hauptideal ist, gilt $(a) \cap (b) = (e')$ für ein $e' \in R$. Nach Teil (iii) ist e' damit ebenfalls ein kgV von a und b, also sind e und e' assoziiert. Wie im vorherigen Absatz folgt daraus $(e) = (e') = (a) \cap (b)$. □

Im Folgenden werden wir nun zwei wichtige Rechenoperationen auf Idealen definieren. Wie die Ringelemente können auch Ideale ***addiert*** und ***multipliziert*** werden.

Proposition 10.13 Sei ein Ring, und seien I, J Ideale in R. Dann ist auch die Teilmenge $I + J = \{\, a + b \mid a \in I, b \in J \,\}$ von R ein Ideal in R.

Beweis: Aus $0_R \in I$ und $0_R \in J$ folgt $0_R = 0_R + 0_R \in I + J$. Seien nun $a, b \in I + J$ und $r \in R$ vorgegeben. Dann gibt es Elemente $a', b' \in I$ und $a'', b'' \in J$ mit $a = a' + a''$ und $b = b' + b''$. Weil I und J Ideale sind, gilt $a' + b' \in I$ und $a'' + b'' \in J$. Es folgt $a + b = (a' + b') + (a'' + b'') \in I + J$. Die Idealeigenschaft von I und J liefert auch $ra' \in I$ und $ra'' \in J$. Es folgt $ra = ra' + ra'' \in I + J$. □

Leider ist die Definition des *Produkts* zweier Ideale I und J nicht ganz so einfach. Man ist versucht, dass Produkt durch $IJ = \{\, ab \mid a \in I, b \in J \,\}$ zu definieren, aber leider ist eine solche Menge im Allgemeinen kein Ideal mehr. (Weiter unten werden wir dies durch ein Gegenbeispiel belegen.) Statt dessen müssen wir das von dieser Produktmenge erzeugte Ideal betrachten.

Definition 10.14 Sei R ein Ring, und seien I, J Ideale in R. Dann ist das ***Produktideal*** IJ das von der Menge $\{ab \mid a \in I, b \in J\}$ erzeugte Ideal in R.

Die folgende Proposition ist für die Berechnung von Produktidealen hilfreich.

> **Proposition 10.15** Sei R ein Ring, und seien I, J von endlichen vielen Ringelementen erzeugte Ideale, $I = (a_1, ..., a_m)$ und $J = (b_1, ..., b_n)$ mit $m, n \in \mathbb{N}$, $a_i, b_j \in R$ für $1 \leq i \leq m$, $1 \leq j \leq n$. Dann wird IJ von der Menge
>
> $$S \quad = \quad \{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$
>
> erzeugt, es gilt also $IJ = (S)$.

Beweis: Nach Definition des Produktideals gilt $IJ = (T)$ mit $T = \{\, ab \mid a \in I, b \in J \,\}$. Nach Lemma 10.6 genügt es also, $S \subseteq (T)$ und $T \subseteq (S)$ nachzuweisen. Die Inklusion $S \subseteq (T)$ ist offenbar erfüllt, weil für alle i, j mit $1 \leq i \leq m$ und $1 \leq j \leq n$ jeweils $a_i \in I$, $b_j \in J$ und damit $a_i b_j \in T$ gilt. Zum Beweis von $T \subseteq (S)$ sei $c \in T$ vorgegeben. Dann gibt es $a \in I$ und $b = J$ mit $c = ab$. Wegen $I = (a_1, ..., a_m)$ gibt es Ringelemente $r_1, ..., r_m \in R$, so dass a in der Form $\sum_{i=1}^{m} r_i a_i$ geschrieben werden kann. Ebenso finden wir $s_1, ..., s_n \in R$ mit $b = \sum_{j=1}^{n} s_j b_j$. Es gilt also

$$c \quad = \quad ab \quad = \quad \left(\sum_{i=1}^{m} r_i a_i\right)\left(\sum_{j=1}^{n} s_j b_j\right) \quad = \quad \sum_{i=1}^{m}\sum_{j=1}^{n} r_i s_j (a_i b_j).$$

Die Gleichung zeigt, dass c in (S) enthalten ist. □

Wir zeigen nun anhand eines Gegenbeispiels, dass das elementweise Produkt zweier Ideale im allgemeinen kein Ideal ist. Sei $R = \mathbb{Z}[x]$, und seien die Ideale I und J definiert durch $I = (2, x)$ und $J = (3, x)$. Nach Proposition 10.5 sind die Elemente aus $I = (2, x)$ die Polynome der Form $2u + xv$ mit $u, v \in \mathbb{Z}[x]$. Wie man sich leicht überlegt, sind es genau die Polynome $f \in \mathbb{Z}[x]$ mit durch 2 teilbarem konstanten Term $f(0)$, die auf diese Weise zu Stande kommen, zum Beispiel $x^2 + 5x - 10 = 2(-5) + x(x + 5)$ mit dem konstanten Term -10. Ebenso besteht J genau aus den Polynomen $g \in \mathbb{Z}[x]$ mit der Eigenschaft, dass $g(0)$ durch 3 teilbar ist.

Wegen $-2, x \in I$ und $3, x \in J$ sind $3x$ und $(-2)x$ in M enthalten. Nehmen wir nun an, dass die Menge gegeben durch $M = \{fg \mid f \in I, g \in J\}$ ein Ideal in $\mathbb{Z}[x]$ ist, dann wäre auch $x = 3x + (-2)x \in M$. Aber andererseits kann x nicht in der Form $x = fg$ mit $f \in I$ und $g \in J$ geschrieben werden. Wäre dies so, dann würde wegen $\text{grad}(f) + \text{grad}(g) = \text{grad}(fg) = \text{grad}(x) = 1$ jeweils $\text{grad}(f), \text{grad}(g) \leq 1$ folgen. Es gäbe also $a, b, c, d \in \mathbb{Z}$ mit $f = ax + b$ und $g = cx + d$. Wir würden dann

$$x \quad = \quad fg \quad = \quad (ax + b)(cx + d) \quad = \quad acx^2 + (bc + ad)x + bd$$

erhalten, also insbesondere $ac = 0$. Ist nun $a = 0$, dann folgt $x = bcx + bd$ und somit $bc = 1$. Wie oben bemerkt, ist $b = f(0)$ aber durch 2 teilbar,was zu $bc = 1$ im Widerspruch steht. Ebenso führt $c = 0$ auf die Gleichung $x = adx + bd$, und wir erhalten $ad = 1$ im Widerspruch zu $3 \mid g(0) \Leftrightarrow 3 \mid d$.

Die Annahme, dass M ein Ideal in $\mathbb{Z}[x]$ ist, war also falsch. Nach Proposition 10.15 ist das Produktideal IJ gegeben durch $IJ = (6, 2x, 3x, x^2)$. Mit Lemma 10.6 lässt sich dies zu $IJ = (6, x)$ vereinfachen, denn einerseits sind die Elemente $6, 2x, 3x, x^2$ offenbar alle in $(6, x)$ enthalten, andererseits liegen 6 und x wegen $x = (-1)(2x) + 3x$ auch in $(6, 2x, 3x, x^2)$.

Im Hinblick auf spätere Anwendungen zeigen wir noch

Lemma 10.16 Für Ideale I, J, K in einem Ring R gilt das Distributivgesetz $I(J+K) = IJ + IK$, außerdem gilt $IJ \subseteq I$ und $IJ \subseteq J$.

Beweis: „$\subseteq$“ Die Elemente der Form ab mit $a \in I$ und $b \in J+K$ bilden ein Erzeugendensystem von $I(J+K)$. Es genügt also zu zeigen, dass alle Elemente dieser Bauart in $IJ + IK$ enthalten sind. Das Element b kann in der Form $b = c + d$ mit $c \in J$ und $d \in K$ geschrieben werden. Es gilt $ab = a(c+d) = ac + ad$, mit $ac \in IJ$ und $ad \in IK$. Also ist ab in $IJ + IK$ enthalten.

„$\supseteq$“ Hier genügt es zu zeigen, dass $IJ \subseteq I(J+K)$ und $IK \subseteq I(J+K)$ gilt. Das Ideal IJ wird erzeugt von den Elementen der Form ab mit $a \in I$ und $b \in J$, und es reicht zu zeigen, dass diese Produkte in $I(J+K)$ enthalten sind. Aus $b \in J$ folgt $b \in J+K$, also ist $ab \in I(J+K)$ erfüllt. Die Inklusion $IK \subseteq I(J+K)$ beweist man genauso. Auch für die Inklusion $IJ \subseteq I$ brauchen wir nur zu zeigen, dass $\{ab \mid a \in I, b \in J\}$ eine Teilmenge von I ist. Dies ist auf Grund der Idealeigenschaft offensichtlich. Die Inklusion $IJ \subseteq J$ ist damit auch klar. □

Definition 10.17 Ein Ideal $\mathfrak{p}$ in einem Ring R wird ***Primideal*** genannt, wenn $\mathfrak{p} \neq (1)$ gilt und für alle $a, b \in R$ die Implikation

$$ab \in \mathfrak{p} \quad \Rightarrow \quad a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p} \quad \text{erfüllt ist.}$$

Man nennt $\mathfrak{p}$ ein ***maximales*** Ideal, wenn $\mathfrak{p} \neq (1)$ ist und kein Ideal I mit der Eigenschaft $\mathfrak{p} \subsetneq I \subsetneq (1)$ existiert, das Ideal also abgesehen vom Einheitsideal bezüglich Inklusion maximal ist.

Gelegentlich wird die Primideal-Bedingung nicht mit Elementen, sondern mit Idealen formuliert.

Proposition 10.18 Ein Ideal $\mathfrak{p}$ in einem Ring R ist genau dann ein Primideal in R, wenn $\mathfrak{p} \neq (1)$ ist und für beliebige Ideale I, J mit $IJ \subseteq \mathfrak{p}$ eine der Bedingungen $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$ erfüllt ist.

Beweis: „$\Leftarrow$“ Nehmen wir an, dass die Idealbedingung für R erfüllt ist, und seien $a, b \in R$ mit $ab \in \mathfrak{p}$ vorgegeben. Dann betrachten wir die Ideale $I = (a)$ und $J = (b)$. Das Produktideal IJ wird auf Grund der Bemerkung von oben durch das Element ab erzeugt, und mit ab ist auch das Ideal IJ in $\mathfrak{p}$ enthalten. Auf Grund unserer Voraussetzung folgt $(a) = I \subseteq \mathfrak{p}$ oder $(b) = J \subseteq \mathfrak{p}$, insbesondere $a \in I$ oder $b \in J$. Da außerdem $\mathfrak{p} \neq (1)$ gilt, handelt es sich bei $\mathfrak{p}$ tatsächlich um ein Primideal.

„$\Rightarrow$“ Sei $\mathfrak{p}$ ein Primideal. Dann ist $\mathfrak{p} \neq (1)$. Seien nun I und J Ideale in R, und nehmen wir an, dass zwar $IJ \subseteq \mathfrak{p}$, aber weder $I \subseteq \mathfrak{p}$ noch $J \subseteq \mathfrak{p}$ erfüllt ist. Dann gibt es Elemente $a \in I \setminus \mathfrak{p}$ und $b \in J \setminus \mathfrak{p}$. Weiter gilt $ab \in IJ \in \mathfrak{p}$. Wir haben also Elemente $a, b \in R$ mit $ab \in \mathfrak{p}$ und $a, b \notin \mathfrak{p}$ gefunden, im Widerspruch zur Primidealeigenschaft. □

An dieser Stelle kommen wir auf die zu Anfang erwähnte Beziehung zwischen Idealen und Teilbarkeitslehre zurück. Für viele wichtige zahlentheoretische Problem (etwa Fermats letzten Satz oder Verallgemeinerungen des quadratischen Reziprozitätsgesetzes, das wir später noch kennenlernen werden) hat es sich als nützlich herausgestellt, Fragen der Teilbarkeit in allgemeinen Ringen wie z.B. dem Ring $\mathbb{Z}[\sqrt{-5}]$ zu studieren. Insbesondere lassen sich in solchen

Ringen Elemente definieren, die ähnlich wie die bekannten Primzahlen nicht weiter zerlegt werden können. Wir werden für solche Elemente später die Bezeichnung *irreduzibel* einführen. Im Ring $\mathbb{Z}[\sqrt{-5}]$ ist zum Beispiel $1-2\sqrt{-5}$ ein irreduzibles Element, ebenso die Primzahl 3. Es kann aber auch vorkommen, dass eine Primzahl p im Ring $\mathbb{Z}[\sqrt{-5}]$ zerlegbar wird, zum Beispiel $41 = (6+\sqrt{-5})(6-\sqrt{-5})$.

Der Mathematiker *Eduard Kummer* beschäftigte sich im 19. Jahrhundert mit dem Problem, dass die Zerlegung von Zahlen in irreduzible Elemente in Ringen wie $\mathbb{Z}[\sqrt{-5}]$ im Allgemeinen nicht mehr eindeutig ist. Zum Beispiel gilt

$$21 \quad = \quad 3\cdot 7 \quad = \quad (1+2\sqrt{-5})(1-2\sqrt{-5}). \qquad (*)$$

Kummer gelang es, die Eindeutigkeit der Zerlegung wieder herzustellen, indem er an Stelle der Zerlegung der Zahl 21 die Zerlegung des Hauptideals (21) in *Primideale* betrachtete. So kann man zum Beispiel zeigen, dass die Ideale in $\mathbb{Z}[\sqrt{-5}]$ gegeben durch

$$\mathfrak{p}_1 = (3, 1+2\sqrt{-5}) \quad , \quad \mathfrak{p}_2 = (3, 1-2\sqrt{-5}) \quad , \quad \mathfrak{p}_3 = (7, 1+2\sqrt{-5}) \quad \text{und} \quad \mathfrak{p}_4 = (7, 1-2\sqrt{-5})$$

Primideale sind. Obwohl die Faktoren in der Produktdarstellung (*) irreduzibel sind, lassen sich die entsprechenden Hauptideale weiter zerlegen Mit Hilfe von Lemma 10.6 und Proposition 10.15 berechnet man zum Beispiel

$$\begin{aligned}
\mathfrak{p}_1\mathfrak{p}_3 \quad &= \quad (3,1+2\sqrt{-5})(7,1+2\sqrt{-5}) \quad = \quad (3\cdot 7,(1+2\sqrt{-5})\cdot 7, 3\cdot(1+2\sqrt{-5}),(1+2\sqrt{-5})(1+2\sqrt{-5})) \\
&= \quad (21, 7+14\sqrt{-5}, 3+6\sqrt{-5}, -19+4\sqrt{-5}) \quad = \quad (21, 1+2\sqrt{-5}, 3+6\sqrt{-5}, -19+4\sqrt{-5}) \quad = \\
&\qquad (21, 1+2\sqrt{-5}, 3+6\sqrt{-5}, 2+4\sqrt{-5}) \quad = \quad (21, 1+2\sqrt{-5}) \quad = \quad (1+2\sqrt{-5}).
\end{aligned}$$

Dabei gilt die Gleichung im vierten Schritt wegen 10.6 und $7+14\sqrt{-5} = (1+2\sqrt{-5})+2(3+6\sqrt{-5})$, im fünften wegen $-19+4\sqrt{-5}+21 = 2+4\sqrt{-5}$. Im vorletzten Schritt wurde verwendet, dass die Elemente $3+6\sqrt{-5}$ und $2+4\sqrt{-5}$ beides Vielfache von $1+2\sqrt{-5}$ sind und im letzten die Gleichung $21 = (1+2\sqrt{-5})(1-2\sqrt{-5})$. Die Rechnung zeigt also, dass das Hauptideal $(1+2\sqrt{-5})$ in die Faktoren $\mathfrak{p}_1$ und $\mathfrak{p}_3$ zerfällt.

Durch ähnliche Rechnungen erhält man die Gleichungen $\mathfrak{p}_1\mathfrak{p}_2 = (3)$, $\mathfrak{p}_2\mathfrak{p}_4 = (1-2\sqrt{-5})$ und $\mathfrak{p}_3\mathfrak{p}_4 = (7)$. Insgesamt gilt also

$$(21) = (3)\cdot(7) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) \qquad , \qquad \text{ebenso} \quad (21) = (1+2\sqrt{-5})(1-2\sqrt{-5}) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4).$$

Bis auf die Reihenfolge der „Primfaktoren“ $\mathfrak{p}_i$ stimmen die Zerlegungen also überein.

Definition 10.19 Sei $\phi : R \to S$ Ringhomomorphismus. Dann nennt man $\ker(\phi) = \phi^{-1}(\{0_S\})$ den ***Kern*** und $\mathrm{im}(\phi) = \phi(R)$ das ***Bild*** von ϕ.

Teil (i) der folgenden Proposition zeigt, dass Kerne von Ringhomomorphismen stets Ideale sind, in Analogie zur Aussage aus der Gruppentheorie, dass es sich bei Kernen von Gruppenhomomorphismen stets um Normalteiler handelt.

Proposition 10.20 Seien R, S Ringe und $\phi : R \to S$ ein Ringhomomorphismus.

(i) Ist J ein Ideal in S, dann ist $\phi^{-1}(J)$ ein Ideal in R.

(ii) Ist I ein Ideal in R und ϕ surjektiv, dann ist $\phi(I)$ ein Ideal in S.

Beweis: zu (i) Wegen $\phi(0_R) = 0_S$ und $0_S \in J$ ist $0_R \in \phi^{-1}(J)$ enthalten. Seien nun $a, b \in \phi^{-1}(J)$ und $r \in R$ vorgegeben. Dann gilt $\phi(a), \phi(b) \in J$, somit auch $\phi(a+b) \in J$ und $a+b \in \phi^{-1}(J)$. Ebenso ist $\phi(ra) = \phi(r)\phi(a) \in J$ und folglich $ra \in \phi^{-1}(J)$.

zu (ii) Wegen $0_R \in I$ gilt $0_S = \phi(0_R) \in \phi(I)$. Seien nun $a, b \in \phi(I)$ und $s \in S$ vorgegeben. Wegen $a, b \in \phi(I)$ gibt es $a', b' \in I$ mit $a = \phi(a')$ und $b = \phi(b')$. Es folgt $a' + b' \in I$ und $a + b = \phi(a') + \phi(b') = \phi(a' + b') \in \phi(I)$. Wegen der Surjektivität gibt es ein $r \in R$ mit $\phi(r) = s$, und mit a' ist auch ra' in I enthalten. Es folgt $sa = \phi(r)\phi(a') \in \phi(I)$. □

Ohne die Voraussetzung der Surjektivität ist Teil (ii) der Proposition im allgemeinen falsch. Betrachtet man z.B. die Inklusionsabbildung $\iota : \mathbb{Z} \to \mathbb{Q}$, $a \mapsto a$, dann ist $(2) = \{2a \mid a \in \mathbb{Z}\}$ ein Ideal in $\mathbb{Z}$, aber die Menge $M = \{2a \mid a \in \mathbb{Z}\}$ ist kein Ideal in $\mathbb{Q}$: Es gilt $\frac{1}{2} \in \mathbb{Q}$, $2 \in M$, aber $\frac{1}{2} \cdot 2 \notin M$.

Man überprüft leicht, dass das Bild $\mathrm{im}(\phi)$ eines Ringhomomorphismus $\phi : R \to S$ zwar im allgemeinen kein Ideal, aber immer ein Teilring von S ist. Wie bei den Gruppen oder den linearen Abbildungen zeigt man, dass ein Homomorphismus $\phi : R \to S$ genau dann injektiv ist, wenn $\ker(\phi) = \{0_R\}$ gilt.

§ 11. *Faktorringe und die Konstruktion von Ringerweiterungen*

Zusammenfassung. In § 4 haben wir aus einer Gruppe G und einem Normalteiler $N \trianglelefteq G$ eine neue Gruppe G/N konstruiert, die sog. Faktorgruppe von G modulo N. Mit dem gleichen Ansatz werden wir in diesem Abschnitt einem Ring R und einem Ideal I den ***Faktorring*** R/I zuordnen. Auf diesem Weg erhält man zum Beispiel für jedes $n \in \mathbb{N}$ den bereits aus der Linearen Algebra bekannten Restklassenring $\mathbb{Z}/n\mathbb{Z}$. Dort haben wir auch schon festgestellt, dass $\mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p ein Körper ist. Diese Beobachtung wird hier auf geeignete Weise verallgemeinert. Außerdem werden wir den aus § 4 bekannten Korrespondenzsatz auf die Ringe übertragen.

Ein weiteres Thema dieses Kapitels ist die Konstruktion von Ringerweiterungen. Von zentraler Bedeutung ist hier die Beobachtung, dass man für jeden Monomorphismus $\phi : R \to S$ von Ringen einen zu S isomorphen Erweiterungsring erhält. Unter Hinzunahme des Konzepts der Faktorringe werden wir auf diese Weise sehen, wie der Körper $\mathbb{R}$ der reellen zum Körper $\mathbb{C}$ der komplexen Zahlen erweitert werden kann. Dieses Prinzip werden wir im Körpertheorie-Teil der Vorlesung weiter vertiefen. Außerdem verwenden wir diesen Ansatz, um jedem Integritätsbereich R einen Quotientenkörper (den „Körper der Brüche von R“) und jedem Ring R den Polynomring $R[x]$ zuzuordnen (dessen Existenz wir in der Linearen Algebra nur postuliert, aber nicht bewiesen hatten).

Wichtige Grundbegriffe

- Nebenklasse eines Ideals, Faktorring
- kanonischer Epimorphismus (für Ringe)
- Kongruenz modulo eines Ideals
- Quotientenkörper eines Integritätsbereichs

Zentrale Sätze

- Homomorphiesatz für Ringe
- Korrespondenzsatz für Ringe
- Faktorringe von Primidealen sind Integritätsbereiche
  Faktorringe von maximalen Idealen sind Körper
- Konstruktion von Ringerweiterungen durch Monomorphismen
- universelle Eigenschaft des Quotientenkörpers und des Polynomrings

In der Gruppentheorie haben wir gesehen, wie die Normalteiler einer Gruppe zur Definition von neuen Gruppen genutzt werden können. Eine ähnliche Rolle spielen die Ideale in der Ringtheorie.

Definition 11.1 Sei R ein Ring, I ein Ideal und $a \in R$. Dann nennen wir die Menge

$$a + I \quad = \quad \{a + i \mid i \in I\}$$

die ***Nebenklasse*** von a modulo I. Die Menge $\{a + I \mid a \in R\}$ aller Nebenklassen von Elementen aus R bezeichnen wir mit R/I.

Proposition 11.2 Sei R ein Ring und I ein Ideal. Dann ist die Relation auf R gegeben durch

$$a \equiv b \bmod I \quad \Leftrightarrow \quad b - a \in I$$

eine Äquivalenzrelation, und die Elemente von R/I sind genau die Äquivalenzklassen dieser Relation. Man spricht in diesem Zusammenhang von einer ***Kongruenzrelation*** und bezeichnet zwei Elemente a, b in derselben Äquivalenzklasse als ***kongruent modulo*** I.

Beweis: Für alle $a \in R$ gilt $a - a = 0_R \in I$ und somit $a \equiv a \bmod I$. Also ist die Relation reflexiv. Für alle $a, b \in R$ gilt die Implikation

$$a \equiv b \bmod I \quad \Rightarrow \quad b - a \in I \quad \Rightarrow \quad (-1)(b-a) \in I \quad \Rightarrow \quad a - b \in I \quad \Rightarrow \quad b \equiv a \bmod I \quad ,$$

also ist die Relation symmetrisch. Zum Nachweis der Transitivität seien $a, b, c \in R$ mit $a \equiv b \bmod I$ und $b \equiv c \bmod I$ vorgegeben. Dann gilt $b - a \in I$ und $c - b \in I$. Es folgt $c - a = (c - b) + (b - a) \in I$ und damit $a \equiv c \bmod I$.

Nun zeigen wir noch, dass für ein beliebig vorgegebenes $a \in R$ die Nebenklasse $a + I$ mit der Äquivalenzklasse von a übereinstimmt. Nach Definition liegt $b \in I$ genau dann in der Äquivalenzklasse von a, wenn $a \equiv b \bmod I$ gilt, was nach Definition $b - a \in I$ bedeutet. Dies wiederum ist gleichbedeutend mit $b = a + (b - a) \in a + I$. □

Nach Definition sind zwei Elemente $a, b \in R$ also genau dann kongruent modulo I, wenn ihre Kongruenzklassen übereinstimmen. Da je zwei Äquivalenzklassen entweder disjunkt oder gleich sind, erhalten wir die Äquivalenz

$$a \equiv b \bmod I \quad \Leftrightarrow \quad b - a \in I \quad \Leftrightarrow \quad a + I = b + I \quad \Leftrightarrow \quad b \in a + I. \tag{11.1}$$

Ein wichtiger Speziallfall ist der Ring $R = \mathbb{Z}$ mit den Idealen der Form $I = (n) = n\mathbb{Z}$, wobei $n \in \mathbb{N}$ ist. Hier wird die Nebenklasse $a + n\mathbb{Z}$ einer Zahl $a \in \mathbb{Z}$ häufig nur mit $\bar{a}$ bezeichnet. Ein Problem bei dieser Notation besteht darin, dass sie die natürliche Zahl n nicht beinhaltet; so kann $\bar{1}$ für $1 + 2\mathbb{Z}$, $1 + 3\mathbb{Z}$ oder für $1 + n\mathbb{Z}$ mit irgendeinem anderen n stehen. Bei Verwendung der Notation muss also darauf geachtet werden, dass sich das n aus dem Kontext heraus ergibt. Die Notation $a \equiv b \bmod n$ bedeutet, dass zwei Elemente $a, b \in \mathbb{Z}$ modulo dem Hauptideal (n) übereinstimmen.

Proposition 11.3 Die Menge $\mathbb{Z}/n\mathbb{Z}$ der Kongruenzklassen ist n-elementig, es gilt

$$\mathbb{Z}/n\mathbb{Z} \quad = \quad \{\bar{a} \mid a \in \mathbb{Z} \, , \; 0 \leq a < n\}.$$

Beweis: Nach Definition gilt $\mathbb{Z}/n\mathbb{Z} = \{\bar{b} \mid b \in \mathbb{Z}\}$. Ist nun $b \in \mathbb{Z}$ beliebig vorgegeben, dann erhält man nach Division mit Rest Elemente $q, a \in \mathbb{Z}$ mit $b = qn + a$ und $0 \leq a < n$. Es gilt also $b - a = nq \in (n)$, und auf Grund der Äquivalenz (11.1) folgt $\bar{a} = \bar{b}$. Dies zeigt, dass $\mathbb{Z}/n\mathbb{Z}$ aus den angegebenen Klassen besteht.

Um zu sehen, dass die Klassen $\bar{a}$ mit $0 \leq a < n$ verschieden sind, seien $a_1, a_2 \in \mathbb{Z}$ mit $0 \leq a_1, a_2 < n$ und $\bar{a}_1 = \bar{a}_2$ vorgegeben. Nach (11.1) gilt dann $a_1 - a_2 \in (n)$, es existiert also ein $q \in \mathbb{Z}$ mit $a_1 - a_2 = qn$. Wegen $|a_1 - a_2| < n$ ist dies nur für $q = 0$ möglich. Es gilt somit $a_1 = a_2$. □

In der Algebra hatten wir den Begriff des Repräsentantensystems für eine Menge von Äquivalenzklassen eingeführt. Dieser Begriff lässt sich auch hier verwenden. Dem Beweis von Proposition 11.3 lässt sich entnehmen, dass für jedes $n \in \mathbb{N}$ die Menge $\{a \in \mathbb{Z} \mid 0 \leq a < n\}$ ein Repräsentantensystem von $\mathbb{Z}/n\mathbb{Z}$ ist. Das entscheidende Argument dabei war, dass für jedes $n \in \mathbb{N}$ auf dem Ring $\mathbb{Z}$ eine *Division mit Rest* durch n definiert ist. Ein solches Konzept existiert auch für Polynomringe über Körpern, und zwar auf der Basis der aus der Schulmathematik bekannten *Polynomdivision*. Wir werden später auf die Division mit Rest noch in einem allgemeineren Kontext eingehen.

Proposition 11.4 Sei K ein Körper, $R = K[x]$ und $f \in K[x]$ ein Polynom vom Grad $n \geq 1$. Dann ist die Teilmenge $S = \{g \in K[x] \mid g \neq 0, \text{grad}(g) < n\} \cup \{0\}$ von $K[x]$ ein Repräsentantensystem von $R/(f)$.

Beweis: Sei $\phi : S \to K[x]/(f)$ gegeben durch $g \mapsto g + (f)$. Ein Repräsentantensystem liegt vor, wenn die Abbildung ϕ bijektiv ist. Zunächst beweisen wir die Surjektivität von ϕ. Sei $\bar{g} \in K[x]/(f)$ vorgegeben und $g \in K[x]$ mit $\bar{g} = g + (f)$. Durch Division mit Rest erhalten wir Polynome $q, r \in K[x]$ mit $g = qf + r$ mit $r = 0$ oder $\text{grad}(f) < n$. Nach Definition ist r in S enthalten. Außerdem gilt $g - r \in (f)$ und somit $\phi(r) = r + (f) = g + (f) = \bar{g}$.

Seien nun $g_1, g_2 \in S$ mit $\phi(g_1) = \phi(g_2)$ vorgegeben. Dann folgt $g_1 + (f) = g_2 + (f)$, also $g_1 - g_2 \in (f)$. Es gibt also ein $q \in K[x]$ mit $g_1 - g_2 = qf$. Im Fall $q \neq 0$ wäre $g_1 - g_2 = qf$ vom Grad $\geq n$. Wegen $g_i = 0$ oder $\text{grad}(g_i) < n$ für $i = 1, 2$ ist das jedoch ausgeschlossen. Also muss $g_1 = g_2$ gelten. □

Proposition 11.5 Sei R ein Ring und I ein Ideal. Dann gibt es (eindeutig bestimmte) Verknüpfungen $+$ und $\cdot$ auf R/I mit der Eigenschaft

$$(a+I)+(b+I) = (a+b)+I \quad \text{und} \quad (a+I)\cdot(b+I) = ab+I \qquad \text{für alle} \quad a, b \in R.$$

Beweis: Nach Satz 4.25 (ii) genügt es zu zeigen, dass für alle $a_0, a, b_0, b \in I$ aus $a_0 \equiv a \bmod I$ und $b_0 \equiv b \bmod I$ jeweils $(a_0 + b_0) + I = (a + b) + I$ und $a_0 b_0 + I = ab + I$ folgt. Auf Grund der Voraussetzung gilt $i = a - a_0 \in I$ und $j = b - b_0 \in I$. Es folgt $(a + b) - (a_0 + b_0) = (a - a_0) + (b - b_0) = i + j \in I$, also $(a + b) \in (a_0 + b_0) + I$ und somit $(a + b) + I = (a_0 + b_0) + I$. Auf Grund der Rechnung

$$ab - a_0 b_0 \quad = \quad ab - ab_0 + ab_0 - a_0 b_0 \quad = \quad a(b - b_0) + (a - a_0)b_0 \quad = \quad aj + b_0 i$$

gilt ebenso $ab - a_0 b_0 \in I$, also $ab \in a_0 b_0 + I$ und somit $ab + I = a_0 b_0 + I$. □

Satz 11.6 Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist R/I mit den beiden soeben definierten Verknüpfungen ein Ring, den man als ***Faktorring*** bezeichnet. Die Abbildung $\pi_I : R \to R/I$ gegeben $a \mapsto a + I$ ist ein Epimorphismus von Ringen, der sog. ***kanonische Epimorphismus***.

Beweis: Wir verwenden die für alle $a, b \in R$ geltenden Gleichungen $(a+I)+(b+I) = (a+b)+I$ und $(a+I)\cdot(b+I) = (ab)+I$, um die Gültigkeit der Ringaxiome in R/I auf die Ringeigenschaften von R zurückzuführen. Beginnen wir mit den Axiomen der Addition. Sind $a, b, c \in R$ vorgegeben, dann gilt

$$\begin{aligned}((a+I)+(b+I))+(c+I) \quad &= \quad ((a+b)+I)+(c+I) \quad = \quad ((a+b)+c)+I \quad = \\ (a+(b+c))+I \quad &= \quad (a+I)+((b+c)+I) \quad = \quad (a+I)+((b+I)+(c+I)).\end{aligned}$$

Also ist das Assoziativgesetz in R/I erfüllt. Ferner gilt $(a+I)+(0+I) = ((a+0)+I) = a+I$ und ebenso $(0+I)+(a+I) = (0+a)+I = a+I$, somit besitzt $0+I$ in R/I die Eigenschaften des Nullelements. Aus $(a+I)+((-a)+I) = (a+(-a))+I = 0+I$ und $((-a)+I)+(a+I) = ((-a)+a)+I = 0+I$ folgt, dass die Nebenklasse $(-a)+I$ bezüglich der Addition ein zu $a+I$ inverses Element ist. Also hat jedes Element in R/I ein Negatives. Schließlich gilt wegen $(a+I)+(b+I) = (a+b)+I = (b+a)+I = (b+I)+(a+I)$ auch das Kommutativgesetz. Die Axiome der Multiplikation und das Distributivgesetz verifiziert man nach dem gleichen Schema. Die Nebenklasse $1+I$ übernimmt in R/I die Rolle des Einselements.

Zum Schluss überprüfen wir die Homomorphismus-Eigenschaft der Abbildung π_I. Sind $a, b \in R$, dann gilt $\pi_I(a+b) = (a+b)+I = (a+I)+(b+I) = \pi_I(a)+\pi_I(b)$, ebenso $\pi_I(ab) = (ab)+I = (a+I)(b+I) = \pi_I(a)\pi_I(b)$ und $\pi_I(1) = 1+I$. Offenbar ist π_I surjektiv, denn jedes Element in R/I hat die Form $a+I$ für ein $a \in R$, es liegt also wegen $\pi_I(a) = a+I$ im Bild von π_I. □

Als Beispiel betrachten wir den Ring $\mathbb{Z}/4\mathbb{Z}$. Es sei noch einmal daran erinnert, dass $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ Kurzschreibweisen für die Elemente $0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}$ sind. Die Addition und Multiplikation des Rings $\mathbb{Z}/4\mathbb{Z}$ sind durch die folgenden Verknüpfungstafeln gegeben.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Beispielsweise gilt $\bar{2}+\bar{3} = \bar{5} = \bar{1}$, wobei die Gleichung $5+4\mathbb{Z} = 1+4\mathbb{Z}$ durch $5-1 = 4 \in 4\mathbb{Z}$ zu Stande kommt. Auf dieselbe Weise überprüft man $\bar{2}\cdot\bar{3} = \bar{6} = \bar{2}$, denn es ist $6+4\mathbb{Z} = 2+4\mathbb{Z}$ wegen $6-2 = 4 \in 4\mathbb{Z}$. Man beachte, dass $\mathbb{Z}/4\mathbb{Z}$ kein Integritätsbereich ist: Es gilt $\bar{2}\cdot\bar{2} = \bar{4} = \bar{0}$, obwohl $\bar{2} \neq \bar{0}$ ist.

Neben $\{0,1,2,3\}$ ist auch $\{1,2,3,4\}$ ein Repräsentantensystem von $\mathbb{Z}/4\mathbb{Z}$. Es gilt also auch $\mathbb{Z}/4\mathbb{Z} = \{\bar{1},\bar{2},\bar{3},\bar{4}\}$. Mit dieser Darstellung der Elemente sehen die Verknüpfungstabellen folgendermaßen aus.

$+$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$

Auch hier überprüfen in jeder Tabelle exemplarisch je einen Eintrag. Es gilt $\bar{4}+\bar{3} = \bar{7} = \bar{3}$, denn wegen $7-3 = 4 \in 4\mathbb{Z}$ ist $7+4\mathbb{Z} = 3+4\mathbb{Z}$. Ebenso findet man $\bar{3}\cdot\bar{4} = \overline{12} = \bar{4}$, denn wegen $12-4 = 8 \in 4\mathbb{Z}$ ist $12+4\mathbb{Z} = 4+4\mathbb{Z}$. Man beachten, dass $\bar{4}$ das Null- und $\bar{1}$ das Einselement von $\mathbb{Z}/4\mathbb{Z} = \{\bar{1},\bar{2},\bar{3},\bar{4}\}$ ist.

Satz 11.7 Sei $n \in \mathbb{N}$. Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Beweis: „⇒“ Im Fall $n = 1$ ist $\mathbb{Z}/n\mathbb{Z}$ ein Nullring und damit kein Körper. Ist $n > 1$ keine Primzahl, dann gibt es $r, s \in \mathbb{N}$ mit $1 < r, s < n$ und $n = rs$. Es folgt dann $\bar{r}, \bar{s} \neq 0$ und $\bar{r}\bar{s} = \bar{n} = \bar{0}$. Dies zeigt, dass $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsbereich ist. Nach Lemma 9.6 ist $\mathbb{Z}/n\mathbb{Z}$ damit auch kein Körper.

„⇐“ Sei $p = n$ eine Primzahl. Dann enthält $\mathbb{Z}/p\mathbb{Z}$ jedenfalls mehr als ein Element und ist damit kein Nullring. Sei nun $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ ein Element ungleich Null und $a \in \mathbb{Z}$ mit $\bar{a} = a + p\mathbb{Z}$. Wegen $a + p\mathbb{Z} \neq \bar{0}$ ist a kein Vielfaches von p, und weil p eine Primzahl ist, muss der größte gemeinsame Teiler von a und p gleich 1 sein. Nach dem Lemma von Bézout gibt es $x, y \in \mathbb{Z}$ mit $xa + yp = 1$. Es folgt $\bar{x}\bar{a} = xa + p\mathbb{Z} = (xa + p\mathbb{Z}) + (0 + p\mathbb{Z}) = (xa + p\mathbb{Z}) + (yp + p\mathbb{Z}) = (xa + yp) + p\mathbb{Z} = 1 + p\mathbb{Z} = \bar{1}$. Also ist $\bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$ invertierbar. Somit haben wir gezeigt, dass jedes Element $\bar{a} \neq \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ ein Inverses besitzt, und folglich ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. □

Ist p eine Primzahl, dann verwendet man für den Körper $\mathbb{Z}/p\mathbb{Z}$ auch die Bezeichung $\mathbb{F}_p$.(Dabei steht der Buchstabe $\mathbb{F}$ für „field“, engl. „Körper“.)

Der euklidische Algorithmus kann verwendet werden, um die multiplikativen Inversen von Elementen der Körper $\mathbb{F}_p$ zu bestimmen. Sei beispielsweise $p = 43$ und $\bar{a} = \overline{37} \in \mathbb{F}_{43}$. Der euklidische Algorithmus liefert für die Gleichung $37x + 43y = 1$ die Lösung $x = 7$, $y = -6$. In $\mathbb{F}_{43}$ gilt also $\overline{37} \cdot \bar{7} = \bar{1}$ und $\overline{37}^{-1} = \bar{7}$.

Als weiteres Beispiel betrachten wir den Körper $\mathbb{F}_{13}$. Mit dem soeben beschriebenen Verfahren findet man hier für die Elemente $\neq \bar{0}$ die folgenden multiplikativen Inversen.

$\bar{a}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
$\bar{a}^{-1}$	$\bar{1}$	$\bar{7}$	$\bar{9}$	$\overline{10}$	$\bar{8}$	$\overline{11}$	$\bar{2}$	$\bar{5}$	$\bar{3}$	$\bar{4}$	$\bar{6}$	$\overline{12}$

Auch mit Polynomringen lassen sich Restklassenringe bilden. Sei zum Beispiel $R = \mathbb{R}[x]$ und $I = (f)$ mit $f = x^2 + 1$. Definieren wir $\mathbf{i} = x + I$, dann gilt im Ring $\mathbf{C} = R/I$ die Gleichung

$$\mathbf{i}^2 \quad = \quad \mathbf{i} \cdot \mathbf{i} \quad = \quad (x+I) \cdot (x+I) \quad = \quad x^2 + I \quad = \quad (x^2 + (-1)f) + I \quad = \quad (-1) + I \quad = \quad -1_{\mathbf{C}}$$

wobei im vierten Schritt verwendet wurde, dass $(-1)f$ im Hauptideal $I = (f)$ liegt. Es handelt sich bei $\mathbf{C}$ also um einen Ring mit einem Element $\mathbf{i}$, dessen Quadrat gleich $-1_{\mathbf{C}}$ ist. Wir werden weiter unten sehen, wie man mit Hilfe dieses Rings die komplexen Zahlen $\mathbb{C}$ konstruieren kann.

Wie in der Gruppen- gibt es auch in der Ringtheorie induzierte Homomorphismen und einen Homomorphiesatz.

Proposition 11.8 Sei $\phi : R \to R'$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal mit $I \subseteq \ker(\phi)$. Dann gibt es einen eindeutig bestimmten Homomorphismus

$$\bar{\phi} : R/I \longrightarrow R' \qquad \text{mit} \quad \bar{\phi}(a + I) = \phi(a) \quad \text{für alle} \quad a \in R.$$

Man bezeichnet ihn als den von ϕ ***induzierten*** Homomorphismus.

Beweis: Für die Existenz der Abbildung $\bar{\phi}$ genügt es nach Satz 4.25 (i) zu zeigen, dass für alle $a_0, a \in I$ aus $a_0 \equiv a \bmod I$ jeweils $\phi(a) = \phi(a_0)$ folgt. Auf Grund der Voraussetung gilt $a - a_0 \in I$ und damit auch $a - a_0 \in \ker(\phi)$. Es folgt $\phi(a) = \phi(a - a_0 + a_0) = \phi(a - a_0) + \phi(a_0) = 0_{R'} + \phi(a_0) = \phi(a_0)$.

Dass $\bar{\phi}$ ein Homomorphismus von Ringen ist, folgt unmittelbar aus der bewiesenen Gleichung und der Homomorphismus-Eigenschaft von ϕ. Zunächst gilt $\bar{\phi}(1 + I) = \phi(1) = 1_{R'}$. Seien $\bar{a}, \bar{b} \in R/I$ vorgegeben und $a, b \in R$ mit $\bar{a} = a + I$, $\bar{b} = b + I$. Dann gilt $\bar{\phi}(\bar{a} + \bar{b}) = \bar{\phi}((a + I) + (b + I)) = \bar{\phi}((a + b) + I) = \phi(a + b) = \phi(a) + \phi(b) = \bar{\phi}(a + I) + \bar{\phi}(b + I) = \bar{\phi}(\bar{a}) + \bar{\phi}(\bar{b})$. Der Beweis der Gleichung $\bar{\phi}(\bar{a}\bar{b}) = \bar{\phi}(\bar{a})\bar{\phi}(\bar{b})$ läuft analog. □

Satz 11.9 *(Homomorphiesatz für Ringe)*

Sei $\phi : R \to R'$ ein Homomorphismus von Ringen und $I = \ker(\phi)$. Dann induziert ϕ einen Isomorphismus $\bar{\phi} : R/I \xrightarrow{\sim} \mathrm{im}(\phi)$ von Ringen.

Beweis: Auf Grund der Proposition existiert ein Homomorphismus $\bar{\phi} : R/I \to R'$ mit $\bar{\phi}(a+I) = \phi(a)$ für alle $a \in R$. Insbesondere gilt $\mathrm{im}(\phi) = \mathrm{im}(\bar{\phi})$, so dass durch $\bar{\phi}$ ein surjektiver Homomorphismus auf $\mathrm{im}(\phi)$ gegeben ist. Zum Nachweis der Injektivität sei $\bar{a} \in \ker(\bar{\phi})$ vorgegeben. Ist $a \in R$ mit $a + I = \bar{a}$, dann gilt $\phi(a) = \bar{\phi}(\bar{a}) = 0_{R'}$ und somit $a \in I$. Es folgt $\bar{a} = a + I = 0 + I$. Der Kern von $\bar{\phi}$ ist somit gleich $\{0 + I\}$, und folglich ist $\bar{\phi}$ injektiv. □

Satz 11.10 *(Korrespondenzsatz für Ideale)*

Sei R ein Ring, I ein Ideal und $\pi : R \to R/I$ der kanonische Epimorphismus. Sei $\bar{\mathcal{I}}$ die Menge der Ideale von R/I und $\mathcal{I}_I$ die Menge der Ideale J von R mit $J \supseteq I$.

(i) Die Zuordnungen $\phi : \mathcal{I}_I \to \bar{\mathcal{I}}$, $J \mapsto \pi(J)$ und $\psi : \bar{\mathcal{I}} \to \mathcal{I}_I$, $\bar{J} \mapsto \pi^{-1}(J)$ sind bijektiv und zueinander invers.

(ii) Für alle Ideale $J, K \in \mathcal{I}_I$ gilt $J \subseteq K \Leftrightarrow \pi(J) \subseteq \pi(K)$.

Beweis: Weil jedes Ideal von R insbesondere eine Untergruppe der Gruppe $(R, +)$ ist, und jedes Ideal von R/I eine Untergruppe von $(R/I, +)$, folgen die Aussagen (i) und (ii) unmittelbar aus Satz 4.31, dem Korrespondenzsatz für Gruppen. □

Wir werden den Korrespondenzsatz unten zur Charakterisierung der maximalen Ideale eines Rings anhand ihrer Restklassenringe verwenden.

Lemma 11.11 Ein Ring ist genau dann ein Körper, wenn (0) und (1) die einzigen Ideale des Rings sind und $(0) \neq (1)$ gilt.

Beweis: „⇒“ Sei R ein Körper und $I \subseteq R$ ein Ideal. Im Fall $I \neq (0)$ sei $a \in I$ ein Element ungleich Null. Dann liegt auch $1 = a^{-1}a$ in I, und es folgt $I = (1)$. Auf Grund der Körpereigenschaft gilt auch $0 \neq 1$ und somit $(0) \neq (1)$.

„⇐“ Sei R ein Ring mit der Eigenschaft, dass $(0) \neq (1)$ die einzigen Ideale in R sind. Ist $a \in R$ ein beliebiges Element, dann gilt entweder $(a) = (0)$ oder $(a) = (1)$. Im ersten Fall ist $a = 0$, im zweiten liegt 1 in (a), und es gibt somit ein $r \in R$ mit $ra = 1$. Also ist a in diesem Fall eine Einheit. Wir haben somit gezeigt, dass jedes Element ungleich Null in R invertierbar ist. Dies zeigt, dass R entweder ein Nullring oder ein Körper ist. Aber wegen $(0) \neq (1)$ gilt $0 \neq 1$, und folglich ist R kein Nullring. □

Satz 11.12 Sei R ein Ring, $\mathfrak{p} \subseteq R$ ein Ideal und $\bar{R} = R/\mathfrak{p}$.

(i) Genau dann ist $\mathfrak{p}$ ein Primideal, wenn $\bar{R}$ ein Integritätsbereich ist.

(ii) Genau dann ist $\mathfrak{p}$ ein maximales Ideal, wenn $\bar{R}$ ein Körper ist.

Beweis: „⇒“ Wegen $\mathfrak{p} \neq (1)$ besteht $\bar{R}$ aus mehr als einem Element, ist also kein Nullring. Seien nun $\bar{a}, \bar{b} \in \bar{R}$ mit $\bar{a}\bar{b} = 0 + \mathfrak{p}$ vorgegeben. Sind $a, b \in R$ mit $\bar{a} = a + \mathfrak{p}$ und $\bar{b} = b + \mathfrak{p}$, dann gilt $(ab) + \mathfrak{p} = (a + \mathfrak{p})(b + \mathfrak{p}) = \bar{a}\bar{b} = 0 + \mathfrak{p}$ und folglich $ab \in \mathfrak{p}$. Aus der Primideal-Eigenschaft erhalten wir $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ und somit $\bar{a} = 0 + \mathfrak{p}$ oder $\bar{b} = 0 + \mathfrak{p}$.

„⇐“ Ist $\bar{R}$ ein Integritätsbereich, dann ist $\bar{R}$ insbesondere kein Nullring. Deshalb muss $\mathfrak{p} \neq (1)$ gelten. Seien nun $a, b \in R$ mit $ab \in \mathfrak{p}$ vorgegeben. Dann gilt $(a + \mathfrak{p})(b + \mathfrak{p}) = (ab) + \mathfrak{p} = 0 + \mathfrak{p}$. Weil $\bar{R}$ ein Integritätsbereich ist, folgt daraus $a + \mathfrak{p} = 0 + \mathfrak{p}$ oder $b + \mathfrak{p} = 0 + \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

zu (ii) Auf Grund des Korrespondenzsatzes gibt es eine Bijektion zwischen den Idealen J von R mit $\mathfrak{p} \subseteq J \subseteq (1)$ und den Idealen von $\bar{R}$. Ist $\mathfrak{p}$ ein maximales Ideal, dann ist $\mathfrak{p} \subsetneq (1)$, und für jedes Ideal J mit $\mathfrak{p} \subseteq J \subseteq (1)$ gilt $\mathfrak{p} = J$ oder $J = (1)$. Dies bedeutet, dass der Faktorring $R/\mathfrak{p}$ genau zwei Ideale besitzt, nämlich (0) oder (1). Also ist $R/\mathfrak{p}$ ein Körper. Setzen wir dies umgekehrt voraus, dann sind $(0) \neq (1)$ die einzigen beiden Ideale im Faktorring. Es gilt dann $\mathfrak{p} \subsetneq (1)$ in R, denn ansonsten gäbe es im Faktorring nur ein einziges Ideal. Zugleich ist $\mathfrak{p}$ maximal, denn jedes Ideal J mit $\mathfrak{p} \subsetneq J \subsetneq (1)$ würde ein Ideal $\bar{J}$ mit $(0) \subsetneq \bar{J} \subsetneq (1)$ im Faktorring liefern. □

Folgerung 11.13 Jedes maximale Ideal ist ein Primideal.

Beweis: Dies folgt direkt aus Satz 11.12, da jeder Körper ein Integritätsbereich ist. □

Aus den Sätzen 11.12 und 11.7 folgt zum Beispiel, dass im Ring $\mathbb{Z}$ die Hauptideale (p) von Primzahlen p alles maximale Ideale sind. Nach Folgerung 11.13 sind dies auch alles Primideale. Dass umgekehrt nicht jedes Primideal ein maximales Ideal ist, sieht man am Nullideal (0) von $\mathbb{Z}$. Wie man an Hand der Definition unmittelbar überprüft, ist (0) ein Primideal. Andererseits ist es z.B. wegen $(0) \subsetneq (2) \subsetneq (1)$ kein maximales Ideal.

Ein wesentliches Hilfmittel bei der Konstruktion von Ringen ist die Übertragung von Verknüpfungen auf andere Mengen mittels Bijektionen.

Lemma 11.14 Seien X und Y Mengen, $\phi : Y \to X$ eine Bijektion und $\cdot$ eine Verknüpfung auf X. Wir definieren auf Y eine Vernüpfung $\odot$, indem wir $a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b))$ für alle $a, b \in Y$ definieren. Die neue Verknüpfung $\odot$ hängt dann mit $\cdot$ auf folgende Weise zusammen.

(i) Ist die Verknüpfung $\cdot$ auf X assoziativ bzw. kommutativ, dann gilt dasselbe jeweils für die Verknüpfung $\odot$ auf Y.

(ii) Ist $e_X \in X$ ein Neutralelement in X bezüglich $\cdot$, dann ist $e_Y = \phi^{-1}(e_X)$ ein Neutralelement in Y bezüglich $\odot$.

(iii) Seien e_X und e_Y wie in (ii) und $a, b \in X$. Ist b ein Inverses von a bezüglich $\cdot$, dann ist $\phi^{-1}(b)$ ein Inverses von $\phi^{-1}(a)$ bezüglich $\odot$.

Man sagt, dass die Verknüpfung $\cdot$ durch die Bijektion ϕ von X auf Y ***übertragen*** wird.

Beweis: zu (i) Seien $a, b, c \in Y$ vorgegeben. Zunächst bemerken wir, dass auf Grund der Definition von ϕ jeweils $\phi(a \odot b) = \phi(a) \cdot \phi(b)$ gilt. Setzen wir nun voraus, dass die Verknüpfung $\cdot$ assoziativ ist. Dann gilt

$$\begin{aligned}\phi((a \odot b) \odot c) &= \phi(a \odot b) \cdot \phi(c) = (\phi(a) \cdot \phi(b)) \cdot \phi(c) = \phi(a) \cdot (\phi(b) \cdot \phi(c)) \\ &= \phi(a) \cdot \phi(b \odot c) = \phi(a \odot (b \odot c)).\end{aligned}$$

Auf Grund der Bijektivität von ϕ folgt daraus $(a \odot b) \odot c = a \odot (b \odot c)$. Nehmen wir nun an, dass $\cdot$ kommuativ ist. Dann gilt $\phi(a \odot b) = \phi(a) \cdot \phi(b) = \phi(b) \cdot \phi(a) = \phi(b \odot a)$, und es folgt $a \odot b = b \odot a$.

zu (ii) Sei $a \in Y$ vorgegeben. Dann gilt $\phi(e_Y \odot a) = \phi(e_Y) \cdot \phi(a) = e_X \cdot \phi(a) = \phi(a)$, weil e_X ein Neutralelement bezüglich $\cdot$ ist. Auf Grund der Bijektivität von ϕ folgt $e_Y \odot a = a$. Ebenso beweist man die Gleichung $a \odot e_Y = a$.

zu (iii) Sei $a \in X$ und $b \in X$ bezüglich der Verknüpfung $\cdot$ ein Inverses von a. Sei $c = \phi^{-1}(a)$ und $d = \phi^{-1}(b)$; zu zeigen ist $c \odot d = d \odot c = e_Y$. Nun gilt $\phi(c \odot d) = \phi(c) \cdot \phi(d) = a \cdot b = e_X = \phi(e_Y)$, und durch Anwendung von ϕ^{-1} auf beide Seiten der Gleichung erhalten wir $c \odot d = e_Y$. Genauso zeigt man $d \odot c = e_Y$. □

Aus dem Lemma ergibt sich unmittelbar, dass ϕ auch zur Übertragung einer kompletten algebraischen Struktur von X auf die Menge Y genutzt werden kann. In dieser Vorlesung sind wir vor allem an Ringstrukturen interessiert.

Satz 11.15 Sei $(R, +, \cdot)$ ein Ring, S eine Menge und $\phi : S \to R$ eine bijektive Abbildung. Seien die Verknüpfungen $\oplus$ und $\odot$ auf S definiert durch

$$a \oplus b = \phi^{-1}(\phi(a) + \phi(b)) \qquad \text{und} \qquad a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b)).$$

Dann ist $(S, \oplus, \odot)$ ein Ring, und ϕ ist ein Isomorphismus von Ringen.

Beweis: Es genügt, mit Hilfe von Lemma 11.14 die einzelnen Ringaxiome für $(S, \oplus, \odot)$ durchzugehen. Zunächst ist zu überprüfen, dass $(S, \oplus)$ eine abelsche Gruppe ist. Weil die Verknüpfung $+$ auf R assoziativ und kommutativ ist, gilt nach Lemma 11.14 dasselbe für die Verknüpfung $\oplus$ auf S. Weil 0_R in der Halbgruppe $(R, +)$ ein Neutralelement ist, handelt es sich bei $0_S = \phi^{-1}(0_R)$ nach Lemma 11.14 (ii) um ein Neutralelement in $(S, \oplus)$. Schließlich besitzt jedes Element $a \in S$ bezüglich $\oplus$ ein Inverses, nämlich nach Lemma 11.14 (iii) das Element $\phi^{-1}(-\phi(a))$. Insgesamt ist $(S, \oplus)$ also tatsächlich eine abelsche Gruppe.

Nach dem gleichen Muster zeigt man, dass $(S, \odot)$ ein abelsches Monoid ist. Das Distributivgesetz kann direkt nachgerechnet werden. Seien dazu $a, b, c \in S$ vorgegeben. Nach Definition der Verknüpfungen $\oplus$ und $\odot$ auf S gilt $\phi(r \oplus s) = \phi(r) + \phi(s)$ und $\phi(r \odot s) = \phi(r) \cdot \phi(s)$ für alle $r, s \in S$. Damit erhalten wir

$$\begin{aligned}a \odot (b \oplus c) &= \phi^{-1}(\phi(a) \cdot \phi(b \oplus c)) = \phi^{-1}(\phi(a) \cdot (\phi(b) + \phi(c))) = \phi^{-1}(\phi(a) \cdot \phi(b) + \phi(a) \cdot \phi(c)) \\ &= \phi^{-1}(\phi(a \odot b) + \phi(a \odot c)) = \phi^{-1}(\phi(a \odot b \oplus a \odot c)) = (a \odot b) \oplus (a \odot c).\end{aligned}$$ □

Das Prinzip der Übertragung von Verknüpfungen kann nun auch für die ***Konstruktion von Ringerweiterungen*** genutzt werden.

Satz 11.16 Sei $\phi : R \to S$ ein Monomorphismus von Ringen. Dann gibt es einen Erweiterungsring $\hat{R} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$.

Beweis: Allgemein gilt: Sind A, B, C, D Mengen mit $A \cap B = C \cap D = \emptyset$, und $\phi_1 : A \to C$, $\phi_2 : B \to D$ bijektive Abbildungen, dann gibt es eine eindeutig bestimmte Abbildung $\phi : A \cup B \to C \cup D$ mit $\phi|_A = \phi_1$ und $\phi|_B = \phi_2$, und diese Abbildung ist bijektiv (Beweis als Übung). Setzen wir $\hat{R} = R \cup (S \setminus \phi(R))$, und wenden wir die soeben formulierte Aussage auf $A = R$, $C = \phi(R)$ und $B = D = S \setminus \phi(R)$ an, so existiert dementsprechend eine eindeutig bestimmte bijektive Abbildung $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}|_{S\setminus\phi(R)} = \mathrm{id}_{S\setminus\phi(R)}$.

Wir nutzen diese bijektive Abbildung zur Definition von Verknüpfungen $\oplus$ und $\odot$ auf $\hat{R}$, indem wir $a \oplus b = \hat{\phi}^{-1}(\phi(a) + \phi(b))$ und $a \odot b = \hat{\phi}^{-1}(\phi(a)\phi(b))$ für alle $a, b \in \hat{R}$ setzen. Nach Satz 11.15 ist $(\hat{R}, \oplus, \odot)$ dann ein Ring, und $\hat{\phi}$ ist ein Isomorphismus von Ringen. Nach Definition gilt $\hat{\phi}|_R = \phi$, es bleibt also nur zu zeigen, dass R ein Teilring von $\hat{R}$ ist. Nach Lemma 11.14 ist wegen $\phi(1_R) = 1_S$ das Element $1_R = \phi^{-1}(1_S)$ das Einselement von $\hat{R}$, und dieses ist in R enthalten. Für alle $a, b \in R$ gilt nach Definition $a \oplus b = \hat{\phi}^{-1}(\phi(a) + \phi(b)) = \hat{\phi}^{-1}(\phi(a+b)) = \hat{\phi}^{-1}(\hat{\phi}(a+b)) = a + b$, also insbesondere $a \oplus b \in R$ für alle $a, b \in R$. Genauso sieht man, dass R auch unter der Multiplikation $\odot$ abgeschlossen ist. □

Als erste Anwendung dieses Satzes zeigen wir, wie man die komplexe Zahlen als Erweiterungskörper der reellen Zahlen konstruieren kann. Wir haben oben basierend auf dem Polynom $f = x^2 + 1 \in \mathbb{R}[x]$ den Ring $\mathbf{C} = \mathbb{R}[x]/I$ mit $I = (f)$ definiert. Die Abbildung $\phi : \mathbb{R} \to \mathbf{C}$, $a \mapsto a + I$ ist ein offenbar ein Homomorphismus von Ringen. Dieser ist injektiv, denn jedes $a \in \ker(\phi)$ mit $a + I = \phi(a) = 0$ in $I = (f)$ enthalten, also ein Vielfaches von $f = x^2 + 1$, was wegen $a \in \mathbb{R}$ nur für $a = 0$ möglich ist.

Wir können nun Satz 11.16 auf diesen Monomorphismus anwenden und erhalten einen Erweiterungsring $\mathbb{C} \supseteq \mathbb{R}$ zusammen mit einem Ringisomorphismus $\hat{\phi} : \mathbb{C} \to \mathbf{C}$, der die Bedingung $\hat{\phi}|_{\mathbb{R}} = \phi$ erfüllt. Setzen wir $i = \hat{\phi}^{-1}(\mathbf{i}) = \hat{\phi}^{-1}(x + I)$, dann gilt $\hat{\phi}(i^2) = \hat{\phi}(i)^2 = \mathbf{i}^2 = -1_{\mathbf{C}} = -\phi(1) = -\hat{\phi}(1)$, woraus auf Grund der Bijektivität $i^2 = -1$ folgt. Jedes Element $z \in \mathbb{C}$ hat darüber hinaus eine eindeutige Darstellung der Form $z = a + ib$ mit $a, b \in \mathbb{R}$. Denn wegen Proposition 11.4 besitzt die Nebenklasse $\hat{\phi}(z) \in \mathbb{R}[x]/(f)$ einen eindeutig bestimmten Repräsentanten vom Grad ≤ 1. Es gibt also eindeutig bestimmte $a, b \in \mathbb{R}$ mit $\hat{\phi}(z) = a + bx + (f) = (a + I) + (b + I) \cdot \mathbf{i}$, und durch Anwendung von $\hat{\phi}^{-1}$ erhalten wir $z = a + ib$.

Wir kommen nun zu einer weiteren wichtige Konstruktion, der Bildung der Quotientenkörper.

Definition 11.17 Sei R ein Integritätsbereich. Ein Erweiterungsring $K \supseteq R$ wird ***Quotientenkörper*** von R genannt, wenn K ein Körper ist und $K = \{ab^{-1} \mid a, b \in R\,,\ b \neq 0_R\}$ gilt.

Beispielsweise ist der Körper $\mathbb{Q}$ der rationalen Zahlen ein Quotientenkörper von $\mathbb{Z}$. Wir werden nun mit Hilfe von Satz 11.16 beweisen, dass jeder Integritätsbereich R einen Quotientenkörper besitzt. Dazu definieren wir auf der Menge $X_R = R \times (R \setminus \{0_R\})$ eine Relation $\sim$ durch die Festlegung $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ für alle $(a, b), (c, d) \in X_R$.

Lemma 11.18 Die Relation $\sim$ ist eine Äquivalenzrelation auf $R \times (R \setminus \{0_R\})$.

Beweis: Für jedes Paar $(a, b) \in X_R$ gilt $ab = ab$ und somit $(a, b) \sim (a, b)$. Deshalb ist die Relation reflexiv. Die Äquivalenz

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc \quad \Leftrightarrow \quad cb = da \quad \Leftrightarrow \quad (c, d) \sim (a, b)$$

für beliebige Paare $(a,b),(c,d) \in X_R$ zeigt, dass die Relation auch symmetrisch ist. Zum Nachweis der Transitivität seien (a,b), (c,d) und (e,f) aus X_R mit $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$ vorgegeben. Dann gilt $ad = bc$ und $cf = de$. Es folgt $adf = bcf = bde$, und mit der Kürzungsregel für Integritätsbereiche folgt $af = be$, also $(a,b) \sim (e,f)$. Dies zeigt, dass die Relation auch transitiv ist. □

Für jedes Paar $(a,b) \in X_R$ bezeichnen wir mit $[a,b]$ die zugehörige Äquivalenzklasse, und die Menge der Äquivalenzklassen mit $X_R/\sim$. Bei der Konstruktion des Quotientenkörpers orientieren wir uns nun an den herkömmlichen Regeln

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{und} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

für das Bruchrechnen.

Proposition 11.19 Auf der Menge $\hat{R} = X_R/\sim$ der Äquivalenzklassen der Relation $\sim$ auf X_R gibt es eindeutig bestimmte Verknüpfungen $\oplus$ und $\odot$ mit

$$[a,b] \oplus [c,d] = [ad+bc, bd] \qquad \text{und} \qquad [a,b] \odot [c,d] = [ac, bd]$$

für alle $(a,b),(c,d) \in X_R$, und $\hat{R}$ bildet mit diesen Verknüpfungen einen Körper.

Beweis: Die Existenz und Eindeutigkeit der Verknüpfungen wird durch Anwendung von Teil (ii) des Satzes 4.25 nachgewiesen. Demnach genügt es zu überprüfen, dass für alls (a,b), (a',b'), (c,d) und (c',d') aus $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$ jeweils $[ad+bc,bd] = [a'd'+b'c', b'd']$ und $[ac,bd] = [a'c', b'd']$ folgt. Beides ist erfüllt, denn wegen $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$ gilt $ab' = a'b$ und $cd' = c'd$, und somit auch

$$(ad+bc)(b'd') \quad = \quad ab'dd' + bb'cd' \quad = \quad a'bdd' + bb'c'd \quad = \quad (a'd'+b'c')(bd)$$

und $(ac)(b'd') = ab'cd' = a'bc'd = (a'c')(bd)$, was zu $[ad+bc,bd] = [a'd'+b'c', b'd']$ und $[ac,bd] = [a'c', b'd']$ äquivalent ist. Im nächsten Schritt zeigen wir, dass $(\hat{R}, \oplus, \odot)$ ein Ring ist, mit $0_{\hat{R}} = [0_R, 1_R]$ als Null- und $1_{\hat{R}} = [1_R, 1_R]$ als Einselement. Wir beginnen mit dem Nachweis, dass $(\hat{R}, \oplus)$ eine abelsche Gruppe ist. Seien dazu $[a,b],[c,d]$ und $[e,f]$ in $\hat{R}$ vorgegeben. Wegen $[a,b] \oplus [c,d] = [ad+bc, bd] = [cb+da, db] = [c,d] \oplus [a,b]$ ist die Verknüpfung kommutativ, und wegen

$$[a,b] \oplus ([c,d] \oplus [e,f]) \quad = \quad [a,b] \oplus [cf+de, df] \quad = \quad [adf+bcf+bde, bdf] \quad =$$
$$[ad+bc, bd] \oplus [e,f] \quad = \quad ([a,b] \oplus [c,d]) \oplus [e,f].$$

ist sie auch assoziativ. Die Rechnung $[a,b] \oplus 0_{\hat{R}} = [a,b] \oplus [0_R, 1_R] = [a \cdot 1_R + b \cdot 0_R, b \cdot 1_R] = [a,b]$ zeigt, dass $0_{\hat{R}} = [0_R, 1_R]$ tatsächlich ein Neutralelement von $(\hat{R}, \oplus)$ ist. Schließlich gilt noch $[a,b] \oplus [-a,b] = [ab + b(-a), b^2] = [0_R, b] = [0_R, 1_R] = 0_{\hat{R}}$, wobei im vorletzten Schritt verwendet wurde, dass $(0_R, b) \sim (0, 1_R)$ gilt. Also ist $[-a,b]$ in $(\hat{R}, \oplus)$ jeweils das Inverse von $[a,b]$.

Nun zeigen wir, dass $(\hat{R}, \odot)$ ein Monoid ist. Wegen $[a,b] \odot [c,d] = [ac,bd] = [ca,db] = [c,d] \odot [a,b]$ ist die Verknüpfung $\odot$ kommutativ, und die Assoziativität ergibt sich aus der Rechnung $[a,b] \odot ([c,d] \odot [e,f]) = [a,b] \odot [ce, df] = [a(ce), b(df)] = [(ac)e, (bd)f] = [ac,bd] \odot [e,f] = ([a,b] \odot [c,d]) \odot [e,f]$. Dass $1_{\hat{R}} = [1_R, 1_R]$ in $(\hat{R}, \odot)$ ein Neutralelement ist, ergibt sich aus der Rechnung $[a,b] \cdot [1_R, 1_R] = [a \cdot 1_R, b \cdot 1_R] = [a,b]$. Es fehlt noch der Nachweis des Distributivgesetzes. Dieses erhält man durch

$$[a,b] \odot ([c,d] \oplus [e,f]) \quad = \quad [a,b] \odot [cf+de, df] \quad = \quad [acf+ade, bdf] \quad =$$
$$[acbf+bdae, b^2df] \quad = \quad [ac,bd] \oplus [ae,bf] \quad = \quad [a,b] \odot [c,d] \oplus [a,b] \odot [e,f].$$

Damit ist der Beweis der Ringeigenschaften abgeschlossen. Darüber hinaus ist $(\hat{R}, \oplus, \odot)$ sogar ein Körper. Ist nämlich $\alpha = [a,b]$ ein Element von $\hat{R}$ mit $[a,b] \neq [0_R, 1_R]$, dann ist $[b,a]$ wegen $b_R \neq 0_R$ ein Kehrwert von α, denn wegen $(ab, ab) \sim (1_R, 1_R)$ gilt $[a,b] \odot [b,a] = [ab, ba] = [1_R, 1_R]$. Also sind sämtliche Elemente der Menge $\hat{R} \backslash \{0_{\hat{R}}\}$ Einheiten. Außerdem ist $\hat{R}$ kein Nullring. Denn andernfalls würde $[0_R, 1_R] = 0_{\hat{R}} = 1_{\hat{R}} = [1_R, 1_R]$ gelten, woraus $(0_R, 1_R) \sim (1_R, 1_R)$ und $0_R \cdot 1_R = 1_R \cdot 1_R$, also $0_R = 1_R$ folgen würde, im Widerspruch dazu, dass der Ring R als Integritätsbereich kein Nullring ist. □

Nach diesen Vorbereitungen können wir nun zeigen

Satz 11.20 Zu jedem Integritätsbereich existiert ein Quotientenkörper.

Beweis: Sei $(\hat{R}, \oplus, \odot)$ der in Proposition 11.19 definierte Körper. Durch die Abbildung $\phi_R : R \to \hat{R}$, $a \mapsto [a, 1_R]$ ist ein Monomorphismus von Ringen definiert. Denn es gilt $\phi_R(1_R) = [1_R, 1_R] = 1_{\hat{R}}$, und für alle $a, b \in R$ ist $\phi_R(a+b) = [a+b, 1_R] = [a, 1_R] \oplus [b, 1_R] = \phi_R(a) \oplus \phi_R(b)$ und $\phi_R(ab) = [ab, 1_R] = [a, 1_R] \odot [b, 1_R] = \phi_R(a) \odot \phi_R(b)$. Außerdem ist ϕ injektiv. Ist nämlich $a \in R$ mit $\phi_R(a) = 0_{\hat{R}}$, dann folgt $[a, 1_R] = \phi_R(a) = [0_R, 1_R]$ und somit $a \cdot 1_R = 0_R \cdot 1_R$, also $a = 0_R$. Nach Satz 11.16 existiert nun ein Erweiterungsring K von R und ein Isomorphismus $\hat{\phi}_R : K \to \hat{R}$ von Ringen mit $\hat{\phi}_R|_R = \phi_R$. Um zu zeigen, dass K nun ein Quotientenkörper von R ist, müssen wir für ein beliebig vorgegebenes Element $\alpha \in K$ zeigen, dass ein Paar $(a,b) \in X_R$ mit $\alpha = ab^{-1}$ existiert. Wegen $\hat{\phi}_R(\alpha) \in \hat{R}$ gibt es ein Paar (a,b) in X_R mit $\hat{\phi}_R(\alpha) = [a,b]$. Auf Grund der Eigenschaft $\hat{\phi}_R|_R = \phi_R$ von $\hat{\phi}_R$ erhalten wir

$$\hat{\phi}_R(\alpha) \quad = \quad [a,b] \quad = \quad [a,1_R] \odot [b,1_R]^{-1} \quad = \quad \phi_R(a)\phi_R(b)^{-1} \quad = \quad \hat{\phi}_R(a)\hat{\phi}_R(b)^{-1} \quad = \quad \hat{\phi}_R(ab^{-1})$$

wobei das Element ab^{-1} im letzten Schritt im Körper K gebildet wird. Auf Grund der Injektivität von $\hat{\phi}_R$ folgt $\alpha = ab^{-1}$, wie gewünscht. □

Durch den folgenden Satz wird präzisiert, in welchem Sinn der Quotientenkörper eines Integritätsbereichs eindeutig bestimmt ist.

Satz 11.21 Sei R ein Integritätsbereich, und seien K und L beides Quotientenkörper von R. Dann existiert ein Isomorphismus $\psi : K \to L$ von Körper mit $\psi|_R = \mathrm{id}_R$.

Beweis: Sei $\hat{R} = X_R / \sim$ der in Proposition 11.19 konstruierte Körper. Wir zeigen zunächst, dass ein Körperisomorphismus $\psi_1 : \hat{R} \to K$ existiert, der jeweils die Äquivalenzklasse $[a,b] \in \hat{R}$ auf ab^{-1} abbildet. Dazu betrachten wir die Abbildung $\hat{\psi} : X_R \to K$ gegeben durch $\hat{\psi}(a,b) = ab^{-1}$. Sind zwei Paare $(a,b), (c,d) \in X_R$ mit $(a,b) \sim (c,d)$ vorgegeben, dann gilt $ad = bc$ nach Definition der Relation $\sim$, was wegen $b, d \neq 0$ zu $ab^{-1} = cd^{-1}$ umgeformt werden kann. Es folgt $\hat{\psi}(a,b) = ab^{-1} = cd^{-1} = \hat{\psi}(c,d)$.

Teil (i) von Satz 4.25 liefert nun eine Abbildung $\psi_1 : \hat{R} \to K$ gegeben durch $\psi_1([a,b]) = \hat{\psi}(a,b) = ab^{-1}$ für alle $(a,b) \in X_R$. Wir überprüfen, dass es sich bei ψ_1 um einen Körperisomorphismus handelt. Wie wir im Beweis von Proposition 11.19 festgestellt haben, ist $[1_R, 1_R]$ das Einselement von $\hat{R}$, und es ist $\psi_1([1_R, 1_R]) = 1_R \cdot 1_R^{-1} =$

$1_R = 1_K$. Die Abbildung ψ_1 ist verträglich mit der Addition und der Multiplikation, denn für beliebig vorgegebene $[a,b],[c,d] \in \hat{R}$ gilt sowohl

$$\begin{aligned} \psi_1([a,b]+[c,d]) &= \psi_1([ad+bc,bd]) = (ad+bc)(bd)^{-1} \\ &= ab^{-1}+cd^{-1} = \psi_1([a,b])+\psi_1([c,d]) \end{aligned}$$

als auch $\psi_1([a,b]\cdot[c,d]) = \psi_1([ac,bd]) = (ac)(bd)^{-1} = (ab^{-1})(cd^{-1}) = \psi_1([a,b])\cdot\psi_1([c,d])$. Dies zeigt, dass ψ_1 jedenfalls ein Körperhomomorphismus ist, und als solcher nach Proposition 9.7 auch injektiv. Darüber hinaus ist ψ_1 auch surjektiv. Ist nämlich $\alpha \in K$ vorgegeben, dann existieren $a,b \in R$ mit $b \neq 0_R$ und $\alpha = ab^{-1}$, da K ein Quotientenkörper von R ist. Es folgt dann $[a,b] \in \hat{R}$ und $\psi_1([a,b]) = ab^{-1} = \alpha$.

Genauso sieht man nun, dass auch ein Körperisomorphismus $\psi_2 : \hat{R} \to L$ existiert. Folglich ist durch $\psi = \psi_2 \circ \psi_1^{-1}$ ein Isomorphismus $K \to L$ definiert. Dieser erfüllt auch die Bedingung $\psi|_R = \mathrm{id}_R$, denn für alle $a \in R$ ist $\psi(a) = (\psi_2 \circ \psi_1^{-1})(a) = (\psi_2 \circ \psi_1^{-1})(a \cdot 1_R^{-1}) = \psi_2([a,1_R]) = a \cdot 1_R^{-1} = a = \mathrm{id}_R$. □

Kommen wir nun zum zweiten Thema dieses Kapitels, den Polynomringen. Die folgende Definition ist bereits aus der Linearen Algebra bekannt.

Definition 11.22 Sei R ein Ring. Ein Erweiterungsring S von R wird ***Polynomring*** über R genannt, wenn es ein ausgezeichnetes Element $x \in S$ gibt mit der Eigenschaft, dass für jedes Element $f \in R[x]\setminus\{0_R\}$ ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0,\ldots,a_n \in R$ existieren, so dass $a_n \neq 0$ ist und f in der Form

$$f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad \text{dargestellt werden kann.}$$

Das ausgezeichnete Elemente x nennt man die ***Variable*** (oder Unbestimmte) des Polynomrings. Für einen Polynomring S über einem Ring R mit der Variablen x wird in der Regel die Bezeichnung $R[x]$ verwendet. Die Elemente von $R[x]$ heißen ***Polynome*** übe dem Ring R. Man bezeichnet die Zahl n in der Definition als den Grad $\mathrm{grad}(f)$ des Polynoms f. Das Polynom $a_n x^n$ ist der ***Leitterm***, das Element $a_n \in R$ der ***Leitkoeffizient*** von f.

Es sei ausdrücklich darauf hingewiesen, dass das Element x im Polynomring $R[x]$ kein Element von R ist, sofern es sich bei R nicht um einen Nullring handelt. Wäre $x = 0_R$, dann würde $1_R = x + 1_R$ gelten, was im Widerspruch dazu steht, dass jedes Element von $R[x]$ ungleich Null *genau eine* Darstellung als Polynomausdruck besitzt. Im Fall $x \in R\setminus\{0_R\}$ erhalten wir ebenfalls einen Widerspruch zu dieser Eindeutigkeit, denn dann könnte x sowohl als Polynom vom Grad 0 (mit $a_0 = x$) als auch als Polynom vom Grad 1 aufgefasst werden (in der Form $1_R \cdot x + 0_R$, also mit $a_0 = 0_R$ und $a_1 = 1_R$).

Für die folgenden Ausführungen ist es wichtig, sich noch einmal ins Gedächtnis zu rufen, wie Polynome addiert und multipliziert werden. Seien $f,g \in R[x]$ mit $f = \sum_{k=0}^{m} a_k x^k$ und $g = \sum_{\ell=0}^{n} b_\ell x^\ell$. Bei der Addition bietet es sich an, die Koeffizienten a_k und b_ℓ auch für $k > m$ und $\ell > n$ zu definieren, indem man $a_k = 0$ und $b_\ell = 0$ setzt. Die Polynome können dann in der Form

$$f = \sum_{k\in\mathbb{N}_0} a_k x^k \qquad \text{und} \qquad g = \sum_{\ell\in\mathbb{N}_0} b_\ell x^\ell$$

dargestellt werden, und die Summe hat dann die Form

$$f+g \quad = \quad \sum_{r\in\mathbb{N}_0}(a_r+b_r)x^r.$$

Das Produkt von f und g erhält man durch die Rechnung

$$fg \quad = \quad \left(\sum_{k=0}^{m}a_kx^k\right)\left(\sum_{\ell=0}^{n}b_\ell x^\ell\right) \quad = \quad \sum_{k=0}^{m}\sum_{\ell=0}^{n}a_kb_\ell x^{k+\ell} \quad = \quad \sum_{r=0}^{m+n}\left(\sum_{\substack{k,\ell\geq 0\\ k+\ell=r}}a_kb_\ell\right)x^r \quad = \quad \sum_{r=0}^{m+n}\left(\sum_{\ell=0}^{r}a_{r-\ell}b_\ell\right)x^r.$$

Wie bei den Quotientenkörpern beschäftigen wir uns zunächst mit der Frage der Eindeutigkeit.

Satz 11.23 *(universelle Eigenschaft des Polynomrings)*

Für jeden Ringhomomorphismus $\phi : R \to S$ und jedes $a \in S$ gibt es einen eindeutig bestimmten Ringhomomorphismus $\hat{\phi} : R[x] \to S$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}(x) = a$.

Beweis: Zunächst beweisen wir die *Existenz* des Homomorphismus $\hat{\phi}$. Jedes Element $0_R \neq f \in R[x]$ besitzt eine Darstellung der Form

$$f \quad = \quad \sum_{k=0}^{n}a_kx^k \qquad \text{mit} \quad n\in\mathbb{N}_0, \quad a_0,\ldots,a_n\in R \quad \text{und} \quad a_n\neq 0_R \quad ,$$

und diese ist eindeutig bestimmt. Wir definieren eine Abbildung $\hat{\phi} : R[x] \to S$, indem wir $\hat{\phi}(0_R) = 0_S$ und $\hat{\phi}(f) = \sum_{k=0}^{n}\phi(a_k)a^k$ setzen. Zu zeigen ist, dass wir auf diese Weise einen Ringhomomorphismus definiert haben. Da das Element 1_R als Polynom in $R[x]$ vom Grad Null aufgefasst werden kann, gilt zunächst $\hat{\phi}(1_R) = \phi(1_R) = 1_S$ nach Definition von $\hat{\phi}$. Seien nun $f, g \in R[x]$ vorgegeben. Ist eines dieser Elemente gleich Null, dann sind die Gleichungen $\hat{\phi}(f+g) = \hat{\phi}(f)+\hat{\phi}(g)$ und $\hat{\phi}(fg) = \hat{\phi}(f)\hat{\phi}(g)$ wegen $\hat{\phi}(0_R) = 0_S$ offensichtlich erfüllt. Wir können also $f, g \neq 0_R$ annehmen und damit voraussetzen, dass f und g Darstellungen der Form

$$f=\sum_{k=0}^{m}a_kx^k \qquad \text{und} \qquad g=\sum_{\ell=0}^{n}b_\ell x^\ell$$

besitzen, mit $m, n \in \mathbb{N}_0$, $a_k, b_\ell \in R$ und $a_m, b_n \neq 0_R$. Wie oben setzen wir $a_k = 0_R$ für $k > m$ und $b_\ell = 0$ für $\ell > n$. Auf Grund der Rechenregeln für die Addition und Multiplikation von Polynomen gilt dann

$$\hat{\phi}(f+g) \quad = \quad \hat{\phi}\left(\sum_{r\in\mathbb{N}_0}(a_r+b_r)x^r\right) \quad = \quad \sum_{r\in\mathbb{N}_0}\phi(a_r+b_r)a^r \quad = \quad \sum_{r\in\mathbb{N}_0}(\phi(a_r)+\phi(b_r))a^r$$

$$= \quad \sum_{k\in\mathbb{N}_0}\phi(a_k)a^k+\sum_{\ell\in\mathbb{N}_0}\phi(b_\ell)a^\ell \quad = \quad \hat{\phi}\left(\sum_{k\in\mathbb{N}_0}a_kx^k\right)+\hat{\phi}\left(\sum_{\ell\in\mathbb{N}_0}b_\ell x^\ell\right) \quad = \quad \hat{\phi}(f)+\hat{\phi}(g)$$

sowie

$$\hat{\phi}(fg) = \hat{\phi}\left(\sum_{r=0}^{m+n}\left(\sum_{\ell=0}^{r} a_{r-\ell}b_\ell\right)x^r\right) = \sum_{r=0}^{m+n}\left(\sum_{\ell=0}^{r}\phi(a_{r-\ell})\phi(b_\ell)\right)a^r = \left(\sum_{k=0}^{m}\phi(a_k)a^k\right)\left(\sum_{\ell=0}^{n}\phi(b_\ell)a^\ell\right) = \hat{\phi}(f)\hat{\phi}(g).$$

Für den Beweis der *Eindeutigkeit* nehmen wir an, dass neben $\hat{\phi}$ durch ψ ein weiterer Ringhomomorphismus $R[x] \to S$ mit $\psi(x) = a$ und $\psi|_R = \phi$ gegeben ist. Auf Grund der Homomorphismus-Eigenschaft gilt $\hat{\phi}(0_R) = 0_S = \psi(0_R)$. Sei nun $f \in R[x]$ ein Element mit $f \neq 0_{R[x]}$, also $f = \sum_{k=0}^{n} a_k x^k$ mit $a_0, \ldots, a_n \in R$ und $a_n \neq 0_R$. Es gilt dann

$$\hat{\phi}(f) = \hat{\phi}\left(\sum_{k=0}^{m} a_k x^k\right) = \sum_{k=0}^{m}\hat{\phi}(a_k x^k) = \sum_{k=0}^{m}\phi(a_k)a^k = \sum_{k=0}^{m}\psi(a_k x^k) = \psi\left(\sum_{k=0}^{m} a_k x^k\right) = \psi(f).$$

Damit ist die Eindeutigkeit von $\hat{\phi}$ bewiesen. □

Ist $S = R$ oder ein Erweiterungsring von R, dann bezeichnet man den eindeutig bestimmten Homorphismus $\hat{\phi}$ aus Satz 11.23 als den ***Auswertungshomomorphismus*** an der Stelle a.

Folgerung 11.24 Je zwei Polynomringe über einem Ring R sind isomorph.

Beweis: Nehmen wir an, dass $R[x] \supseteq R$ und $\tilde{R}[y] \supseteq R$ beides Polynomringe über R sind. Nach Satz 11.23 gibt es eindeutig bestimmte Homomorphismen $\phi : R[x] \to \tilde{R}[y]$ und $\psi : \tilde{R}[y] \to R[x]$ mit $\phi|_R = \psi|_R = \mathrm{id}_R$ sowie $\phi(x) = y$ und $\psi(y) = x$. Damit ist $\psi \circ \phi$ ein Ringhomomorphismus $R[x] \to R[x]$ mit $(\psi \circ \phi)|_R = \mathrm{id}_R$ und $(\psi \circ \phi)(x) = x$. Aber auch der Homomorphismus $\mathrm{id}_{R[x]}$ besitzt diese Eigenschaft. Auf Grund der Eindeutigkeit muss also $\psi \circ \phi = \mathrm{id}_{R[x]}$ gelten. Genauso beweist man die Gleichung $\phi \circ \psi = \mathrm{id}_{\tilde{R}[y]}$. Also ist ϕ ein Isomorphismus von Ringen. □

Kommen wir nun zum Beweis der Existenz eines Polynomrings über jedem Ring R. Ein Polynom der Form $a_0 + a_1 x + \ldots + a_n x^n$ ist bestimmt durch die Folge $a_0, a_1, \ldots, a_n$ seiner Koeffizienten, also durch die Abbildung $k \mapsto a_k$ (wobei k für $k > n$ auf 0_R abgebildet wird). Diese Beobachtung führt uns auf die Idee, Polynome durch Abbildungen darzustellen.

Es sei P_R die Menge aller Abbildungen $f : \mathbb{N}_0 \to R$ mit der Eigenschaft, dass $f(k) = 0_R$ für alle bis auf endlich viele $k \in \mathbb{N}_0$ gilt. Zur Definition geeigneter Verknüpfungen orientieren wir uns an den Rechenregeln zur Addition und Multiplikation von Polynomen. Dementsprechend definieren wir auf P_R zwei Verknüpfungen $\oplus$ und $\odot$ durch

$$(f \oplus g)(n) = f(n) + g(n) \qquad \text{und} \qquad (f \odot g)(n) = \sum_{k=0}^{n} f(n-k)g(k) = \sum_{k+\ell=n} f(\ell)g(k).$$

Für jedes $a \in R$ sei $\tilde{a} \in P_R$ das Element gegeben durch $\tilde{a}(0) = a$ und $\tilde{a}(n) = 0_R$ für alle $n \geq 1$. Diese Elemente sollen den konstanten Polynomen $a \in R$ entsprechen. Außerdem definieren wir ein Element $\tilde{x} \in P_R$ durch $\tilde{x}(1) = 1_R$ und $\tilde{x}(n) = 0_R$ für $n \neq 1$. Dieses Element übernimmt die Rolle der Variablen x im Polynomring $R[x]$.

Lemma 11.25 Das Tripel $(P_R, \oplus, \odot)$ ist ein Ring, mit $\tilde{0}$ als Null- und $\tilde{1}$ als Einselement.

Beweis: Zunächst überprüfen wir, dass $(P_R, \oplus)$ eine abelsche Gruppe ist. Seien $f, g, h \in P_R$ vorgegeben. Es gilt

$$((f \oplus g) \oplus h)(n) = (f \oplus g)(n) + h(n) = (f(n) + g(n)) + h(n) = f(n) + (g(n) + h(n)) =$$
$$f(n) + (g \oplus h)(n) = (f \oplus (g \oplus h))(n)$$

für jedes $n \in \mathbb{N}_0$ und somit $(f \oplus g) \oplus h = f \oplus (g \oplus h)$ für alle $f, g, h \in P_R$. Ebenso gilt $(f \oplus g)(n) = f(n) + g(n) = g(n) + f(n) = (g \oplus f)(n)$ für alle $n \in \mathbb{N}_0$ und somit $f \oplus g = g \oplus f$.

Für jedes $n \in \mathbb{N}_0$ gilt $(f \oplus \tilde{0})(n) = f(n) + \tilde{0}(n) = f(n) + 0_R = f(n)$, also $f \oplus \tilde{0} = f$. Sei nun die Abbildung $(-f) : \mathbb{N}_0 \to R$ definiert durch $(-f)(n) = -f(n)$ für alle $n \in \mathbb{N}_0$. Dann gilt $-f \in P_R$, und für alle $n \in \mathbb{N}_0$ ist $(f \oplus (-f))(n) = f(n) + (-f)(n) = f_n + (-f(n)) = 0_R = \tilde{0}(n)$. Wir erhalten $f \oplus (-f) = \tilde{0}$. Insgesamt ist $(P_R, \oplus)$ also tatsächlich eine abelsche Gruppe.

Als nächstes beweisen wir für die Verknüpfung $\odot$ das Assoziativgesetz. Seien dazu $f, g, h \in P_R$ vorgegeben. Für alle $n \in \mathbb{N}_0$ gilt

$$\begin{aligned}((f \odot g) \odot h)(n) &= \sum_{k+\ell=n} (f \odot g)(k) h(\ell) = \sum_{k+\ell=n} \left(\sum_{i+j=k} f(i) g(j) \right) h(\ell) = \\ &\sum_{k+\ell=n} \sum_{i+j=k} f(i) g(j) h(\ell) = \sum_{i+j+\ell=n} f(i) g(j) h(\ell).\end{aligned}$$

Ebenso erhalten wir

$$\begin{aligned}(f \odot (g \odot h))(n) &= \sum_{i+k=n} f(i)(g \odot h)(k) = \sum_{i+k=n} f(i) \left(\sum_{j+\ell=k} g(j) h(\ell) \right) = \\ &\sum_{i+k=n} \sum_{j+\ell=k} f(i) g(j) h(\ell) = \sum_{i+j+k=n} f(i) g(j) h(\ell).\end{aligned}$$

Insgesamt gilt also $(f \odot g) \odot h = f \odot (g \odot h)$. Nun überprüfen wir, dass $\tilde{1}$ in $(P_R, \odot)$ das Neutralelement ist. Wegen $\tilde{1}(k) = 0_R$ für $k > 0$ gilt für alle $n \in \mathbb{N}_0$ jeweils

$$(f \odot \tilde{1})(n) = \sum_{k=0}^{n} f(n-k) \tilde{1}(k) = f(n-0) \cdot 1 = f(n)$$

und somit $f \odot \tilde{1} = f$. Zum Schluss müssen wir noch das Distributivgesetz überprüfen. Wieder seien $f, g, h \in P_R$ vorgegeben. Für jedes $n \in \mathbb{N}_0$ gilt

$$\begin{aligned}(f \odot (g \oplus h))(n) &= \sum_{k=0}^{n} f(n-k)(g \oplus h)(k) = \sum_{k=0}^{n} f(n-k)(g(k) + h(k)) = \\ \sum_{k=0}^{n} f(n-k) g(k) + \sum_{k=0}^{n} f(n-k) h(k) &= (f \odot g)(n) + (f \odot h)(n) = ((f \odot g) \oplus (f \odot h))(n)\end{aligned}$$

also tatsächlich $f \odot (g \oplus h) = (f \odot g) \oplus (f \odot h)$. □

Lemma 11.26 Sei $a \in R$ und $m \in \mathbb{N}_0$. Dann gilt $(\tilde{a} \odot \tilde{x}^m)(m) = a$, und $(\tilde{a} \odot \tilde{x}^m)(n) = 0_R$ für alle $n \in \mathbb{N}_0 \setminus \{m\}$.

Beweis: Wir beweisen durch vollständige Induktion über $m \in \mathbb{N}_0$, dass $x^m(m) = 1_R$ und für alle $n \neq \mathbb{N}_0 \setminus \{m\}$ jeweils $\tilde{x}^m(n) = 0_R$ gilt. Für $m = 0$ ist $\tilde{x}^0 = \tilde{1}$, und es gilt $\tilde{1}(0) = 1_R$ und $\tilde{1}(n) = 0_R$ für alle $n > 0$. Sei nun $m \in \mathbb{N}_0$ vorgegeben,

und setzen wir die Aussage für dieses m voraus. Zunächst gilt

$$\tilde{x}^{m+1}(m+1) \quad = \quad (\tilde{x}^m \odot \tilde{x})(m+1) \quad = \quad \sum_{k=0}^{m+1} (\tilde{x}^m)(m+1-k)\tilde{x}(k) \quad = \quad \tilde{x}^m(m+1-1)\tilde{x}(1)$$

$$= \quad \tilde{x}^m(m)\tilde{x}(1) \quad = \quad 1_R \cdot 1_R \quad = \quad 1_R \quad ,$$

wobei wir im dritten und fünften Schritt die definierende Eigenschaft von $\tilde{x}$ und im fünften Schritt außerdem die Induktionsvoraussetzung angewendet haben. Für jedes $n \in \mathbb{N}_0 \setminus \{m+1\}$ gilt dagegen $n-1 \neq m$ und somit

$$\tilde{x}^{m+1}(n) \quad = \quad (\tilde{x}^m \odot \tilde{x})(n) \quad = \quad \sum_{k=0}^{m+1} (\tilde{x}^m)(n-k)\tilde{x}(k) \quad = \quad \tilde{x}^m(n-1)\tilde{x}(1) \quad = \quad 0_R \cdot 1_R \quad = \quad 0_R.$$

Damit ist der Induktionsbeweis abgeschlossen. Für jedes $m \in \mathbb{N}$ gilt nun außerdem

$$(\tilde{a} \odot x^m)(n) \quad = \quad \sum_{k=0}^{n} \tilde{a}(n-k)x^m(k) \quad = \quad \tilde{a}(0)x^m(n) \quad = \quad a \cdot x^m(n) \quad ,$$

also $(\tilde{a} \odot x^m)(n) = a \cdot 1_R = a$ im Fall $n = m$ und $(\tilde{a} \odot x^m)(n) = a \cdot 0_R = 0_R$ im Fall $n \neq m$. □

Lemma 11.27 Für jedes $f \in P_R \setminus \{\tilde{0}\}$ gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, a_1, ..., a_n \in R$, so dass $a_n \neq 0_R$ und

$$f \quad = \quad (\tilde{a}_n \odot \tilde{x}^n) \oplus \ ... \ \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 \qquad \text{gilt.}$$

Beweis: Zum Nachweis der *Existenz* sei $f \in P_R \setminus \{\tilde{0}\}$ vorgegeben und $n \in \mathbb{N}_0$ maximal mit der Eigenschaft $f(n) \neq 0_R$. Sei $a_k = f(k)$ für $0 \leq k \leq n$ und $g = (\tilde{a}_n \odot \tilde{x}^n) \oplus ... \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0$. Dann gilt für $0 \leq k \leq n$ jeweils

$$g(k) \quad = \quad \sum_{\ell=0}^{n} (\tilde{a}_\ell \odot \tilde{x}^\ell)(k) \quad = \quad a_k \quad = \quad f(k) \quad ,$$

wobei im zweiten Schritt Lemma 11.26 angewendet wurde. Für $k > n$ gilt $g(k) = 0_R = f(k)$, insgesamt also $f = g$. Für den Nachweis der *Eindeutigkeit* seien $m \in \mathbb{N}_0$ und $b_0, ..., b_m \in R$, so dass $b_m \neq 0_R$ und

$$f \quad = \quad (\tilde{b}_m \odot \tilde{x}^m) \oplus \ ... \ \oplus (\tilde{b}_1 \odot \tilde{x}) \oplus \tilde{b}_0 \qquad \text{erfüllt ist.}$$

Wie im letzten Absatz überprüft man, dass $f(k) = b_k$ für $0 \leq k \leq m$ und $f(k) = 0_R$ für $k > m$ gilt. Somit ist m die maximale Zahl mit der Eigenschaft $f(m) \neq 0_R$, und es folgt $m = n$. Außerdem gilt $b_k = f(k) = a_k$ für $0 \leq k \leq n$. □

Satz 11.28 Zu jedem Ring R existiert ein Polynomring über R.

Beweis: Sei $\phi : R \to P_R$ definiert durch $\phi(a) = \tilde{a}$ für alle $a \in R$. Diese Abbildung ist ein Homomorphismus von Ringen. Denn ϕ bildet 1_R auf das Einselement $\tilde{1}$ von P_R ab. Für beliebige $a, b \in R$ gilt außerdem $\phi(a+b) = \phi(a) \oplus \phi(b)$ und $\phi(ab) = \phi(a) \odot \phi(b)$. Denn es gilt $\phi(a+b)(0) = a + b = \phi(a)(0) + \phi(b)(0) = (\phi(a) \oplus \phi(b))(0)$ und $\phi(ab)(0) = ab = \phi(a)(0)\phi(b)(0) = (\phi(a) \odot \phi(b))(0)$, und für jedes $n \in \mathbb{N}$ gilt $\phi(a+b)(n) = 0_R = (\phi(a) \oplus \phi(b))(n)$ sowie

$\phi(ab)(n) = \phi(a)(n)\cdot\phi(b)(n) = (\phi(a)\odot\phi(b))(n)$. Außerdem ist ϕ injektiv. Ist nämlich $\phi(a) = \tilde{0}$ für ein $a \in R$, dann folgt $a = \tilde{a}(0) = \phi(a)(0) = \tilde{0}(0) = 0_R$.

Wir können nun Satz 11.16 auf den Monomorphismus ϕ anwenden. Wir erhalten einen Erweiterungsring von R, den wir mit $R[x]$ bezeichnen, und einen Isomorphismus $\hat{\phi} : R[x] \to P_R$ mit $\hat{\phi}|_R = \phi$. Außerdem setzen wir $x = \hat{\phi}^{-1}(\tilde{x})$. Wegen $\hat{\phi}|_R = \phi$ gilt $\hat{\phi}(a) = \phi(a) = \tilde{a}$ für alle $a \in R$. Sei nun $f \in R[x] \setminus \{0\}$ beliebig vorgegeben und $\tilde{f} = \hat{\phi}(f)$. Nach Lemma 11.27 gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, ..., a_n \in R$ mit $a_n \neq 0_R$, so dass

$$\tilde{f} \quad = \quad (\tilde{a}_n \odot \tilde{x}^n) \oplus \ ... \ \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 \qquad \text{gilt.}$$

Durch Anwendung von $\hat{\phi}^{-1}$ auf beide Seiten der Gleichung erhalten wir auf Grund der Homomorphismus-Eigenschaft die Gleichung $f = a_n x^n + ... + a_1 x + a_0$. Aus der Eindeutigkeit von n und $a_0, ..., a_n$ für das Element $\tilde{f}$ folgt auch die Eindeutigkeit für das Element f. Nehmen wir nämlich an, dass auch $f = b_m x^m + ... + b_1 x + b_0$ erfüllt ist, mit $m \in \mathbb{N}_0$ und $b_0, b_1, ..., b_m$. Dann folgt

$$(\tilde{a}_n \odot \tilde{x}^n) \oplus \ ... \ \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 \quad = \quad \hat{f} \quad = \quad \hat{\phi}(f) \quad = \quad (\tilde{b}_m \odot \tilde{x}^m) \oplus \ ... \ \oplus (\tilde{b}_1 \odot \tilde{x}) \oplus \tilde{b}_0 \quad ,$$

und die Eindeutigkeitsaussage in Lemma 11.27, angewendet auf das Element $\hat{f} \in P_R \setminus \{\tilde{0}\}$, liefert die Gleichungen $m = n$ und $a_k = b_k$ für $0 \leq k \leq n$. □

Zum Abschluss des Kapitels befassen wir uns noch mit den algebraischen Eigenschaften der Polynomringe.

Proposition 11.29 Sei R ein Ring und $R[x]$ ein Polynomring über R.

(i) Sind $0_R \neq f, g \in R[x]$ und gilt auch $f + g \neq 0_R$ und $fg \neq 0_R$, dann folgt

$$\text{grad}(f+g) \leq \max\{\text{grad}(f), \text{grad}(g)\} \quad \text{und} \quad \text{grad}(fg) \leq \text{grad}(f) + \text{grad}(g).$$

(ii) Ist R ein Integritätsbereich, dann gilt dasselbe auch für den Ring $R[x]$. In diesem Fall gilt sogar $\text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$ für alle $f, g \in R[x]$ mit $f, g \neq 0_R$.

Beweis: zu (i) Sei $m = \text{grad}(f)$ und $n = \text{grad}(g)$. Dann können wir f und g in der Form $f = \sum_{k=0}^{m} a_k x^m$ und $g = \sum_{\ell=0}^{n} b_\ell x^\ell$ darstellen, mit geeigneten $a_k, b_\ell \in R$. Wie zuvor definieren wir die Koeffizienten von a_k und b_ℓ auch für $k > m$ und $\ell > n$, indem wir sie auf Null setzen. Wie wir oben festgestellt haben, gilt $f + g = \sum_{r\in\mathbb{N}_0}(a_r + b_r)x^r$. Dabei ist $a_r + b_r \neq 0_R$ nur möglich, wenn $a_r \neq 0_R$ oder $b_r \neq 0_R$ gilt, also wenn $r \leq m$ oder $r \leq n$ ist, was mit $r \leq \max\{m, n\}$ gleichbedeutend ist. Daraus folgt $\text{grad}(f+g) \leq \max\{m,n\} = \max\{\text{grad}(f), \text{grad}(g)\}$. Ebenso zeigt die Gleichung $fg = \sum_{r=0}^{m+n}(\sum_{\ell=0}^{r} a_{r-\ell} b_\ell)x^r$, dass $\text{grad}(fg) \leq m + n = \text{grad}(f) + \text{grad}(g)$ gilt.

zu (ii) Der Koeffizient von x^{m+n} des Polynoms fg ist gegeben durch $\sum_{\ell=0}^{m+n} a_{m+n-\ell} b_\ell = a_m b_n$, denn für $\ell > n$ ist $b_\ell = 0_R$, und für $\ell < n$ ist $m + n - \ell > m$ und somit $a_{m+n-\ell} = 0_R$. Ist R ein Integritätsbereich, dann folgt aus $a_m \neq 0_R$ und $b_n \neq 0_R$ auch $a_m b_n \neq 0_R$. Inbesondere ist das Produkt zweier Polynome ungleich Null wiederum ungleich Null; außerdem ist mit R auch der Polynomring $R[x]$ kein Nullring. Dies zeigt, dass auch $R[x]$ ein Integritätsbereich ist. □

Folgerung 11.30 Sei R ein Integritätsbereich. Dann gilt $R[x]^\times = R^\times$, d.h. die Einheitengruppe des Polynomrings $R[x]$ stimmt mit der Einheitengruppe des Grundrings R überein.

Beweis: Sei $a \in R^\times$. Dann gibt es ein $b \in R$ mit $ab = 1_R = 1_{R[x]}$. Dies zeigt, dass jede Einheit in R auch eine Einheit in $R[x]$ ist. Sei nun umgekehrt f eine Einheit in $R[x]$. Dann gibt es ein Element $g \in R[x]$ mit $fg = 1_{R[x]} = 1_R$. Mit Proposition 11.29 (ii) erhalten wir $\operatorname{grad}(f) + \operatorname{grad}(g) = \operatorname{grad}(fg) = \operatorname{grad}(1_R) = 0$, und wegen $\operatorname{grad}(f), \operatorname{grad}(g) \geq 0$ folgt daraus $\operatorname{grad}(f) = \operatorname{grad}(g) = 0$. Also sind f und g beides Elemente des Grundrings R. Aus der Gleichung $fg = 1$ folgt nun, dass f in $R^\times$ enthalten ist. □

Man beachte, dass die Folgerung für Nicht-Integritätsbereiche im Allgemeinen falsch ist. Hier kann es in $R[x]^\times$ auch Elemente mit Polynomgrad ≥ 1 geben. Im Restklassenring $\mathbb{Z}/4\mathbb{Z}$ gilt beispielsweise $\bar{2} \cdot \bar{2} = \bar{0}$, das Element $\bar{2}$ ist also ein Nullteiler. Daraus folgt, dass das Polynom $f = \bar{2}x + \bar{1}$ im Polynomring $\mathbb{Z}/4\mathbb{Z}[x]$ eine Einheit ist, denn es gilt $f \cdot f = (\bar{2}x + \bar{1})(\bar{2}x + \bar{1}) = (\bar{2} \cdot \bar{2})x^2 + (\bar{2} + \bar{2})x + \bar{1} = \bar{0} \cdot x^2 + \bar{0} \cdot x + \bar{1} = \bar{1}$.

§ 12. *Euklidische Ringe, Hauptidealringe und faktorielle Ringe*

Zusammenfassung. Beim *euklidischen Algorithmus* handelt es sich um ein Verfahren, das in endlich vielen Schritten den ggT zweier Ringelemente ermittelt. Die Ringe, für die ein solches Verfahren existiert, bezeichnet man als *euklidische Ringe*. Wir werden zeigen, dass jeder euklidische Ring auch ein Hauptidealring ist.

Für den Begriff der *Primzahl* gibt es in beliebigen Integritätsbereichen zwei naheliegende Verallgemeinerungen, nämlich den Begriff des *Primelements* und den des *irreduziblen* Elements. In den *faktoriellen Ringen*, zu denen die Hauptidealringe zählen, fallen beide Begriffe zusammen. Darüber hinaus sind diese Ringe dadurch ausgezeichnet, dass für deren Elemente eine „im Wesentlichen eindeutige" Primfaktorzerlegung existiert.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Normfunktion auf $\mathbb{C}$	– Euklidische Ringe sind Hauptidealringe.
– euklidischer Ring, Höhenfunktion	– Hauptidealringe sind faktorielle Ringe.
– irreduzibles Element, Primelement	– Korrektheit des Euklidischen Algorithmus
– Repräsentantensystem der Primelemente	– Nachweis von irreduziblen Elementen mit der Normfuktion
– faktorieller Ring	– Beschreibung der Primideale und der maximalen Ideale in Hauptidealringen
	– Charakterisierung der faktoriellen Ringe

In Satz 9.17 haben wir für jedes $d \in \mathbb{Z}$ den quadratischen Zahlring $\mathbb{Z}[\sqrt{d}]$ und im Fall $d \equiv 1 \bmod 4$ auch den Ring $\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ eingeführt. Um die Teilerrelation und auch die Idealstruktur dieser Ringe zu untersuchen, wird sich die folgende Funktion als wichtiges Hilfsmittel erweisen.

Definition 12.1 Die ***Normfunktion*** $N : \mathbb{C} \to \mathbb{R}_+$ ist definiert durch

$$N(z) \quad = \quad z\bar{z} \quad = \quad |z|^2 \quad \text{für alle} \quad z \in \mathbb{C}.$$

Wie der komplexe Absolutbetrag ist auch die Normfunktion N ***multiplikativ***. Das bedeutet, dass für alle $z, w \in \mathbb{C}$ die Gleichung $N(zw) = N(z)N(w)$ erfüllt ist.

Lemma 12.2 Sei $d \in \mathbb{N}$.

(i) Ist $\alpha \in \mathbb{Z}[\sqrt{-d}]$, $\alpha = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, dann ist $N(\alpha) = a^2 + db^2 \in \mathbb{N}_0$.

(ii) Gilt $(-d) \equiv 1 \bmod 4$, $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ und ist $\alpha = \frac{1}{2}a + \frac{1}{2}b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2$, dann ist $N(\alpha) = \frac{1}{4}a^2 + \frac{1}{4}db^2 \in \mathbb{N}_0$.

Sind α, β im Fall (i) oder (ii) jeweils Elemente des Rings R und gilt $\alpha \mid \beta$, dann ist $N(\alpha)$ ein Teiler von $N(\beta)$ im Ring $\mathbb{Z}$.

Beweis: Ist $z = u + iv \in \mathbb{C}$ mit $u, v \in \mathbb{R}$, dann gilt jeweils $N(z) = z\bar{z} = (u+iv)(u-iv) = u^2 + v^2$. Wendet man dies unter (i) auf $u = a$ und $v = b\sqrt{-d}$ an, dann erhält man $N(\alpha) = a^2 + db^2$. Aus $a, b \in \mathbb{Z}$ folgt offenbar $N(\alpha) \in \mathbb{N}_0$. Ebenso erhält man mit $u = \frac{1}{2}a$ und $v = \frac{1}{2}b\sqrt{-d}$ die Gleichung in Teil (ii). Man überprüft unmittelbar, dass im Fall $a \equiv b \equiv 0 \bmod 2$ die Zahlen a^2 und b^2 durch 4 teilbar sind. Deshalb ist auch $a^2 + db^2$ ein Vielfaches von 4, und es folgt $N(\alpha) \in \mathbb{N}_0$. Im Fall $a \equiv b \equiv 1 \bmod 2$ gilt $a^2 \equiv b^2 \equiv 1 \bmod 4$. Wegen $d \equiv 3 \bmod 4$ ist dann $a^2 + db^2 \equiv 0 \bmod 4$ und somit $N(\alpha) \in \mathbb{N}_0$ in dieser Situation ebenfalls erfüllt.

Sei nun entweder $R = \mathbb{Z}[\sqrt{-d}]$ oder $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$, letzteres nur unter der Voraussetzung im $-d \equiv 1 \bmod 4$. Seien $\alpha, \beta \in R$ mit $\alpha \mid \beta$. Dann existiert ein $\gamma \in R$ mit $\beta = \gamma\alpha$. Auf Grund der Multiplikativität von N folgt $N(\beta) = N(\gamma)N(\alpha)$. Also ist $N(\alpha)$ ein Teiler von $N(\beta)$ im Ring $\mathbb{Z}$. □

Wir führen einen neuen Ringtyp ein, der dadurch gekennzeichnet ist, dass in ihm eine „Division mit Rest“ ausgeführt werden kann (und sinnvoll definiert ist). Wie wir sehen werden, hat dies unter anderem zur Folge, dass je zwei Ringelemente a, b einen ggT besitzen, sofern sie nicht beide Null sind.

Definition 12.3 Eine ***Höhenfunktion*** auf einem Integritätsbereich R ist eine Abbildung $h : R \setminus \{0_R\} \to \mathbb{N}$ mit der folgenden Eigenschaft: Sind $a, b \in R$, $b \neq 0_R$, dann gibt es Elemente $q, r \in R$, so dass die Gleichung $a = qb + r$ erfüllt ist und außerdem entweder $r = 0_R$ oder $h(r) < h(b)$ gilt. Ein ***euklidischer Ring*** ist ein Integritätsbereich, auf dem eine Höhenfunktion existiert.

Gelegentlich bietet es sich an, für die Höhenfunktion eine Abbildung $R \setminus \{0_R\} \to \mathbb{N}_0$, also mit Wertebereich $\mathbb{N}_0$ statt $\mathbb{N}$ zu verwenden. Der Begriff des euklidischen Rings ändert sich dadurch nicht. Ist nämlich h eine Höhenfunktion mit Wertebereich $\mathbb{N}_0$, dann ist durch $\tilde{h}(a) = h(a) + 1$ eine Höhenfunktion mit Wertebereich $\mathbb{N}$ definiert.

Wir werden nun drei konkrete Beispiele für euklidische Ringe angeben. Im Hinblick auf das erste Beispiel erinnern wir an die Definition der untern Gaußklammer: Nach Definition ist $\lfloor x \rfloor$ für $x \in \mathbb{R}$ jeweils die größte ganze Zahl a mit $a \leq x$. Es ist also beispielsweise $\lfloor \frac{6}{5} \rfloor = 1$ und $\lfloor -\frac{3}{2} \rfloor = -2$.

Proposition 12.4

(i) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring, denn die Abbildung $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ gegeben durch $h(a) = |a|$ ist eine Höhenfunktion auf diesem Ring.

(ii) Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein euklidischer Ring mit der Höhenfunktion gegeben durch die Gradabbildung, also $h(f) = \mathrm{grad}(f)$ für alle $f \in K[x] \setminus \{0_K\}$.

(iii) Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring, wobei eine Höhenfunktion durch die auf $\mathbb{Z}[i] \setminus \{0\}$ eingeschränkte Normfunktion gegeben ist.

Beweis: zu (i) Als Teilring des Körpers $\mathbb{Q}$ ist $\mathbb{Z}$ auf jeden Fall ein Integritätsbereich. Um zu zeigen, dass h tatsächlich eine Höhenfunktion ist, seien $a, b \in \mathbb{Z}$ mit $b \neq 0$ vorgegeben. Wir betrachten zunächst den Fall $b > 0$. Setzen wir $q = \lfloor \frac{a}{b} \rfloor$ und $r = a - qb$, dann ist die Gleichung $a = qb + r$ nach Definition erfüllt. Auf Grund der Definition der unteren Gaußklammer gilt $q \leq \frac{a}{b} < q + 1$. Multiplikation mit b liefert $qb \leq a < (q+1)b$, und durch Subtraktion von qb erhalten wir schließlich $0 \leq r < b$. Also gilt entweder $r = 0$ oder $h(r) < h(b)$.

Betrachten wir nun den Fall $b < 0$. Dann ist $b_1 = -b > 0$, und wie wir bereits gezeigt haben, gibt es $q_1, r_1 \in R$ mit $a = q_1 b_1 + r_1$ und $r_1 = 0$ oder $h(r_1) < h(b_1)$. Setzen wir $q = -q_1$ und $r = r_1$, dann gilt $a = qb + r$ und entweder $r = 0$ oder $h(r) = h(r_1) < h(b_1) = h(b)$.

zu (ii) Nach Proposition 11.29 ist mit K auch der Ring $K[x]$ ein Integritätsbereich. Sei nun $0 \neq g \in K[x]$ vorgegeben, mit $m = \text{grad}(g)$ und

$$g \quad = \quad \sum_{i=0}^{m} b_i x^i \quad , \quad b_0, ..., b_m \in R \ , \ b_m \neq 0.$$

Durch vollständige Induktion über $n \in \mathbb{N}_0$ zeigen wir: Ist $f \in K[x]$ mit $n = \text{grad}(f)$, dann gibt es ein $q \in K[x]$, so dass für $r = f - qg$ entweder $r = 0$ oder $\text{grad}(r) < m$ gilt. Im Fall $n < m$ können wir einfach $q = 0$, $r = f$ setzen, und es ist nichts zu zeigen. Sei nun $n \in \mathbb{N}_0$, $n \geq m$, und setzen wir die Aussage für die Polynomgrade $< n$ als gültig voraus. Sei f ein Polynom vom Grad n, also

$$f \quad = \quad \sum_{i=0}^{n} a_i x^i \quad \text{mit} \quad a_0, ..., a_n \in K \ , \ a_n \neq 0.$$

Setzen wir $q_0 = \frac{a_n}{b_m} x^{n-m}$, dann ist $f_0 = f - q_0 g$ ein Polynom vom Grad $< n$, und wir können die Induktionsvoraussetzung auf f_0 anwenden. Wir erhalten ein $q_1 \in K[x]$, so dass $r = f_0 - q_1 g$ entweder gleich Null oder $\text{grad}(r) < m$ erfüllt ist. Wegen $r = f - (q_0 + q_1)g$ erhalten wir durch $q = q_0 + q_1$ ein Element mit den gewünschten Eigenschaften. Insgesamt haben wir damit gezeigt: Sind $f, g \in K[x]$ mit $g \neq 0$, dann gibt es $q, r \in K[x]$ mit $f = qg + r$ und $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$.

zu (iii) Als Teilring des Körper $\mathbb{C}$ ist $\mathbb{Z}[i]$ jedenfalls ein Integritätsbereich. Für den Nachweis, dass h eine Höhenfunktion ist, seien $\alpha, \beta \in \mathbb{Z}[i]$ vorgegeben, wobei wir $\beta \neq 0$ voraussetzen. Wir müssen zeigen, dass ein $q \in \mathbb{Z}[i]$ mit $\alpha - q\beta = 0$ oder $h(\alpha - q\beta) < h(\beta)$ existiert. Sei $\alpha = a + ib$ und $\beta = c + id$ mit $a, b, c, d \in \mathbb{Z}$. Wegen $\beta \neq 0$ ist $(c, d) \neq (0, 0)$. Es gilt

$$\frac{\alpha}{\beta} \quad = \quad \frac{a+ib}{c+id} \quad = \quad \frac{(a+ib)(c-id)}{(c+id)(c-id)} \quad = \quad \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2} \quad = \quad r + is \quad ,$$

wenn wir die Zahlen $r, s \in \mathbb{Q}$ durch

$$r = \frac{ac+bd}{c^2+d^2} \qquad \text{und} \qquad s = \frac{bc-ad}{c^2+d^2}$$

definieren. Seien nun $r_0, s_0 \in \mathbb{Z}$ so gewählt, dass $|r - r_0| \leq \frac{1}{2}$ und $|s - s_0| \leq \frac{1}{2}$ gilt, und setzen wir $q = r_0 + is_0$. Dann folgt

$$h(\tfrac{\alpha}{\beta} - q) \quad = \quad (r - r_0)^2 + (s - s_0)^2 \quad \leq \quad \tfrac{1}{4} + \tfrac{1}{4} \quad = \quad \tfrac{1}{2} \quad < \quad 1.$$

Es gilt dann $\alpha - q\beta = 0$ oder zumindest $h(\alpha - q\beta) = h(\frac{\alpha}{\beta} - q)h(\beta) \leq \frac{1}{2}h(\beta) < h(\beta)$. □

Schon an dieser Stelle sei darauf hingewiesen, dass $\mathbb{Z}[\sqrt{d}]$ keineswegs für jedes $d \in \mathbb{Z}$ ein euklidischer Ring ist, ebensowenig der Ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$ im Fall $d \equiv 1 \bmod 4$. Weiter unten werden wir sehen, dass beispielsweise die Ringe $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\sqrt{-5}]$ keine euklidischen Ringe sind.

Die folgenden Regeln für die Nullstellen von Polynomen über Körpern sind im Prinzip bereits aus der Schulmathematik bekannt. Ihre Gültigkeit beruht aber letztlich darauf, dass es sich bei den Polynomringen über Körpern um euklidische Ringe handelt.

Folgerung 12.5 Sei K ein Körper und $0 \neq f \in K[x]$.

(i) Ist $a \in K$ eine Nullstelle von f, dann gilt $f = (x-a)g$ für ein Polynom $g \in K[x]$.

(ii) Ist $\text{grad}(f) = n$ mit $n \in \mathbb{N}_0$, dann hat f höchstens n Nullstellen in K.

Beweis: zu (i) Da $K[x]$ ein euklidischer Ring ist, gibt es Polynome $g, r \in K[x]$ mit $f = (x-a)g + r$ mit $r = 0$ oder $\text{grad}(r) < \text{grad}(x-a) = 1$. Es gilt also $r \in K$. Daraus folgt $r = r(a) = f(a) - (a-a)g(a) = 0 - 0 = 0$ und somit $f = (x-a)g$.

zu (ii) Diese Aussage beweisen wir durch vollständige Induktion über n. Ist $n = 0$, dann handelt es sich bei f um eine Konstante in $K^\times$, und f besitzt dann offensichtlich keine Nullstellen. Setzen wir nun die Aussage für n voraus, und sei f ein Polynom vom Grad $n+1$. Seien $a_1, ..., a_r$ die verschiedenen Nullstellen von f, wobei $r \in \mathbb{N}_0$ ist. Im Fall $r = 0$ ist die Aussage $r \leq \text{grad}(f)$ offenbar erfüllt. Andernfalls gibt es nach (i) ein Polynom $g \in K[x]$ mit $f = (x-a_1)g$, und für $2 \leq i \leq r$ ist a_i wegen $(a_i - a_1)g(a_i) = f(a_i) = 0$ und $a_i - a_1 \neq 0$ eine Nullstelle von g. Die Gleichung $f = (x-a_i)g$ zeigt, dass $\text{grad}(g) = n$ ist. Wir können also die Induktionsvoraussetzung auf g anwenden und erhalten die Abschätzung $r - 1 \leq n$. Daraus folgt $r \leq n+1$ wie gewünscht. □

In einem euklidischen Ring R kann durch wiederholte Division mit Rest ein größter gemeinsamer Teiler d zweier Ringelemente $a, b \in$R in endlich vielen Schritten ermittelt werden. Dieses Verfahren, das wir nun präzise ausformulieren werden, und dessen Korrektheit im Folgenden nachgewiesen werden soll, bezeichnet man als ***euklidischen Algorithmus***. Neben dem größten gemeinsamen Teiler dieses Verfahren Elemente $x, y \in R$ mit der Eigenschaft

$$d \quad = \quad xa + yb.$$

Aus der Existenz des Algorithmus wird sich also ergeben, dass das ***Lemma von Bézout*** aus § 7 nicht nur in $\mathbb{Z}$, sondern in beliebigen euklidischen Ringen gültig ist.

Lemma 12.6 Sei R ein Ring, und seien $a, b, q \in R$ mit $b \neq 0$. Dann gilt die Gleichung $\text{ggT}(a, b) = \text{ggT}(a - qb, b)$. Genauer ausformuliert bedeutet das: Ein Ringelement d ist genau dann ein größter gemeinsamer Teiler von a und b, wenn d ein größter gemeinsamer Teiler von $a - qb$ und b ist.

Beweis: „⇒“ Sei d ein größter gemeinsamer Teiler von a und b. Dann gibt es $c_1, c_2 \in R$ mit $a = c_1 d$ und $b = c_2 d$. Es folgt $a - qb = c_1 d - q c_2 d$, also ist d ein gemeinsamer Teiler von $a - qb$ und b. Ist $e \in R$ ein weiterer gemeinsamer Teiler dieser beiden Zahlen, dann gibt es $c_3, c_4 \in R$ mit $a - qb = c_3 e$ und $b = c_4 e$. Man erhält $a = (a - qb) + qb = c_3 e + c_4 e = (c_3 + c_4)e$. Also ist e ein gemeinsamer Teiler von a und b, und aus $d = \text{ggT}(a, b)$ folgt $e | d$. Damit ist gezeigt, dass d ein größter gemeinsamer Teiler von $a - qb$ und b ist. Die Beweisrichtung „⇐“ läuft analog. □

EUKLIDISCHER ALGORITHMUS

Eingabe: ein euklidischer Ring R mit Höhenfunktion h
Elemente $a, b \in R$ mit $b \neq 0$

Ausgabe: Elemente $d, x, y \in R$ mit $d = \mathrm{ggT}(a,b)$ und $d = xa + yb$

Ablauf: (1) definiere $(a_1, x_1, y_1) = (a, 1, 0)$ und $(a_2, x_2, y_2) = (b, 0, 1)$
(2) Sei das Tupel (a_n, x_n, y_n) bereits definiert.
Wenn $a_n = 0$ ist,
dann setze $d = a_{n-1}$, $x = x_{n-1}$, $y = y_{n-1}$ und gib d, x, y als Ergebnis aus. (STOP)
Ansonsten
bestimme $q, r \in R$ mit
$a_{n-1} = qa_n + r$ und $r = 0$ oder $h(r) < h(a_n)$.
Definere $(a_{n+1}, x_{n+1}, y_{n+1}) = (r, x_{n-1} - qx_n, y_{n-1} - qy_n)$.
Wiederhole Schritt 2.

Satz 12.7 Sei R ein euklidischer Ring mit Höhenfunktion h. Der euklidische Algorithmus hält für jedes Paar (a,b) mit $a, b \in R$ und $b \neq 0$ nach einer endlichen Zahl von Wiederholungen. Er liefert als Ausgabe tatsächlich $d = \mathrm{ggT}(a,b)$ und Ringelemente $x, y \in R$ mit $d = xa + yb$.

Beweis: Gehen wir zunächst davon aus, dass der zweite Schritt unendlich oft wiederholt wird. Dann ist das Tupel (a_n, x_n, y_n) für alle $n \in \mathbb{N}$ definiert. Nach Definition gilt für jedes $n \in \mathbb{N}$ aber jeweils $r = a_{n+1}$ und $h(a_{n+1}) = h(r) < h(a_n)$, wobei $q, r \in \mathbb{Z}$ die in Schritt 2 definierten Elemente in der Gleichung $a_{n-1} = qa_n + r$ sind. Wir erhalten also eine unendliche absteigende Folge

$$h(a_2) > h(a_3) > h(a_4) > h(a_5) > \ldots \qquad \text{von Zahlen in } \mathbb{N}_0.$$

Aber eine solche Folge existiert nicht: Eine absteigende Folge in $\mathbb{N}_0$, die bei einer Zahl $b \in \mathbb{N}_0$ beginnt, kann höchstens $b+1$ Schritte lang sein. Damit ist gezeigt, dass der euklidische Algorithmus nach einer endlichen Anzahl von Schritten abbricht.

Sei nun $(a_n, x_n, y_n) = (0, x_n, y_n)$ das letzte Tupel, das vom euklidischen Algorithmus berechnet wird. Wir beweisen durch vollständige Induktion über k, dass für $2 \leq k \leq n$ die Gleichung

$$\mathrm{ggT}(a_{k-1}, a_k) \quad = \quad \mathrm{ggT}(a,b)$$

erfüllt ist. Für $k = 2$ haben wir nach Definition $a_1 = a$ und $a_2 = b$, also ist die Gleichung $\mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a,b)$ offensichtlich erfüllt. Nehmen wir nun an, dass die Gleichung für k bereits bewiesen ist. Nach Definition gibt es ein $q \in \mathbb{Z}$ mit $a_{k-1} = qa_k + a_{k+1}$, und es folgt

$$\mathrm{ggT}(a_k, a_{k+1}) \quad = \quad \mathrm{ggT}(a_k, a_{k-1} - qa_k) \quad = \quad \mathrm{ggT}(a_k, a_{k-1}) \quad = \quad \mathrm{ggT}(a_{k-1}, a_k) \quad = \quad \mathrm{ggT}(a,b),$$

wobei wir im zweiten Schritt 12.6 und im letzten Schritt die Induktionsvoraussetzung angwendet haben. Nun beweisen wir noch durch vollständige Induktion die Gleichung

$$x_k a + y_k b = a_k \qquad \text{für} \quad 1 \leq k \leq n.$$

Es gilt $x_1 a + y_1 b = 1 \cdot a + 0 \cdot b = a = a_1$ und $x_2 a + y_2 b = 0 \cdot a + 1 \cdot b = b = a_2$. Nehmen wir nun an, dass die Gleichung für k bereits bewiesen ist. Nach Definition existiert ein q, für das die Gleichungen $a_{k+1} = a_{k-1} - q a_k$, $x_{k+1} = x_{k-1} - q x_k$ und $y_{k+1} = y_{k-1} - q y_k$ erfüllt sind. Es folgt

$$\begin{aligned} x_{k+1}a + y_{k+1}b &= (x_{k-1} - q x_k)a + (y_{k-1} - q y_k)b = (x_{k-1}a + y_{k-1}b) - q(x_k a + y_k b) \\ &= a_{k-1} - q a_k = a_{k+1}. \end{aligned}$$

Der Algorithmus liefert $d = a_{n-1}$, $x = x_{n-1}$ und $y = y_{n-1}$ als Ergebnis. Nun gilt allgemein $\mathrm{ggT}(c, 0) = c$ für jedes Ringelement c ungleich Null. Aus dem bereits Bewiesenen folgt $\mathrm{ggT}(a, b) = \mathrm{ggT}(a_{n-1}, a_n) = \mathrm{ggT}(a_{n-1}, 0) = a_{n-1} = d$ und $xa + yb = x_{n-1}a + y_{n-1}b = d$. □

Als Anwendungbeispiel berechnen wir den ggT der Zahlen $a = 16170$ und $b = 1326$.

q	a_n	x_n	y_n
–	16170	1	0
–	1326	0	1
12	258	1	−12
5	36	−5	61
7	6	36	−439
6	0	(−221)	(2695)

Wir erhalten $\mathrm{ggT}(a, b) = 6 = 36a + (-439)b$. (Die Zahlen in Klammern werden für das Ergebnis nicht mehr benötigt.)

Wie wir gesehen haben, sind auch Polynomringe über Körpern Beispiele für euklidische Ringe. Folglich kann der euklidische Algorithmus auch auf diese Ring angewendet werden. Als Beispiel berechnen wir den ggT der beiden Polynome $f = x^4 - 3x^3 - x^2 + 5x - 6$ und $g = x^3 - 3x^2 + x - 3$ in $\mathbb{Q}[x]$.

q	a_n	x_n	y_n
–	$x^4 - 3x^3 - x^2 + 5x - 6$	1	0
–	$x^3 - 3x^2 + x - 3$	0	1
x	$-2x^2 + 8x - 6$	1	$-x$
$-\frac{1}{2}x - \frac{1}{2}$	$2x - 6$	$\frac{1}{2}x + \frac{1}{2}$	$-\frac{1}{2}x^2 - \frac{1}{2}x + 1$
$-x + 1$	0	$(\frac{1}{2}x^2 + \frac{1}{2})$	$(-\frac{1}{2}x^3 + \frac{1}{2}x - 1)$

Als Ergebnis erhalten wir

$$\mathrm{ggT}(f, g) = 2x - 6 = (\tfrac{1}{2}x - \tfrac{1}{2})f + (-\tfrac{1}{2}x^2 - \tfrac{1}{2}x + 1)g.$$

Als weiteres Beispiel berechnen wir den ggT der Elemente $\alpha = 12+14i$ und $\beta = 32-6i$ im Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen. Um den Teiler q in jedem Schritt zu bestimmen, gehen wir folgendermaßen vor. Zunächst berechnen wir den Quotienten $\frac{a_{n-1}}{a_n}$ in der Form $r+si$ mit $r,s \in \mathbb{Q}$. Anschließend wählen wir $r_0, s_0 \in \mathbb{Z}$ mit $|r-r_0| \leq \frac{1}{2}$ und $|s-s_0| \leq \frac{1}{2}$ und sezten $q = r_0 + s_0 i$.

a_{n-1}/a_n	q	a_n	x_n	y_n
–	–	$12+14i$	1	0
–	–	$32-6i$	0	1
$\frac{15}{53}+\frac{26}{53}i$	0	$12+14i$	1	0
$\frac{15}{17}-\frac{26}{17}i$	$1-2i$	$-8+4i$	$-1+2i$	1
$-\frac{1}{2}-2i$	$-1-2i$	$-4+2i$	-4	$1+2i$
2	2	0	$(7+2i)$	$(-1-4i)$

Also ist $\mathrm{ggT}(\alpha,\beta) = -4+2i = (-4)\alpha + (1+2i)\beta$.

Satz 12.8 Jeder euklidische Ring R ist ein Hauptidealring.

Beweis: Sei I ein Ideal in R. Zu zeigen ist, dass es sich bei I um ein Hauptideal handelt, wozu wir $I \neq (0)$ voraussetzen können. Sei nun h eine Höhenfunktion auf R und $a \in I \setminus \{0\}$ ein Element mit $h(a) \leq h(b)$ für alle $b \in I$. Wir zeigen, dass dann $I = (a)$ gilt.

Ist $b \in I$ beliebig vorgegeben, dann liefert Division mit Rest Elemente $q, r \in R$ mit $b = qa + r$, wobei $r = 0$ oder $h(r) < h(a)$ gilt. Im ersten Fall ist b in (a) enthalten. Ansonsten ist mit $a, b \in I$ auch $r = b - qa$ ein Element aus I. Aber die Ungleichung $h(r) < h(a)$ widerspricht der Bedingung, die wir an das Element a gestellt haben. Es folgt $I \subseteq (a)$, und zusammen mit $a \in I$ erhalten wir $I = (a)$. □

Aus dem Satz folgt, dass der Ring $\mathbb{Z}$ der ganzen Zahlen ein Hauptidealring ist. Dasselbe gilt für die Polynomringe $K[x]$ über beliebigen Körpern K und für den Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen. Das folgende Beispiel zeigt, dass nicht jeder quadratische Zahlring ein Hauptidealring ist, und damit auch kein euklidischer Ring sein kann.

Proposition 12.9 Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ***kein*** Hauptidealring, denn beispielsweise ist das Ideal $\mathfrak{p} = (3, 1+2\sqrt{-5})$ kein Hauptideal.

Beweis: Um zu sehen, dass $\mathfrak{p}$ kein Hauptideal ist, verwenden wir die oben eingeführte Normfunktion N. Nehmen wir an, dass $\mathfrak{p}$ ein Hauptideal ist. Dann gibt es ein $\alpha \in R$ mit $\mathfrak{p} = (\alpha)$. Da die Elemente 3 und $1+2\sqrt{-5}$ in $\mathfrak{p}$ liegen, gibt es $\beta, \gamma \in R$ mit $3 = \alpha\beta$ und $1+2\sqrt{-5} = \alpha\gamma$. Die Multiplikativität der Normfunktion liefert $9 = N(3) = N(\alpha)N(\beta)$ und $21 = N(1+2\sqrt{-5}) = N(\alpha)N(\gamma)$. Also ist $N(\alpha)$ ein gemeinsamer Teiler von 9 und 21, damit auch ein Teiler vom $\mathrm{ggT}(9,21) = 3$. Es folgt $N(\alpha) \in \{1,3\}$.

Betrachten wir zunächst den Fall $N(\alpha) = 3$. Schreiben wir $\alpha = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$, dann gilt $a^2 + 5b^2 = N(\alpha) = 3$. Aber die Gleichung $a^2 + 5b^2 = 3$ besitzt keine Lösung mit $a, b \in \mathbb{Z}$, also ist dieser Fall ausgeschlossen.

Also gilt $N(\alpha) = 1$. Aus $a^2 + 5b^2 = 1$ folgt $b = 0$ und $a \in \{\pm 1\}$, damit $\alpha \in \{\pm 1\}$. Es folgt $\mathfrak{p} = (\alpha) = (1)$. Wir zeigen nun, dass auch dies unmöglich ist. Ein beliebiges Element ρ in $\mathfrak{p} = (3, 1 + 2\sqrt{-5})$ hat die Form $3\beta + (1 + 2\sqrt{-5})\gamma$ mit $\beta, \gamma \in R$. Schreiben wir $\beta = a + b\sqrt{-5}$ und $\gamma = c + d\sqrt{-5}$ mit $a, b, c, d \in \mathbb{Z}$, dann folgt

$$\begin{aligned} \rho &= 3(a + b\sqrt{-5}) + (1 + 2\sqrt{-5})(c + d\sqrt{-5}) = 3a + 3b\sqrt{-5} + (c - 10d) + (2c + d)\sqrt{-5} \\ &= (3a + c - 10d) + (3b + 2c + d)\sqrt{-5}. \end{aligned}$$

Addiert man die beiden Koeffizienten, dann erhält man den Wert $3a+3b+3c-9d$, ein Vielfaches von 3. Ist also $\rho \in \mathfrak{p}$, $\rho = m + n\sqrt{-5}$, dann ist $m + n$ stets durch 3 teilbar. Dies zeigt, dass beispielsweise das Element $1 = 1 + 0\sqrt{-5}$ nicht in $\mathfrak{p}$ liegt, weshalb $\mathfrak{p} \neq (1)$ gilt. Die Annahme, dass $\mathfrak{p}$ ein Hauptideal ist, hat also insgesamt zu einem Widerspruch geführt. □

Definition 12.10 Sei R ein Ring. Ein Element $p \in R$ wird ***irreduzibel*** genannt, wenn p weder eine Einheit noch Null ist und die Implikation

$$p = ab \quad \Rightarrow \quad a \in R^\times \text{ oder } b \in R^\times$$

für alle $a, b \in R$ erfüllt ist. Nichteinheiten ungleich Null, die nicht irreduzibel sind, bezeichnen wir als ***reduzible*** Ringelemente.

Definition 12.11 Sei R ein Ring. Ein Element $p \in R$ heißt ***Primelement***, wenn p weder eine Einheit noch Null ist und außerdem die Implikation

$$p \mid (ab) \quad \Rightarrow \quad p \mid a \quad \text{oder} \quad p \mid b \qquad \text{für alle } a, b \in R \text{ erfüllt ist.}$$

Der folgende Satz stellt einen Zusammenhang zwischen den beiden neuen Begriffen her.

Satz 12.12 In einem Integritätsbereich ist jedes Primelement irreduzibel.

Beweis: Sei p ein Primelement. Dann ist p jedenfalls ungleich Null und keine Einheit. Seien nun $a, b \in R$ mit $p = ab$ vorgegeben. Dann gilt insbesondere $p \mid (ab)$, und auf Grund der Primelement-Eigenschaft gilt $p \mid a$ oder $p \mid b$. Setzen wir o.B.d.A. voraus, dass $p \mid a$ der Fall ist. Dann gibt es ein $c \in R$ mit $a = cp$, und wir erhalten $p = ab = cpb$. Die Kürzungsregel liefert $cb = 1$, also ist b eine Einheit. Damit ist die Irreduzibilität von p nachgewiesen. □

In § 10 haben wir die Assoziiertheits-Relation auf den Elementen eines Rings R eingeführt: Zwei Elemente $a, b \in R$ sind assoziiert zueinander, wenn $a \mid b$ und $b \mid a$ gilt. Man überprüft leicht, dass es sich dabei um eine Äquivalenzrelation handelt, für die wir im weiteren Verlauf das Symbol $\sim$ verwenden. Wir erinnern daran, dass in einem Integritätsbereich R für zwei Elemente a, b nach Lemma 10.8 die Feststellung $a \sim b$ gleichbedeutend damit ist, dass $b = \varepsilon a$ für ein $\varepsilon \in R^\times$ erfüllt ist.

Proposition 12.13 Sei R ein Integritätsbereich, und seien $p, q \in R$ mit $p \sim q$.

(i) Ist p irreduzibel, dann gilt dasselbe für q.

(ii) Ist p ein Primelement, dann ist auch q ein Primelement.

Beweis: Nach Voraussetzung gibt es ein $\varepsilon \in R^\times$ mit $q = \varepsilon p$.

zu (i) Sei p irreduzibel. Wäre q eine Einheit, dann würde $p = \varepsilon^{-1} q$ als Produkt zweier Einheiten ebenfalls in $R^\times$ liegen. Wäre $q = 0$, dann würde auch $p = \varepsilon^{-1} 0 = 0$ folgen. Seien nun $a, b \in R$ Ringelemente mit $q = ab$. Dann folgt $p = \varepsilon^{-1} q = (\varepsilon^{-1} a) b$. Weil p irreduzibel ist, erhalten wir $\varepsilon^{-1} a \in R^\times$ oder $b \in R^\times$. Es folgt $a = \varepsilon(\varepsilon^{-1} a) \in R^\times$ oder $b \in R^\times$.

zu (ii) Sei p ein Primelement. Wie unter (i) folgt daraus zunächst, dass q dann weder eine Einheit noch Null ist. Seien nun $a, b \in R$ mit $q \mid (ab)$ vorgegeben. Dann gibt es ein $c \in R$ mit $ab = cq$. Es folgt $ab = c\varepsilon p$, also $p \mid (ab)$. Weil p ein Primelement ist, gilt $p \mid a$ oder $p \mid b$. Ohne Beschränkung der Allgemeinheit können wir $p \mid a$ annehmen. Dies bedeutet, dass ein $c' \in R$ mit $a = c' p = c' \varepsilon^{-1} q$ existiert. Daraus wiederum folgt $q \mid a$. Die Implikation $q \mid (ab) \Rightarrow q \mid a$ oder $q \mid b$ ist damit bewiesen. □

Proposition 12.14 Im Ring $\mathbb{Z}$ der ganzen Zahlen sind die irreduziblen Elemente genau die Zahlen der Form $\pm p$, wobei p die Primzahlen durchläuft.

Beweis: „⇒“ Sei p eine Primzahl. Dann gilt nach Definition $p \neq 0$. Außerdem ist p keine Einheit, denn die beiden Einheiten ± 1 im Ring $\mathbb{Z}$ sind keine Primzahlen. Wäre p nicht irreduzibel, dann gäbe es nach Definition Zahlen $r, s \in \mathbb{Z}$ mit $p = rs$, wobei r und s beides keine Einheiten, also ungleich ± 1 sind. Indem wir gegebenenfalls r durch $-r$ und s durch $-s$ ersetzen, können wir $r, s \in \mathbb{N}$ annehmen. Aus $r, s > 1$ folgt dann $1 < r, s < p$. Aber dies zusammen mit der Gleichung $p = rs$ widerspricht der definierenden Eigenschaft der Primzahlen. Da sich die Eigenschaft eines Elements, irreduzibel zu sein, durch Multiplikation mit Einheiten nicht ändert, ist auch $-p$ für jede Primzahl p ein irreduzibles Element in $\mathbb{Z}$.

„⇐“ Sei umgekehrt $n \in \mathbb{Z}$ ein irreduzibles Element, und nehmen wir an, dass $\pm n$ beides keine Primzahlen sind. Da Multiplikation mit Einheiten an der Irreduzibilitäts-Eigenschaft nichts ändert, können wir $n > 0$ annehmen. Da n keine Primzahl ist, gilt entweder $n = 1$, oder es gibt $r, s \in \mathbb{N}$ mit $n = rs$ und $1 < r, s < n$. Im ersten Fall wäre n eine Einheit, was aber der Voraussetzung an n, ein irreduzibles Element zu sein, widerspricht. Im zweiten Fall haben wir n als Produkt von Nicht-Einheiten dargestellt, was ebenfalls einen Widerspruch zur Voraussetzung bedeutet. □

Wir werden im nächsten Abschnitt zeigen, dass in einer allgemeinen Klasse von Ringen, welche die Hauptidealringe umfasst, die irreduziblen Elemente genau mit den Primelementen zusammenfallen. Also sind in $\mathbb{Z}$ auch die Primelemente genau die Zahlen $\pm p$, wobei p die Primzahlen durchläuft.

In beliebigen Integritätsbereichen sind irreduzible Elemente dagegen im allgemeinen nicht prim. Um dies zu sehen, formulieren wir ein Kriterium, mit dem sich leicht feststellen lässt, ob Elemente in Ringen der Form $\mathbb{Z}[\sqrt{-d}]$ (mit $d \in \mathbb{N}$) irreduzibel sind. Wieder verwenden wir dazu die multiplikative Funktion $N : \mathbb{C} \to \mathbb{R}_+$, die auf $\mathbb{Z}[\sqrt{-d}]$ wegen $N(a + b\sqrt{-d}) = a^2 + d b^2$ für $a, b \in \mathbb{Z}$ nur die natürlichen Zahlen und Null als Werte annimmt.

Proposition 12.15 Sei $d \in \mathbb{N}$, $R = \mathbb{Z}[\sqrt{-d}]$ und $\alpha \in R$ beliebig.

(i) Das Element α ist genau dann eine Einheit in R, wenn $N(\alpha) = 1$ ist.

(ii) Ist $N(\alpha)$ eine Primzahl, dann ist α in R irreduzibel.

(iii) Gilt $N(\alpha) = p^2$ mit einer Primzahl p, und besitzt die Gleichung $a^2 + d\,b^2 = p$ keine Lösung mit $a, b \in \mathbb{Z}$, dann ist α ebenfalls ein irreduzibles Element.

Beweis: zu (i) „⇒“ Ist α eine Einheit, dann gibt es ein $\beta \in R$ mit $\alpha\beta = 1$. Auf Grund der Multiplikativität von N gilt $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Weil $N(\alpha)$ und $N(\beta)$ beides natürliche Zahlen sind, muss $N(\alpha) = N(\beta) = 1$ gelten. „⇐“ Sei $\alpha = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$. Nach Voraussetzung gilt

$$a^2 + d\,b^2 \quad = \quad N(\alpha) \quad = \quad 1.$$

Da a^2 und b^2 natürliche Zahlen sind, muss $a = 0$ oder $b = 0$ gelten, darüber hinaus $a = \pm 1$ oder $d = -1$, $b = \pm 1$. Es folgt $\alpha = \pm 1$ oder $\alpha = \pm\sqrt{-1}$, wobei letzteres nur im Fall $d = -1$ auftreten kann. Alle vier Elemente sind Einheiten in R, denn es gilt $1 \cdot 1 = 1$, $(-1)(-1) = 1$ und $\sqrt{-1} \cdot (-\sqrt{-1}) = 1$.

zu (ii) Sei $\alpha \in R$ und $p = N(\alpha)$ eine Primzahl. Dann kann α keine Einheit sein, denn nach (i) ist dafür $N(\alpha) = 1$ erforderlich. Sei nun $\alpha = \beta\gamma$ eine Zerlegung von α mit $\beta, \gamma \in R$. Dann folgt $p = N(\alpha) = N(\beta)N(\gamma)$. Da $N(\beta), N(\gamma)$ natürliche Zahlen und p eine Primzahl ist, folgt $N(\beta) = 1$ oder $N(\gamma) = 1$. Nach (i) ist damit β oder γ eine Einheit. Damit ist die Irreduzibilität von α bewiesen.

zu (iii) Nehmen wir an, dass $\alpha \in R$ die angegebenen Voraussetzungen erfüllt, aber nicht irreduzibel ist. Wegen $N(\alpha) = p^2$ kann α keine Einheit sein. Ist $\alpha = \beta\gamma$ mit $\beta, \gamma \in R$, und sind β, γ beides keine Einheiten, dann ist wegen $N(\beta)N(\gamma) = p^2$ nur $N(\beta) = N(\gamma) = p$ möglich. Schreiben wir $\beta = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, dann gilt $p = N(\beta) = a^2 + d\,b^2$. Aber dies ist unmöglich, da die Gleichung nach Voraussetzung mit $a, b \in \mathbb{Z}$ nicht lösbar ist. Also ist α irreduzibel. □

Folgerung 12.16 Sei $d \in \mathbb{N}$. Für die Einheitengruppe von $R = \mathbb{Z}[\sqrt{-d}]$ gilt $R^\times = \{\pm 1, \pm\sqrt{-1}\}$, falls $d = 1$ ist, ansonsten $R^\times = \{\pm 1\}$.

Beweis: Dies ist ein Nebenergebnis des Beweises von Proposition 12.15. □

Als Anwendung der bisherigen Ergebnisse zeigen wir, dass die Elemente 2 und $1 + \sqrt{-3}$ im Ring $R = \mathbb{Z}[\sqrt{-3}]$ irreduzibel, aber keine Primelemente sind. Beide Elemente sind nach Proposition 12.15 (iii) irreduzibel, denn es gilt

$$N(2) \quad = \quad N(1 + \sqrt{-3}) \quad = \quad 4 \quad = \quad 2^2 \quad ,$$

aber die Gleichung $a^2 + 3b^2 = 2$ ist mit $a, b \in \mathbb{Z}$ nicht lösbar. Um zu zeigen, dass 2 und $1 + \sqrt{-3}$ keine Primelemente sind, betrachten wir in R die Gleichung

$$4 \quad = \quad 2 \cdot 2 \quad = \quad (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Die Zahl 2 ist ein Teiler des Produkts $(1 + \sqrt{-3})(1 - \sqrt{-3})$. Andererseits teilt 2 keine der beiden Elemente $1 \pm \sqrt{-3}$. Wäre dies der Fall, dann gäbe es ein $\gamma \in R$ mit $1 \pm \sqrt{-3} = 2\gamma$, und diese γ wäre eines der beiden Elemente $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$.

Insbesondere läge eine dieser beiden Zahlen in R. Dies würde bedeuten, dass $a, b \in \mathbb{Z}$ existieren, so dass eine der beiden Gleichungen

$$\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{-3} \quad = \quad a + b\sqrt{-3}$$

erfüllt ist. Vergleichen wir aber den Realteil auf beiden Seiten, dann erhalten wir $a = \frac{1}{2}$ im Widerspruch zu $a \in \mathbb{Z}$. Also ist 2 in R tatsächlich kein Primelement. Genauso zeigt man, dass auch das Element $1 + \sqrt{-3}$ nicht prim ist.

Die Primelemente hängen mit den bereits in § 11 definierten Primidealen eng zusammen. Es gilt nämlich

Proposition 12.17 Sei R ein Integritätsbereich und $p \in R$, $p \neq 0_R$. Genau dann ist p ein Primelement in R, wenn das Hauptideal (p) ein Primideal ist.

Beweis: „⇒“ Wäre $(p) = (1)$, dann wäre die 1 in (p) enthalten, und folglich gäbe es ein $r \in R$ mit $rp = 1$. Dies würde bedeuten, dass p eine Einheit ist, was aber nach Voraussetzung nicht der Fall ist. Seien nun $a, b \in R$ mit $ab \in (p)$. Dann gibt es ein $r \in R$ mit $ab = rp$, also ist p ein Teiler von ab. Weil p ein Primelement ist, folgt $p|a$ oder $p|b$. Im ersten Fall gilt $a \in (p)$, im zweiten $b \in (p)$.

„⇐“ Wäre p eine Einheit, dann gäbe es ein $r \in R$ mit $rp = 1$. Daraus würde dann $1 \in (p)$ und $(p) = (1)$ folgen, was aber der Voraussetzung widerspricht. Seien nun $a, b \in R$, so dass $p|(ab)$ gilt. Dann folgt $ab \in (p)$, und aus der Primidealeigenschaft von (p) folgt $a \in (p)$ oder $b \in (p)$. Im ersten Fall wäre $p|a$, im zweiten $p|b$ erfüllt. □

Satz 12.18 Sei R ein Hauptidealring, aber kein Körper, und $p \in R$. Dann sind die folgenden Aussagen äquvialent.

(i) Das Element p ist prim.

(ii) Das Element p ist irreduzibel.

(iii) Das Ideal (p) ist maximal.

(iv) Das Ideal (p) ist ein Primideal, und es gilt $p \neq 0_R$.

Beweis: „(i) ⇒ (ii)“ Nach Satz 12.12 ist jedes Primelment in einem Integritätsbereich irreduzibel.

„(ii) ⇒ (iii)“ Zunächst ist $(p) = (1)$ unmöglich, denn sonst wäre p eine Einheit und damit kein irreduzibles Element. Sei nun $\mathfrak{m}$ ein Ideal mit $(p) \subseteq \mathfrak{m} \subseteq (1)$ und $a \in R$ mit $\mathfrak{m} = (a)$. Wegen $(p) \subseteq (a)$ gilt $a|p$, es gibt also ein $b \in R$ mit $p = ab$. Weil p irreduzibel ist, muss a oder b eine Einheit sein. Im ersten Fall ist $\mathfrak{m} = (a) = (1)$, im zweiten $\mathfrak{m} = (p)$. Also ist (p) in der Tat ein maximales Ideal.

“(iii) ⇒ (iv)“ Nach Folgerung 11.13 ist jedes maximale Ideal in einem Ring ein Primideal. Nehmen wir nun an, es gilt $(p) = (0_R)$. Auf Grund der Maximalität von (p) sind dann (0_R) und (1_R) die einzigen, voneinander verschiedenen, Ideale in R. Wegen $0_R \neq 1_R$ ist R kein Nullring. Für jedes $c \in R$ mit $c \neq 0_R$ gilt aber $(c) = (1_R)$, somit $1_R \in (c)$, und daraus folgt, dass $rc = 1_R$ für ein $r \in R$ erfüllt ist. Jedes Element in R ungleich null wäre also invertierbar und R somit ein Körper. Aber das ist laut Voraussetzung ausgeschlossen.

“(iv) ⇒ (i)“ Das folgt aus Proposition 12.17. □

Definition 12.19 Ein ***faktorieller Ring*** ist ein Integritätsbereich R mit der Eigenschaft, dass jedes Element $r \in R$, das weder gleich Null noch eine Einheit ist, als Produkt von Primelementen dargestellt werden kann. Dies bedeutet: Es gibt ein $n \in \mathbb{N}$ und Primelemente $p_1, ..., p_n \in R$, so dass

$$r \quad = \quad p_1 \cdot p_2 \cdot ... \cdot p_n \qquad \text{gilt.}$$

Lemma 12.20 Sei R ein Integritätsbereich.

(i) Seien $a, a', b, b' \in R$, wobei $a \sim a'$, $b \sim b'$ und $a|b$ gilt. Dann gilt auch $a'|b'$.

(ii) Jedes Element in R, das eine Einheit teilt, ist selbst eine Einheit.

(iii) Ein Element, das von einem Primelement geteilt wird, ist keine Einheit.

Beweis: zu (i) Wegen $a \sim a'$ und $b \sim b'$ gibt es Einheiten ε, μ in R mit $a' = \varepsilon a$ und $b' = \mu b$. Aus $a|b$ folgt, dass ein $c \in R$ mit $b = ac$ existiert. Wir erhalten $b' = \mu ac = \mu\varepsilon^{-1}a'c$ und somit $a'|b'$.

zu (ii) Sei $\varepsilon \in R^\times$ und $a \in R$ mit $a|\varepsilon$. Weil die Elemente ε und 1_R assoziiert sind, gilt $a|1_R$ nach Teil (i). Umgekehrt ist 1_R das Einselement ein Teiler von a, denn es gilt $a = 1_R \cdot a$. Also sind a und 1_R assoziiert. Dies bedeutet, dass ein $\mu \in R^\times$ mit $a = \mu \cdot 1_R = \mu$ existiert.

zu (iii) Wäre $\varepsilon \in R^\times$ und p ein Primelement mit $p|\varepsilon$, dann wäre p nach (ii) eine Einheit. Ein Ringelement kann nach Definition aber nicht zugleich Einheit und Primelement sein. □

Proposition 12.21 In einem faktoriellen Ring R ist jedes irreduzible Element ein Primelement.

Beweis: Sei $p \in R$ irreduzibel. Da R faktoriell und p weder gleich Null noch eine Einheit ist, gibt es eine Darstellung $p = p_1 \cdot ... \cdot p_n$ von p als Produkt von Primlementen. Im Fall $n > 1$ könnten wir p damit als Produkt $p = p_1 \cdot (p_2 \cdot ... \cdot p_n)$ schreiben. Dabei ist p_1 eine Nicht-Einheit, ebenso das Produkt $p_2 \cdot ... \cdot p_n$ nach Teil (iii) von Lemma 12.20. Aber dies widerspricht der Irreduzibilität von p. Also ist $n = 1$ und $p = p_1$ ein Primelement. □

Satz 12.22 Sei R ein Integritätsbereich. Dann sind äquivalent

(i) R ist ein faktorieller Ring.

(ii) Jedes Element $r \in R$, dass weder gleich Null noch eine Einheit ist, kann als Produkt von irreduziblen Elementen dargestellt werden, und diese Darstellung ist im wesentlichen eindeutig. Dies bedeutet genau: Sind $m, n \in \mathbb{N}$ und $p_1 \cdot ... \cdot p_m = r = q_1 \cdot ... \cdot q_n$ zwei Darstellungen von r als Produkt irreduzibler Elemente p_i, q_j, dann ist $m = n$, und nach eventueller Umnummerierung der Elemente ist p_i assoziiert zu q_i für $1 \leq i \leq m$.

Beweis: „(ii) ⇒ (i)“ Hier genügt es zu zeigen, dass unter der gegebenen Voraussetzung jedes irreduzible Element in R ein Primelement ist. Sei $p \in R$ irreduzibel. Dann ist p weder gleich Null noch eine Einheit. Seien nun $a, b \in R$ mit $p|(ab)$ vorgegeben. Zu zeigen ist, dass p ein Teiler von a oder ein Teiler von b ist.

Nehmen wir zunächst an, dass $a = 0_R$ oder $b = 0_R$ gilt. Weil das Nullelement 0_R von jedem Ringelement geteilt wird, folgt daraus sofort $p|a$ oder $p|b$. Nehmen wir nun an, dass eines der Elemente a, b eine Einheit ist, o.B.d.A. das Element b. Dann wären a und ab assoziiert, und aus $p|(ab)$ würde nach Teil (i) von Lemma 12.20 $p|a$ folgen. Also können wir auch $a, b \notin R^\times$ annehmen. Wegen $p|(ab)$ gibt es ein $c \in R$ mit $ab = pc$. Wäre $c = 0_R$, dann würde daraus $ab = 0_R$ und somit $a = 0_R$ oder $b = 0_R$ folgen. Aber dies haben wir bereits ausgeschlossen.

Weil a und b beide weder gleich Null noch Einheiten sind, besitzen sie jeweils eine Darstellung als Produkt von irreduziblen Elementen. Seien also $p_i, q_j \in R$ irreduzible Elemente, so dass $a = p_1 \cdot \ldots \cdot p_m$ und $b = q_1 \cdot \ldots \cdot q_n$ erfüllt ist. Das Element c kann keine Einheit sein, denn sonst hätten wir eine Gleichung der Form $(p_1 \cdot \ldots \cdot p_m)(q_1 \cdot \ldots \cdot q_n) = pc$, wobei rechts ein einziges irreduzibles Element, auf der linken Seite aber ein Produkt von mindestens zwei irreduziblen Elementen steht. Dies widerspricht der vorausgesetzten Eindeutigkeit. Weil also auch c weder gleich Null noch eine Einheit ist, besitzt auch c eine Zerlegung der Form $r_1 \cdot \ldots \cdot r_k$ mit irreduziblen Elementen r_i. Wir erhalten also eine Gleichung der Form

$$(p_1 \cdot \ldots \cdot p_m) \cdot (q_1 \cdot q_n) \quad = \quad (r_1 \cdot \ldots \cdot r_k) \cdot p.$$

Auf Grund der Eindeutigkeit der Produktzerlegung ist p zu einem Faktor auf der linken Seite der Gleichung assoziiert. Gilt $p \sim p_i$ für ein $i \in \{1, \ldots, m\}$, dann ist p ein Teiler von a. Gilt $p \sim q_j$ für ein $j \in \{1, \ldots, n\}$, dann ist p ein Teiler von b.

"(i) $\Rightarrow$ (ii)" Nach Voraussetzung besitzt jede Nicht-Einheit $r \in R$, $r \neq 0_R$ eine Darstellung als Produkt von Primelementen, damit insbesondere als Produkt von irreduziblen Elementen. Zu zeigen bleibt, dass diese Produktdarstellung im Wesentlichen eindeutig ist. Seien also

$$p_1 \cdot \ldots \cdot p_m \quad = \quad r \quad = \quad q_1 \cdot \ldots \cdot q_n$$

zwei Darstellungen von r also Produkt von irreduziblen Elementen p_i, q_j. Wie wir bereits gezeigt haben, sind die p_i und q_j zugleich Primelemente. Wir beweisen nun durch vollständige Induktion über n, dass $n = m$ gilt und nach Umnummerierung p_i zu q_i assoziiert ist, für $1 \leq i \leq n$. Im Fall $n = 1$ gilt

$$p_1 \cdot \ldots \cdot p_m \quad = \quad q_1.$$

Weil q_1 irreduzibel ist, muss auch das Element auf der linken Seite der Gleichung irreduzibel sein. Dies ist nur dann der Fall, wenn $m = 1$ gilt, denn ansonsten wäre das Element links ein Produkt der beiden Nicht-Einheiten p_1 und $p_2 \cdot \ldots \cdot p_m$.

Setzen wir nun die Aussage für n als gültig voraus, und nehmen wir an, dass eine Gleichung der Form

$$p_1 \cdot \ldots \cdot p_m \quad = \quad q_1 \cdot \ldots \cdot q_n \cdot q_{n+1}$$

mit $m \in \mathbb{N}$ und irreduziblen Elementen p_i, q_j besteht (wobei diese Elemente wiederum zugleich auch prim sind). Weil das Element auf der rechten Seite der Gleichung nicht irreduzibel ist, kann auch das Element links nicht irreduzibel sein, es muss also $m \geq 2$ gelten. Wiederum teilt q_1 als Primelement einen der Faktoren p_i, zum Beispiel p_1. Es gilt also wiederum $q_1 = p_1\varepsilon$ für ein $\varepsilon \in R^\times$, und wir erhalten

$$p_1 \cdot p_2 \cdot \ldots \cdot p_m \quad = \quad (p_1\varepsilon) \cdot q_2 \cdot \ldots \cdot q_{n+1}.$$

Durch Kürzung erhalten wir $p_2 \cdot \ldots \cdot p_m = (\varepsilon q_2) \cdot \ldots \cdot q_{n+1}$. Nach Induktionsvoraussetzung gilt $m - 1 = n \Leftrightarrow m = n + 1$. Außerdem ist nach Umnummerierung das Element p_2 assoziiert zu εq_2 (also auch zu q_2), und es gilt $p_i \sim q_i$ für $3 \leq i \leq m$. □

Definition 12.23 Sei R ein Integritätsbereich und $P \subseteq R$ eine Teilmenge bestehend aus Primelementen. Wir nennen P ein ***Repräsentantensystem der Primelemente*** in R, wenn jedes Primelement $q \in R$ zu genau einem $p \in P$ assoziiert ist.

Beispielsweise bilden die Primzahlen $p \in \mathbb{N}$ ein Repräsentantensystem der Primelmente in $\mathbb{Z}$. Ist K ein Körper, dann bilden die *normierten* irreduziblen Polynome (also die irreduziblen Polynome mit dem Leitkoeffizienten 1_K) ein Repräsentantensystem in $K[x]$.

Folgerung 12.24 Sei R ein faktorieller Ring und $P \subseteq R$ ein Repräsentantensystem der Primelemente. Dann gibt es für jedes Element $0_R \neq f \in R$ eine eindeutig bestimmte Familie $(\nu_p(f))_{p\in P}$ von Zahlen $\nu_p(f) \in \mathbb{N}_0$ und eine eindeutig bestimmte Einheit $\varepsilon \in R^\times$, so dass

$$f \quad = \quad \varepsilon \prod_{p\in P} p^{\nu_p(f)} \qquad \text{erfüllt ist.}$$

Dabei gilt $\nu_p(f) = 0$ für alle bis auf endlich viele Elemente $p \in P$.

Beweis: Da R ein faktorieller Ring ist, besitzt f eine Darstellung $f = q_1 \cdot \ldots \cdot q_m$ als Produkt von Primelementen. Für jedes i gibt es ein $p_i \in P$ und eine Einheit $\varepsilon_i \in R^\times$, so dass $q_i = \varepsilon_i p_i$ gilt. Setzen wir $\varepsilon = \varepsilon_1 \cdot \ldots \cdot \varepsilon_m$, dann ist also die Gleichung $f = \varepsilon \cdot p_1 \cdot \ldots \cdot p_m$ erfüllt. Definieren wir nun für jedes $p \in P$ die Zahl $\nu_p(f) \in \mathbb{N}_0$ durch $\nu_p(f) = \big|\{i \in \{1,\ldots,m\} \;\big|\; p_i = p\}\big|$, dann ist die Gleichung $f = \varepsilon \prod_{p\in P} p^{\nu_p(f)}$ erfüllt, und für alle bis auf endlich viele $p \in P$ gilt $\nu_p(f) = 0$. Die Eindeutigkeit der Zahlen $\nu_p(f)$ folgt direkt aus der Eindeutigkeit der Zerlegung von f als Produkt irreduzibler Elemente, und mit den Zahlen $\nu_p(f)$ ist auch die Einheit ε eindeutig bestimmt. □

Für alle $a, b \in R \setminus \{0_R\}$ gilt offenbar $\nu_p(ab) = \nu_p(a) + \nu_p(b)$. Seien nämlich

$$a = \varepsilon \prod_{p\in P} p^{\nu_p(a)} \qquad \text{und} \qquad b = \varepsilon' \prod_{p\in P} p^{\nu_p(b)}$$

die Darstellungen von $a, b \in R$ wie im Satz angegeben. Dann gilt $ab = \varepsilon\varepsilon' \prod_{p\in P} p^{\nu_p(a)+\nu_p(b)}$, und aus der Eindeutigkeit der Exponenten $\nu_p(ab)$ folgt $\nu_p(ab) = \nu_p(a)+\nu_p(b)$. Die Teilbarkeitsrelation lässt sich mit Hilfe der Zahlen $\nu_p(a)$ also folgendermaßen umformulieren.

Lemma 12.25 Sei R ein faktorieller Ring, $P \subseteq R$ ein Repräsentantensystem der Primelemente, und seien $f, g \in R$ mit $f, g \neq 0_R$. Dann gilt $f \,|\, g$ genau dann, wenn $\nu_p(f) \leq \nu_p(g)$ für alle $p \in P$ erfüllt ist.

Beweis: Ist f ein Teiler von g, dann gibt es ein $h \in R, h \neq 0$ mit $g = fh$. Es folgt $\nu_p(g) = \nu_p(fh) = \nu_p(f)+\nu_p(h) \geq \nu_p(f)$ für alle $p \in P$. Gilt umgekehrt

$$f = \varepsilon \prod_{p\in P} p^{\nu_p(f)} \qquad \text{und} \qquad g = \varepsilon' \prod_{p\in P} p^{\nu_p(g)}$$

mit $\varepsilon, \varepsilon' \in R^\times$ und $\nu_p(f) \leq \nu_p(g)$ für alle $p \in P$, dann erhalten wir durch $h = \varepsilon'\varepsilon^{-1} \prod_{p\in P} p^{\nu_p(g)-\nu_p(f)}$ ein Element $h \in R$ mit $g = fh$. Es folgt $f \,|\, g$. □

Folgerung 12.26 Sei R ein faktorieller Ring, und seien $a, b \in R \setminus \{0_R\}$ teilerfremd. Ist $0_R \neq c \in R$ ein Element mit $a|(bc)$, dann folgt $a|c$.

Beweis: Nehmen wir an, dass $a \nmid c$ gilt. Dann gibt es ein Primelement $p \in P$ mit $v_p(a) > v_p(c)$. Andererseits gilt $v_p(a) \leq v_p(bc) = v_p(b) + v_p(c)$ und somit $v_p(b) > 0$. Damit wäre dann p ein Primteiler von b, was aber der Teilerfremdheit von a und b widerspricht. □

Satz 12.27 Sei R ein faktorieller Ring, und sei $P \subseteq R$ ein Repräsentantensystem der Primelemente in R. Seien $f_1, ..., f_m \in R$ beliebige Elemente ungleich Null. Für jedes $p \in P$ definieren wir

$$u_p = \min\{v_p(f_i) \mid 1 \leq i \leq m\} \qquad \text{und} \qquad w_p = \max\{v_p(f_i) \mid 1 \leq i \leq m\}.$$

Dann ist $f = \prod_{p \in P} p^{u_p}$ ein ggT und $g = \prod_{p \in P} p^{w_p}$ ein kgV der Elemente $f_1, ..., f_m$. Dies zeigt also insbesondere, dass in einem faktoriellen Ring für beliebige endliche Mengen von Elementen jeweils ein kgV und ein ggT existiert.

Beweis: Wegen $v_p(f) = u_p \leq v_p(f_i)$ für alle $p \in P$ und $1 \leq i \leq m$ ist f nach Lemma12.25 ein gemeinsamer Teiler von $f_1, ..., f_m$. Ist $h \in R$ ein weiteres Element mit $h|f_i$ für $1 \leq i \leq m$, dann folgt ebenfalls auf Grund des Lemmas jeweils $v_p(h) \leq v_p(f_i)$ für alle $p \in P$ und $1 \leq i \leq m$. Damit gilt $v_p(h) \leq u_p = v_p(f)$ für alle $p \in P$, und folglich ist h ein Teiler von f. Der entsprechende Beweis für das kgV läuft analog. □

Wir beenden den Abschnitt mit einem Satz, der die faktoriellen Ringe in die bisher definierten Ringtypen einordnet.

Satz 12.28 Jeder Hauptidealring R ist faktoriell.

Beweis: Wir wissen bereits, dass jedes irreduzible Element in einem Hauptidealring R auch ein Primelement ist, nach Proposition 12.18. Daher genügt es zu zeigen, dass für jede Nichteinheit $a \in R$, $a \neq 0_R$ eine Zerlegung in irreduzible Elemente existiert. Nehmen wir nun an, dass $a \in R$ wäre eine Nichteinheit ungleich Null, die keine solche Zerlegung besitzt. Wir zeigen, dass dann eine Folge $(a_n)_{n \in \mathbb{N}}$ von Ringelementen existiert, so dass folgende Bedingungen erfüllt sind.

(i) $a_n \neq 0_R$ und $a_n \notin R^\times$

(ii) Das Element a_n ist nicht als Produkt irreduzibler Elemente darstellbar.

(iii) $a_{n+1}|a_n$ und $a_n \nmid a_{n+1}$

Nach Voraussetzung besitzt das Element $a_1 = a$ die Eigenschaften (i) und (ii). Zu zeigen ist nun, dass für ein vorgegebenes a_n mit den Eigenschaften (i) und (ii) ein Element a_{n+1} existiert, so dass (iii) gilt und die Bedingungen (i),(ii) auch für a_{n+1} erfüllt sind. Das Element a_n ist nicht irreduzibel, weil die Irreduzibilität der Bedingung (ii) widersprechen würde. Sei $a_n = rs$ eine Darstellung von a_n als Produkt von Nicht-Einheiten. Dann ist eines der Elemente r, s

nicht als Produkt von irreduziblen Elementen darstellbar, denn ansonsten würde sich erneut ein Widerspruch zu (ii) ergeben. Wir können annehmen, dass das Element $a_{n+1} = r$ keine solche Darstellung besitzt. Wäre $a_{n+1} = 0_R$, dann würde $a_n = 0_R$ folgen, im Widerspruch zu (i). So aber sind die Bedingungen (i) und (ii) für a_{n+1} erfüllt. Offenbar gilt auch $a_{n+1}|a_n$. Würde $a_n|a_{n+1}$ gelten, dann gäbe es ein $\varepsilon \in R$ mit $a_{n+1} = \varepsilon a_n$, und aus $a_{n+1} = \varepsilon a_n = \varepsilon rs = \varepsilon a_{n+1}s$ würde mit der Kürzungsregel $\varepsilon s = 1_R$ folgen, im Widerspruch dazu, dass s keine Einheit ist. So aber ist die Bedingung (iii) für a_n und a_{n+1} erfüllt.

Sei nun $(a_n)_{n\in\mathbb{N}}$ eine Folge mit den Eigenschaften (i), (ii) und (iii). Aus der Bedingung (iii) folgt für die Hauptideale (a_n) nach Satz 10.12 (i) die Beziehung

$$(a_1) \quad \subsetneq \quad (a_2) \quad \subsetneq \quad (a_3) \quad \subsetneq \quad (a_4) \quad \subsetneq \quad \ldots$$

Wir zeigen, dass auch die Vereinigung $I = \bigcup_{n=1}^{\infty}(a_n)$ ein Ideal im Ring R ist. Wegen $0_R \in (a)$ liegt 0_R auch in I. Seien nun $a, b \in I$ und $r \in R$ vorgegeben. Dann gibt es $m, n \in \mathbb{N}$ mit $a \in (a_m)$ und $b \in (a_n)$. Setzen wir o.B.d.A. die Ungleichung $m \leq n$ voraus, dann liegen a und b wegen $(a_m) \subseteq (a_n)$ also beide in (a_n). Weil (a_n) ein Ideal ist, folgt $a + b \in (a_n)$ und $ra_n \in (a_n)$, damit auch $a + b \in I$ und $ra \in I$.

Da R nun ein Hauptidealring ist, gibt es ein $b \in R$ mit $I = (b)$. Insbesondere gilt dann $(a_n) \subseteq (b)$ für alle $n \in \mathbb{N}$. Nach Definition von I gibt es andererseits ein $m \in \mathbb{N}$ mit $b \in (a_m)$, also $b \in (a_n)$ für alle $n \geq m$. Es folgt $(b) \subseteq (a_n)$ und damit $(a_n) = (b)$ für alle $n \geq m$. Aber dies widerspricht der vorherigen Feststellung $(a_m) \subsetneq (a_{m+1})$. Die Annahme, dass es ein Element gibt, das sich nicht in irreduzible Elemente zerlegen lässt, hat also zu einem Widerspruch geführt. □

Die Umkehrung dieses Satzes ist falsch: Es gibt faktorielle Ringe, die keine Hauptidealringe sind. Im nächsten Kapitel werden wir sehen, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist. Daraus folgt unter anderem, dass $\mathbb{Z}[x]$ ein faktorieller Ring ist. Aber R ist kein Hauptidealring, denn das Ideal $I = (2, x)$ ist kein Hauptideal.

Zum Beweis nehmen wir an, es gibt ein $f \in \mathbb{Z}[x]$ mit $(f) = I$, $f = a_n x^n + \ldots + a_1 x + a_0$ mit $a_0, \ldots, a_n \in \mathbb{Z}$. Wegen $f \in (2, x)$ gibt es Polynome $g, h \in \mathbb{Z}[x]$ mit $f = 2g + xh$. Dies zeigt, dass der konstante Term a_0 eine gerade ganze Zahl sein muss. Aber aus $(f) = (2, x)$ folgt auch $2 \in (f)$, also $2 = uf$ für ein weiteres Polynom $u \in \mathbb{Z}[x]$. Dies ist nur möglich, wenn f eine Konstante ist. Wegen $x \in (f)$, also $x = vf$ für ein $v \in \mathbb{Z}[x]$ muss diese Konstante gleich 1 sein. Aber dies steht im Widerspruch dazu, dass a_0 gerade ist.

Anhang: Beispiel für einen Hauptidealring, der kein euklidischer Ring ist

Die naheliegende Frage, ob solche Ringe existieren, wird in der aktuellen Lehrbuchliteratur übergangen, so dass unklar bleibt, ob die Hauptidealringe überhaupt eine echte Verallgemeinerung der euklidischen Ringe darstellen. Wir zeigen, dass der Ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ zwar ein Hauptidealring, aber kein euklidischer Ring ist. Dabei folgen wir im Wesentlichen der Darstellung von [Wi], der einen zuvor erbrachten Beweis in der Veröffentlichung [Ca] weiter vereinfachen konnte.

Satz 12.29 Der Ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ ist ein Hauptidealring.

Beweis: In Satz 9.17 wurde gezeigt, dass die Elemente von R durch $R = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{-19} \mid a, b \in \mathbb{Z}\ ,\ a \equiv b \bmod 2\}$ gegeben sind. Sei nun I ein Ideal in R ungleich (0). Zu zeigen ist, dass es sich bei I um ein Hauptideal handelt. Die Normfunktion $N(z) = |z|^2$ nimmt auf $R \setminus \{0\}$ nur Werte aus $\mathbb{N}$ an, denn für alle $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ und $a \equiv b \bmod 2$ ist

$$N(\tfrac{1}{2}a + \tfrac{1}{2}b\sqrt{-19}) \quad = \quad \tfrac{1}{4}(a^2 + 19b^2)$$

positiv und ganzzahlig. Sind nämlich a und b beide gerade, dann sind die Zahlen a^2 und $19b^2$ beide durch vier teilbar. Sind a und b beide ungerade, dann gilt $a^2 \equiv b^2 \equiv 1 \bmod 4$, und wegen $19 \equiv 3 \bmod 4$ folgt $a^2 + 19b^2 \equiv 1 + 3 \cdot 1 \equiv 4 \equiv 0 \bmod 4$.

Auf Grund dieser Eigenschaft der Normfunktion gibt es ein $\alpha \in I \setminus \{0\}$, so dass $|\alpha|$ minimal ist. Nehmen wir nun an, I ist kein Hauptideal. Dann gibt es ein $\beta \in I \setminus (\alpha)$. Sei $\rho = \frac{\beta}{\alpha}$. In einem ersten Schritt zeigen wir, dass β so gewählt werden kann, dass $|\mathrm{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$ erfüllt ist. Dazu setzen wir $r = \frac{1}{\sqrt{19}}\mathrm{Im}(\rho)$ und wählen $s \in \mathbb{Z}$ so, dass $|2r - s| \leq \frac{1}{2}$ erfüllt ist. Definieren wir dann $\beta' = \beta - \frac{1}{2}s(1 + \sqrt{-19})\alpha$, dann folgt

$$\frac{\beta'}{\alpha} \quad = \quad \frac{\beta}{\alpha} - \tfrac{1}{2}s(1 + \sqrt{-19}) \quad = \quad \mathrm{Re}(\rho) + i\mathrm{Im}(\rho) - \tfrac{1}{2}s - i \cdot \tfrac{1}{2}s\sqrt{19} \quad = \quad \mathrm{Re}(\rho) + i \cdot r\sqrt{19} - \tfrac{1}{2}s - i \cdot \tfrac{1}{2}s\sqrt{19}$$

und somit $\mathrm{Im}(\frac{\beta'}{\alpha}) = \sqrt{19}(r - \frac{1}{2}s)$ und $|\mathrm{Im}(\frac{\beta'}{\alpha})| \leq \frac{1}{4}\sqrt{19}$. Ersetzen wir also β durch β', dann ist die Ungleichung $|\mathrm{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$ erfüllt. Außerdem gilt weiterhin $\beta \in I \setminus (\alpha)$, wenn wir β durch β' ersetzen. Denn mit β liegt auch $\beta' = \beta - \frac{1}{2}s(1 + \sqrt{-19})\alpha$ in I, und wäre β' ein Element des Hauptideals (α), dann würde dies auch für β gelten.

In einem zweiten Schritt zeigen wir, dass ein $\gamma \in I \setminus \{0\}$ mit $|\gamma| < |\alpha|$ existiert und führen damit die Minimalität von α zum Widerspruch. Zunächst betrachten wir den Fall, dass sogar $|\mathrm{Im}(\rho)| < \frac{1}{2}\sqrt{3}$ erfüllt ist. Wählen wir $a \in \mathbb{Z}$ so, das $|\mathrm{Re}(\rho) - a| \leq \frac{1}{2}$ gilt, dann folgt $|\rho - a|^2 < (\frac{1}{2})^2 + (\frac{1}{2}\sqrt{3})^2 = 1$. Sei nun $\gamma = \beta - a\alpha$. Dann liegt γ in I, das Element ist wegen $\beta \notin (\alpha)$ ungleich Null, und es gilt $|\beta - a\alpha| = |\alpha||\rho - a| < |\alpha|$, wie gewünscht.

Nun betrachten wir noch den Fall $\frac{1}{2}\sqrt{3} \leq |\mathrm{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$. Sei $\delta = 2\beta - \frac{1}{2}(1 + \sqrt{-19})\alpha$. Dann gilt $\frac{\delta}{\alpha} = 2\rho - \frac{1}{2}(1 + \sqrt{19})$. Ersetzen wir nötigenfalls β durch $-\beta$ und ρ durch $-\rho$, dann können wir $\frac{1}{2}\sqrt{3} \leq \mathrm{Im}(\rho) \leq \frac{1}{4}\sqrt{19}$ annehmen. Es folgt dann $\sqrt{3} \leq \mathrm{Im}(2\rho) \leq \frac{1}{2}\sqrt{19}$ und $\sqrt{3} - \frac{1}{2}\sqrt{19} \leq \mathrm{Im}(2\rho - \frac{1}{2}(1 + \sqrt{-19})) = \mathrm{Im}(\frac{\delta}{\alpha}) \leq 0$. Wir wählen nun $a \in \mathbb{Z}$ so, dass $|\mathrm{Re}(2\rho - \frac{1}{2}(1 + \sqrt{-19})) - a| \leq \frac{1}{2}$ erfüllt ist und definieren $\gamma = \delta - a\alpha$. Dann gilt

$$\left|\frac{\gamma}{\alpha}\right|^2 \quad = \quad \left|\frac{\delta}{\alpha} - a\right|^2 \quad = \quad |\mathrm{Re}(\tfrac{\delta}{\alpha} - a) + i\,\mathrm{Im}(\tfrac{\delta}{\alpha})|^2 \quad = \quad |\mathrm{Re}(\tfrac{\delta}{\alpha} - a)|^2 + |\mathrm{Im}(\tfrac{\delta}{\alpha})|^2 \quad \leq \quad \tfrac{1}{4} + (\sqrt{3} - \tfrac{1}{2}\sqrt{19})^2.$$

Wir zeigen, dass $(\sqrt{3} - \frac{1}{2}\sqrt{19})^2 < \frac{3}{4}$ ist. Daraus folgt dann $|\frac{\gamma}{\alpha}|^2 < 1$ und $|\gamma| < |\alpha|$, so dass wir auch in diesem Fall am Ziel sind. Aus $\sqrt{19} < \sqrt{27} = 3\sqrt{3}$ folgt $\frac{1}{2}\sqrt{19} < \frac{3}{2}\sqrt{3}$. Durch Subtraktion von $\sqrt{3}$ auf beiden Seiten erhalten wir $\frac{1}{2}\sqrt{3} > \frac{1}{2}\sqrt{19} - \sqrt{3}$, und $\frac{1}{2}\sqrt{19} - \sqrt{3}$ ist positiv wegen $3 < \frac{19}{4} \Leftrightarrow 12 < 19$. Durch Quadrieren erhalten wir nun die gewünschte Abschätzung $(\sqrt{3} - \frac{1}{2}\sqrt{19})^2 < \frac{3}{4}$. □

Satz 12.30 Der Ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ ist kein euklidischer Ring.

Beweis: Mit ähnlichen Argumenten wie in Prop. 12.15 zeigen wir zunächst, dass die Einheitengruppe von R durch $R^\times = \{\pm 1\}$ gegeben ist, und dass die Elemente 2 und 3 in R irreduzibel sind. Wegen $1 \cdot 1 = 1$ und $(-1)(-1) = 1$ sind ± 1 jedenfalls Einheiten. Ist umgekehrt $\varepsilon \in R^\times$, dann gilt $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$. Aus $N(\varepsilon), N(\varepsilon^{-1}) \in \mathbb{N}$ und $N(\varepsilon)N(\varepsilon^{-1}) = 1$ folgt $N(\varepsilon) = 1$. Schreiben wir $\varepsilon = \frac{1}{2}a + \frac{1}{2}b\sqrt{-19}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \bmod 2$, dann folgt

$\frac{1}{4}a^2+\frac{19}{4}b^2 = N(\varepsilon) = 1$ und $a^2+19b^2 = 4$. Die einzigen ganzzahligen Lösungen dieser Gleichung sind $(a,b) = (\pm 2, 0)$. Es folgt $\varepsilon \in \{\pm 1\}$. Die Einheitengruppe von R also gegeben durch $R^\times = \{\pm 1\}$ und besteht genau aus den Elementen mit Norm 1.

Wegen $N(2) = 4 > 1$ und $N(3) = 9 > 1$ sind 2 und 3 jedenfalls keine Einheiten. Wäre 2 reduzibel, dann gäbe es Elemente $\alpha, \beta \in R$, die keine Einheiten in R sind und $\alpha\beta = 2$ erfüllen. Es wäre dann $N(\alpha)N(\beta) = N(\alpha\beta) = N(2) = 4$. Wegen $\alpha, \beta \notin R^\times$ gilt außerdem $N(\alpha), N(\beta) > 1$. Damit bleibt $N(\alpha) = N(\beta) = 2$ als einzige Möglichkeit. Schreiben wir $\alpha = \frac{1}{2}a + \frac{1}{2}b\sqrt{-19}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \bmod 2$, dann ist $N(\alpha) = 2$ äquivalent zu $\frac{1}{4}a^2+\frac{19}{4}b^2 = 2 \Leftrightarrow a^2+19b^2 = 8$. Aber diese Gleichung besitzt offenbar keine Lösung mit $(a,b) \in \mathbb{Z}^2$. Ebenso zeigt die Unlösbarkeit der Gleichung $a^2 + 19b^2 = 12$, dass 3 im Ring R irreduzibel ist.

Nach diesen Vorbereitungen nehmen wir nun an, dass R euklidisch und $h : R \setminus \{0\} \to \mathbb{N}$ eine Höhenfunktion auf R ist. Weiter sei $\pi \in R$ eine Nichteinheit mit der Eigenschaft, dass $h(\pi)$ für alle Nicht-Einheiten aus $R \setminus \{0\}$ ein minimaler Wert ist. Wir zeigen, dass π dann in der Menge $\{\pm 2, \pm 3\}$ enthalten sein muss. Durch Division mit Rest erhalten wir Elemente $\gamma, \rho \in R$ mit $2 = \gamma\pi + \rho$, wobei $\rho = 0$ oder $\rho \neq 0$ und $h(\rho) < h(\pi)$ gelten muss. Auf Grund der Minimalität von $h(\pi)$ gibt es nur die beiden Möglichkeiten, dass $\rho = 0$ oder eine Einheit ist. Es gilt also $\rho \in \{-1, 0, 1\}$. Im Fall $\rho = 0$ wäre π ein Teiler von 2. Auf Grund der Irreduzibilität von 2 sind 2 und π dann assoziiert, und daraus folgt $\pi \in \{\pm 2\}$.

Betrachten wir nun den Fall $\rho = 1$. Die Gleichung $2 = \gamma\pi + 1$ liefert dann $\gamma\pi = 1$. Aber dies steht im Widerspruch dazu, dass π keine Einheit ist. Als letzte Möglichkeit betrachten wir den Fall $\rho = -1$. Dann gilt $2 = \gamma\pi - 1$. Dann gilt $\gamma\pi = 3$. Weil 3 irreduzibel ist, sind π und 3 assoziiert, also $\pi \in \{\pm 3\}$. Damit haben wir insgesamt gezeigt, dass in jedem möglichen Fall $\pi \in \{\pm 2, \pm 3\}$ gilt.

Sei nun $\theta = \frac{1}{2}(1+\sqrt{-19})$. Wiederum wenden wir Division mit Rest an und erhalten Elemente $\gamma, \rho \in R$ mit $\theta = \gamma\pi + \rho$, wobei $\rho = 0$ oder $\rho \neq 0$ und $h(\rho) < h(\pi)$ gilt. Wie zuvor schließen wir daraus $\rho \in \{-1, 0, 1\}$. Im Fall $\rho = 0$ gilt $\theta = \gamma\pi$. Im Fall $\rho = 1$ ist $\theta - 1 = \gamma\pi$, und im Fall $\rho = -1$ ist $\theta + 1 = \gamma\pi$. Also ist eines der Elemente $\theta - 1, \theta, \theta + 1$ auf jeden Fall durch π teilbar. Es gilt aber $\pi \in \{\pm 2, \pm 3\}$, und wie man sich leicht überzeugt, ist keines der sechs Elemente

$$\tfrac{1}{2}(\theta - 1) \;,\; \tfrac{1}{2}\theta \;,\; \tfrac{1}{2}(\theta + 1) \;,\; \tfrac{1}{3}(\theta - 1) \;,\; \tfrac{1}{3}\theta \;,\; \tfrac{1}{3}(\theta + 1)$$

in R enthalten. Die Annahme, dass eine Höhenfunktion h auf R existiert, hat also insgesamt zu einem Widerspruch geführt. Also ist R kein euklidischer Ring. □

Zum Schluss sei noch erwähnt, dass $\mathbb{Z}[\sqrt{d}]$ in einzelnen Fällen auch für positives d euklidisch ist. Beispielsweise sind $\mathbb{Z}[\sqrt{2}]$ und $\mathbb{Z}[\sqrt{3}]$ euklidische Ringe, mit $h(a + b\sqrt{2}) = |a^2 - 2b^2|$ bzw. $h(a + b\sqrt{3}) = |a^2 - 3b^2|$ als Höhenfunktion. Dies lässt sich auf ähnliche Weise wie beim Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen zeigen. Es gibt aber auch Fälle, in denen der Ring $\mathbb{Z}[\sqrt{d}]$ euklidisch ist, die Höhenfunktion aber eine andere Gestalt besitzt. In [Ha] wird dies zum Beispiel für den Ring $\mathbb{Z}[\sqrt{14}]$ nachgewiesen.

§ 13. Irreduzibilitätskriterien und Gauß'sches Lemma

Zusammenfassung. Wie wir insbesondere in der Körpertheorie noch sehen werden, ist es für verschiedene Anwendungen notwendig, die Irreduzibilität von Polynomen über Körpern nachzuweisen. In diesem Abschnitt werden wir mehrere solche Kriterien zur Verfügung stellen, wobei wir für die Herleitung insbesondere auf die Theorie des letzten Kapitels zurückgreifen werden. Von besonderem Interesse ist für uns die Situtation, in der K Quotientenkörper eines faktoriellen Rings R ist, wie sie z.B. für $K = \mathbb{Q}$ und $R = \mathbb{Z}$ vorliegt. Hier werden wir unter anderem zeigen, dass für die Irreduzibilität eines Polynoms $f \in R[x]$ über dem Körper K bereits die Irreduzibilität in $R[x]$ hinreichend ist.

Wichtige Grundbegriffe	***Zentrale Sätze***
– primitives Polynom	– Kriterium für Nullstellen ganzzahliger Polynome
	– Gauß'sches Lemma
	– Polynomringe über faktoriellen Ringen sind faktoriell.
	– Eisenstein-Kriterium
	– Reduktionskriterium

Wir beginnen mit einigen elementaren Feststellungen zur Irreduzibilität von Polynomen über Körpern.

Proposition 13.1 Sei K ein Körper und $f \in K[x]$ nicht konstant, also $f \notin K$.

(i) Ist $\operatorname{grad}(f) = 1$, dann ist f im Ring $K[x]$ irreduzibel.

(ii) Im Fall $\operatorname{grad}(f) \in \{2, 3\}$ ist f genau dann irreduzibel, wenn f in K keine Nullstelle besitzt.

(iii) Im Fall $\operatorname{grad}(f) \in \{4, 5\}$ ist f genau dann irreduzibel, wenn f in K keine Nullstelle besitzt und durch kein normiertes, irreduzibles Polynom vom Grad 2 teilbar ist.

Beweis: zu (i) Sei $f \in K[x]$ mit $\operatorname{grad}(f) = 1$. Dann ist f ungleich null und als nicht-konstantes Polynom nach Folgerung 11.30 auch keine Einheit. Seien nun $g, h \in K[x]$ mit $f = gh$. Nach Teil (ii) von Proposition 11.29 gilt $\operatorname{grad}(g)+\operatorname{grad}(h) = \operatorname{grad}(gh) = \operatorname{grad}(f) = 1$. Wegen $\operatorname{grad}(g), \operatorname{grad}(h) \geq 0$ folgt daraus $\operatorname{grad}(g) = 0$ oder $\operatorname{grad}(h) = 0$. Nach Folgerung 11.30 ist also eines der beiden Polynome g, h eine Einheit in $K[x]$.

zu (ii) „⇒" Nehmen wir an, dass f irreduzibel ist, aber eine Nullstelle $a \in K$ besitzt. Nach Folgerung 12.5 existiert dann ein $g \in K[x]$ mit $f = (x-a)g$. Wegen $\operatorname{grad}(x-a) = 1$ ist $x-a$ in $K[x]$ keine Einheit. Aus $\operatorname{grad}(f) = \operatorname{grad}(x-a)+\operatorname{grad}(g) = 1+\operatorname{grad}(g)$ folgt $\operatorname{grad}(g) = \operatorname{grad}(f)-1 \geq 1$, und somit ist auch g keine Einheit in $K[x]$. Aber nun folgt aus der Gleichung $f = (x-a)g$, dass f in $K[x]$ nicht irreduzibel ist, im Widerspruch zur Voraussetzung.

„⇐" Nach Voraussetzung besitzt f in K keine Nullstelle. Nehmen wir an, dass f in $K[x]$ nicht irreduzibel ist. Wegen $f \notin K$ ist f in $K[x]$ auch keine Einheit und somit ein reduzibles Element. Sei $f = gh$ eine Zerlegung von f in Nicht-Einheiten $g, h \in K[x]$. Dann sind g und h ungleich null, und außerdem nicht-konstant, denn andernfalls wäre eines der Elemente g, h in $K^\times$ enthalten und somit auch eine Einheit in $K[x]$. Es gilt also $\operatorname{grad}(g), \operatorname{grad}(h) \geq 1$. Da

zugleich $\text{grad}(g) + \text{grad}(h) = \text{grad}(f) \leq 3$ gilt, muss eines der Polynom g, h vom Grad 1 sein. Aber dies bedeutet, dass eines dieser beiden Polynome, und damit auch das Polynom f, in K eine Nullstelle besitzt, im Widerspruch zur Voraussetzung. Denn ist beispielsweise $g = cx + d$ mit $c \in K^\times$ und $d \in K$, dann gilt für $a = -\frac{d}{c}$ offenbar $g(a) = 0_K$.

zu (iii) „⇒“ Wie in Teil (ii) überprüft man unmittelbar, dass aus der Existenz einer Nullstelle in K die Reduzibilität f in $K[x]$ folgt. Ebenso ist f in $K[x]$ reduzibel, wenn ein normierter Teiler $g \in K[x]$ vom Grad 2 existiert. Denn dann existiert ein $h \in K[x]$ mit $f = gh$, und wegen $\text{grad}(g) = 2$ und $\text{grad}(h) = \text{grad}(f) - \text{grad}(g) = \text{grad}(f) - 2 \geq 4 - 2 = 2$ sind g und h keine Einheiten in $K[x]$.

„⇐“ Nehmen wir an, dass f in $K[x]$ kein irreduzibles Element und $f = gh$ eine Zerlegung von f in Nicht-Einheiten $g, h \in K[x]$ ist. Wir zeigen, dass f dann eine Nullstelle in K oder einen irreduziblen, normierten Teiler vom Grad 2 besitzt. Wenn wir davon ausgehen, dass f in K keine Nullstelle besitzt, dann müssen g und h beide vom Grad ≥ 2 sein. Denn wegen $g, h \notin K$ gilt auf jeden Fall $\text{grad}(g), \text{grad}(h) \geq 1$, und wäre eines dieser Polynome vom Grad 1, dann würde daraus die Existenz einer Nullstelle von f in K folgen, wie wir bereits unter (ii) festgestellt haben. Aber aus $\text{grad}(g), \text{grad}(h) \geq 2$ und $\text{grad}(g) + \text{grad}(h) = \text{grad}(f) \leq 4$ folgt $\text{grad}(g) = 2$ oder $\text{grad}(h) = 2$. Nach eventueller Vertauschung von g und h können wir $\text{grad}(g) = 2$ annehmen. Bezeichnet $c \in K^\times$ den Leitkoeffizienten von g, dann ist $\tilde{g} = c^{-1}g$ ein normiertes Polynom vom Grad 2. Außerdem ist $\tilde{g}$ in $K[x]$ irreduzibel, dann andernfalls hätte $\tilde{g}$ nach Teil (ii) in K eine Nullstelle, und dies wäre auch eine Nullstelle von f, im Widerspruch zu unserer Annahme. Darüber hinaus ist $\tilde{g}$ weiterhin ein Teiler von f in $K[x]$, denn es gilt $f = \tilde{g} \cdot (ch)$. □

Aus Teil (ii) von Proposition 13.1 folgt beispielsweise die Irreduzibilität des Polynom $f = x^2 - 2$ in $\mathbb{Q}[x]$. Denn andernfalls wäre eine der beiden reellen Nullstellen $\pm\sqrt{2}$ in $\mathbb{Q}$ enthalten, im Widerspruch zu Irrationalität von $\sqrt{2}$. Das Beispiel zeigt auch, dass die Irreduzibilität eines Polynoms im Allgemeinen davon abhängt, über welchem Grundkörper man das Polynom betrachtet. Im Polynomring $\mathbb{R}[x]$ ist f ein reduzibles Element, wie man anhand der Zerlegung $f = (x - \sqrt{2})(x + \sqrt{2})$ erkennen kann.

Mit Hilfe von Teil (iii) kann man beispielsweise zeigen, dass $g = x^5 + x^2 + \bar{1}$ im Polynomring $\mathbb{F}_2[x]$ irreduzibel ist. Dafür überprüft man zunächst, dass g wegen $g(\bar{0}) = g(\bar{1}) = \bar{1}$ in $\mathbb{F}_2$ keine Nullstelle besitzt. Das Polynom kann also nur dann reduzibel sein, wenn ein normierter Teiler vom Grad 2 existiert. Die normierten Polynome von Grad 2 in $\mathbb{F}_2[x]$ sind x^2, $x^2 + \bar{1}$, $x^2 + x$ und $x^2 + x + \bar{1}$, und wie man unmittelbar nachrechnet, ist $h = x^2 + x + \bar{1}$ als einziges dieser vier Polynome nullstellenfrei und somit irreduzibel. Aber andererseits ist h kein Teiler von g. Denn wäre dies der Fall, dann müsste h auch ein Teiler von $g - x^3 \cdot h = x^4 + x^3 + x^2 + \bar{1}$ und von $g - x^3 \cdot h - x^2 \cdot h = \bar{1}$ sein.

Um die soeben formulierte Proposition anwenden zu können, benötigen wir einfach zu handhabende Kriterien für die Existenz von Nullstellen. Für Quotientenkörper faktorieller Ringe erweist sich der folgende Satz als hilfreich.

Satz 13.2 Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$ ein Polynom vom Grad $n \geq 1$. Sei $f = a_n x^n + \ldots + a_1 x + a_0$ mit $a_0, \ldots, a_n \in R$.

(i) Ist $\alpha \in K$ eine Nulstelle von f, $\alpha = \frac{p}{q}$ mit $p, q \in R$ und $q \neq 0$, wobei p und q teilerfremd sind, dann gilt $q \mid a_n$ und $p \mid a_0$.

(ii) Ist insbesondere f normiert, also $a_n = 1$, dann liegt α in R und ist ein Teiler von a_0.

Beweis: Offenbar ist die Aussage (ii) eine direkte Folgerung von (i). Zum Beweis von (i) sei $\alpha = \frac{p}{q}$ wie angegeben. Es gilt

$$f(\alpha)=0 \quad \Leftrightarrow \quad a_n\alpha^n + \sum_{k=0}^{n-1} a_k\alpha^k = 0 \quad \Leftrightarrow \quad a_n\alpha^n = -\sum_{k=0}^{n-1} a_k\alpha^k \quad \Leftrightarrow \quad a_n(\tfrac{p}{q})^n = -\sum_{k=0}^{n-1} a_k(\tfrac{p}{q})^k$$
$$\Leftrightarrow \quad a_n p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k} = q\left(-\sum_{k=0}^{n-1} a_k p^k q^{n-1-k}\right).$$

Dies zeigt, dass $a_n p^n$ durch q teilbar ist. Weil mit p und q auch p^n und q teilerfremd sind, muss $q \mid a_n$ gelten. Nun gilt ebenso

$$f(\alpha)=0 \quad \Leftrightarrow \quad \sum_{k=1}^{n} a_k\alpha^k + a_0 = 0 \quad \Leftrightarrow \quad a_0 = -\sum_{k=1}^{n} a_k\alpha^k \quad \Leftrightarrow \quad a_0 = -\sum_{k=1}^{n} a_k(\tfrac{p}{q})^k$$
$$\Leftrightarrow \quad a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k} = p\left(-\sum_{k=1}^{n} a_k p^{k-1} q^{n-k}\right).$$

Dies zeigt, dass $a_0 q^n$ von p geteilt wird. Weil p und q^n teilerfremd sind, folgt daraus $p \mid a_0$. □

Mit Hilfe dieses Kriteriums kann beispielsweise leicht gezeigt werden, dass Polynom $f = x^3 - x + 2$ in $\mathbb{Q}[x]$ irreduzibel ist. Wäre es reduzibel, dann hätte es wegen $\text{grad}(f) = 3$ eine rationale Nullstelle. Weil aber $\mathbb{Z}$ faktoriell und $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$ ist, und weil f in $\mathbb{Z}[x]$ liegt und normiert ist, muss jede rationale Nullstelle von f ein ganzzahliger Teiler von 2 sein. Die einzigen möglichen Nullstellen von f in $\mathbb{Q}$ sind damit $\pm 1, \pm 2$. Es gilt aber $f(1) = f(-1) = 2$, $f(2) = 4$ und $f(-2) = -4$. Somit besitzt f in $\mathbb{Q}$ keine Nullstelle.

Unser nächstes Ziel ist die Formulierung und der Beweis des Gaußschen Lemmas, dass einen Zusammenhang zwischen der Irreduzibilität über einem faktoriellen Ring R und über dessen Quotientenkörper K herstellt. In den Anwendungen ist man meistens am Spezialfall $R = \mathbb{Z}$ und $K = \mathbb{Q}$ interessiert.

> **Lemma 13.3** Sei R ein faktorieller Ring und K sein Quotientenkörper. Sind $a_1, ..., a_n \in K^\times$ beliebig vorgegeben, dann gibt ein $\alpha \in K^\times$, so dass die Elemente $a_i' = \alpha a_i$ in R liegen und $\text{ggT}(a_1', ..., a_n') = 1$ gilt.

Beweis: Nach Definition des Quotientenkörpers gibt es Elemente $r_i, s_i \in K$ mit $s_i \neq 0$, so dass $a_i = r_i/s_i$ für $1 \leq i \leq n$ gilt. Setzen wir $\alpha = s_1 ... s_n$, dann liegt α in $K^\times$, und es gilt

$$\alpha a_i = r_i \left(\prod_{k=1}^{i-1} s_k\right)\left(\prod_{k=i+1}^{n} s_k\right) \quad \in \quad R.$$

Wir können also o.B.d.A. voraussetzen, das $a_i \in R$ für $1 \leq i \leq n$ gilt Sei nun $d = \text{ggT}(a_1, ..., a_n)$, $\alpha = d^{-1}$ und $a_i' = \alpha a_i$ für $1 \leq i \leq n$. Angenommen, die Elemente $a_1', ..., a_n'$ sind nicht teilerfremd. Dann gibt es ein Primelement p mit $p | a_i'$ für $1 \leq i \leq n$. Es folgt $pd | a_i$ für $1 \leq i \leq n$ und somit $pd | d$ nach Definition des ggT. Dies bedeutet, dass ein $a \in R$ mit $pda = d$ existiert, und die Kürzungsregel liefert $pa = 1$. Aber dies ist unmöglich, denn ein Primelement kann nicht zugleich Einheit sein. Also ist $\text{ggT}(a_1', ..., a_n') = 1$ erfüllt. □

> **Definition 13.4** Sei R ein faktorieller Ring und $f = \sum_{k=0}^{n} a_k x^k \in R[x]$. Wir nennen das Polynom f ***primitiv***, wenn $f \neq 0$ ist und die Koeffizienten $a_0, ..., a_n$ keinen gemeinsamen Primteiler besitzen.

Wir betrachten einige Beispiele.

(i) Normierte Polynome in $R[x]$, also Polynome der Form $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ mit höchstem Koeffizienten 1 und ansonsten beliebigen Koeffizienten $a_0, \ldots, a_{n-1} \in R$, sind immer primitiv.

(ii) Das Polynom $2x^2 + 4x + 6$ ist nicht primitiv, denn es gilt $\mathrm{ggT}(2,4,6) = 2$.

(iii) Ist R ein Integritiätsbereich und $f \in R[x]$ ein irreduzibles Element vom Grad ≥ 1, dann ist f primitiv. Ansonsten hätten die Koeffizienten von f einen gemeinsamen Primteiler $p \in R$, und es würde ein Polynom $\tilde{f} \in R[x]$ mit $f = p\tilde{f}$ existieren. Dies aber bedeutet, dass f als Produkt von Nichteinheiten dargestellt werden kann und somit reduzibel ist.

Folgerung 13.5 Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in K[x]$ ein Polynom mit $f \neq 0$. Dann gibt es ein $\alpha \in K^\times$, so dass αf in $R[x]$ liegt und primitiv ist.

Beweis: Das folgt unmittelbar aus Lemma 13.3, angewendet auf die Koeffizienten des Polynoms f. □

Sei nun R ein Integritätsbereich, $\mathfrak{p} \subseteq R$ ein Primideal und $\bar{R} = R/\mathfrak{p}$ der zugehörige Restklassenring, mit dem kanonischen Epimorphismus $\pi : R \to \bar{R}$. Wir bezeichnen mit $\mathfrak{p}[x] = \mathfrak{p}R[x]$ die Menge aller Polynome, deren Koeffizienten im Primideal $\mathfrak{p}$ enthalten sind. Es handelt sich um das von der Teilmenge $\mathfrak{p}$ in $R[x]$ erzeugte Ideal.

Lemma 13.6 Der Homomorphismus $\phi : R[x] \to \bar{R}[x]$ gegeben durch $\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \pi(a_i)x_i$ induziert einen Isomorphismus $R[x]/\mathfrak{p}[x] \cong \bar{R}[x]$ von Ringen.

Beweis: Weil der kanonische Epimorphismus $\pi : R \to \bar{R}$ surjektiv ist, gilt dasselbe offenbar auch für ϕ. Außerdem ist $\mathfrak{p}[x]$ ist der Kern von ϕ. Also folgt die Aussage aus dem Homomorphiesatz. □

Folgerung 13.7 Das Ideal $\mathfrak{p}[x]$ ist ein Primideal in $R[x]$.

Beweis: Weil $\mathfrak{p}$ in R ein Primideal ist, handelt es sich beim Faktorring $\bar{R}$ nach Satz 11.12 um einen Integritätsbereich. Damit ist auch der Polynomring $\bar{R}[x]$ ein Integritätsbereich, auf Grund der Isomorphie also auch $R[x]/\mathfrak{p}[x]$. Wiederum nach Satz 11.12 folgt daraus, dass $\mathfrak{p}[x]$ ein Primideal ist. □

Satz 13.8 *(Lemma von Gauß)*
Sei R ein faktorieller Ring, und seien $f, g \in R[x]$ primitive Polynome. Dann ist auch fg primitiv.

Beweis: Angenommen, das Produkt fg ist nicht primitiv und das Primelement $p \in R$ ein gemeinsamer Teiler der Koeffizienten. Nach Proposition 12.17 ist (p) in R ein Primideal, und nach Folgerung 13.7 erzeugt p auch ein Primideal in $R[x]$, das wir ebenfalls mit (p) bezeichnen. Nun sind fg nach Voraussetzung in (p) enthalten, es folgt $f \in (p)$ oder $g \in (p)$. Setzen wir o.B.d.A. den ersten Fall voraus, dann ist p ein gemeinsamer Teiler der Koeffizienten von f, im Widerspruch dazu, dass f primitiv ist. □

Satz 13.9 Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$ ein Polynom mit $\text{grad}(f) \geq 1$.

(i) Ist $g \in R[x]$ ein primitives Polynom mit der Eigenschaft, dass g ein Teiler von f in $K[x]$ ist, so ist g bereits ein Teiler von f in $R[x]$.

(ii) Ist f irreduzibel in $R[x]$, dann auch in $K[x]$.

Beweis: zu (i) Nach Voraussetzung gibt es ein $h \in K[x]$ mit $f = gh$, und Folgerung 13.5 liefert uns ein Element $\alpha \in K^\times$, so dass $\tilde{h} = \alpha h$ in $R[x]$ liegt und primitiv ist. Nach dem Lemma von Gauß ist $g\tilde{h}$ primitiv, und es gilt $f = g(\alpha^{-1}\tilde{h})$.

Sei $\alpha = a/b$ eine Darstellung von α als gekürzter Bruch, also mit $a, b \in R$, $b \neq 0$ und $\text{ggT}(a,b) = 1$. Dann erhalten wir aus $f = g(\alpha^{-1}\tilde{h})$ Gleichung $af = bg\tilde{h}$. Angenommen, p ist ein Primteiler von a. Dann wäre p auch ein gemeinsamer Primteiler der Koeffizienten von $g\tilde{h}$. Aber das ist unmöglich, weil $g\tilde{h}$ primitiv ist. Es folgt $\alpha^{-1} = b/a \in R$, und die Gleichung $f = g(\alpha^{-1}\tilde{h})$ zeigt, dass g auch in $R[x]$ ein Teiler von f ist.

zu (ii) Sei $f = gh$ mit $g, h \in K[x]$. Ferner sei $\alpha \in K^\times$ ein Element mit der Eigenschaft, dass $\tilde{g} = \alpha g$ in $R[x]$ liegt und primitiv ist. Wegen $f = \tilde{g}(\alpha^{-1}h)$ ist auch $\tilde{g}$ ein Teiler von f in $K[x]$. Weil aber $\tilde{g}$ außerdem primitiv ist, ist $\tilde{g}$ nach Teil (i) sogar ein Teiler von f in $R[x]$. Es gibt also ein $\tilde{h} \in R[x]$ mit $f = \tilde{g}\tilde{h}$. Wegen $\tilde{g}\tilde{h} = f = \tilde{g}(\alpha^{-1}h)$ gilt $\tilde{h} = \alpha^{-1}h$. Weil f nach Voraussetzung in $R[x]$ irreduzibel ist, ist $\tilde{g}$ oder $\tilde{h}$ eine Einheit in $R[x]$, also ein Element aus $R^\times$. Wegen $\tilde{g} = \alpha g$ und $\tilde{h} = \alpha^{-1}h$ folgt daraus $g \in K^\times$ oder $h \in K^\times$. Also ist g oder h eine Einheit in $K^\times$, und folglich ist f auch in $K[x]$ irreduzibel. □

Um also beispielsweise zu zeigen, dass ein normiertes Polynom $f \in \mathbb{Z}[x]$ im Polynomring $\mathbb{Q}[x]$ irreduzibel ist, genügt es, die Irreduzibilität in $\mathbb{Z}[x]$ nachzuweisen. In vielen Fällen ist dies bedeutend einfacher. Überprüfen wir beispielsweise die Irreduzibilität des Polynoms $f = x^4 + 1$ in $\mathbb{Z}[x]$, indem wir davon ausgehen, dass eine Zerlegung $f = gh$ in Nicht-Einheiten $g, h \in \mathbb{Z}[x]$ gegeben ist und dies zum Widerspruch führen. Da f normiert ist, dürfen wir annehmen, dass auch g und h beide normiert sind. Denn die einzige weitere Möglichkeit besteht darin, dass g und h beide -1 als Leitkoeffizient besitzen, und in diesem Fall ist dann $f = (-g)(-h)$ eine Zerlegung in normierte, ganzzahlige Faktoren. Die Zerlegung $f = gh$ zeigt auch, dass das Produkt der konstanten Terme von g und h gleich 1 ist. Die konstanten Terme von g und h sind also entweder beide gleich 1 oder beide gleich -1.

Da f als normiertes Polynom primitiv ist, muss $\text{grad}(g), \text{grad}(h) \geq 1$ gelten. Denn ansonsten wären g und h Nicht-Einheiten in $\mathbb{Z}$, würden also einen Primteiler p besitzen, und dieses p wäre dann auch ein gemeinsamer Teiler der Koeffizienten von f, im Widerspruch zu $p \nmid 1$. Aber auch $\text{grad}(g) = 1$ oder $\text{grad}(h) = 1$ ist ausgeschlossen. Denn in diesem Fall wäre eines der beiden Polynome gleich $x - 1$ oder $x + 1$. Aber wegen $f = gh$ wäre dann 1 oder -1 eine Nullstelle von f, im Widerspruch dazu, dass f nullstellenfrei ist. Wegen $\text{grad}(g) + \text{grad}(h) = \text{grad}(f) = 4$ müssten g und h also beide vom Grad 2 sein.

Insgesamt kommen wir zu dem Ergebnis, dass $a, b \in \mathbb{Z}$ existieren, so dass entweder $g = x^2 + ax + 1$ und $h = x^2 + bx + 1$ oder $g = x^2 + ax - 1$ und $h = x^2 + bx - 1$ erfüllt ist. Die Berechnung der beiden Produkte ergibt

$$(x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a+b)x^3 + (ab+2)x^2 + (a+b)x + 1$$

und

$$(x^2 + ax - 1)(x^2 + bx - 1) = x^4 + (a+b)x^3 + (ab-2)x^2 - (a+b)x + 1.$$

Aber der Vergleich mit dem Term vom Grad 3 in x^4+1 zeigt, dass dann $b=-a$ gelten muss. Der quadratische Term $(ab+2)x^2$ wäre dann entweder gleich $(2-a^2)x^2$ oder gleich $-(2+a^2)x^2$, auf jeden Fall ungleich null. Dies zeigt, dass in $\mathbb{Z}[x]$ auch keine Zerlegung von f in zwei Faktoren vom Grad 2 existiert. Insgesamt ist damit nachgewiesen, dass f in $\mathbb{Z}[x]$ und damit auch in $\mathbb{Q}[x]$ irreduzibel ist.

Aus dem Gauß'schen Lemma kann ein weiteres wichtiges Ergebnis abgeleitet werden.

Satz 13.10 Ist R ein faktorieller Ring, dann ist auch $R[x]$ faktoriell.

Beweis: Sei $f \in R[x]$ ungleich 0_R und keine Einheit in $R[x]$. Wir zeigen zunächst, dass f in $R[x]$ eine Zerlegung in irreduzible Elemente besitzt. Sei c ein ggT der Koeffizienten von f im Ring R. Dann können wir f in der Form $f=cg$ schreiben, mit einem primitiven Polynom g. Weil R faktoriell ist, kann c in R als Produkt irreduzibler Elemente dargestellt werden.

Wir zeigen nun durch vollständige Induktion über $m=\text{grad}(g)$, dass auch g ein Produkt irreduzibler Elemente ist. Im Fall $m=0$ ist g in $R[x]$ eine Einheit und nichts zu zeigen. Setzen wir nun $m \geq 1$ voraus. Besitzt g keine Zerlegung in Nicht-Einheiten, so ist g nach Definition irreduzibel. Nehmen wir nun an, es gilt $g=h_1h_2$, wobei h_1 und h_2 in $R[x]$ keine Einheiten sind. Wäre $\text{grad}(h_1)=0$ oder $\text{grad}(h_2)=0$, dann wäre h_1 oder h_2 eine Nicht-Einheit in R und würde somit von einem Primelement p des Rings R geteilt. Somit wäre dann p ein Teiler von g, im Widerspruch dazu, dass g primitiv ist. So aber gilt $0<\text{grad}(g_1),\text{grad}(g_2)<m$. Wir können auf g_1 und g_2 die Induktionsvoraussetzung anwenden und erhalten Darstellungen beider Polynome als Produkte irreduzibler Elemente von $R[x]$. Daraus ergibt sich eine ebensolche Darstellung für g, womit der Induktionsschritt abgeschlossen ist.

Nun müssen wir noch zeigen, dass die Darstellung von unserem Polynom f im Wesentlichen eindeutig ist. Wieder stellen wir f als Produkt cg mit einem Element $c \in R$ und einem primitiven Polynom $g \in R[x]$ dar. In jeder Darstellung von f als Produkt irreduzibler Elemente bilden die Faktoren vom Grad 0 (bis auf Einheiten) eine Zerlegung von c, und die übrigen Faktoren eine Zerlegung von g. Da die Eindeutigkeit der Faktorzerlegung in R bereits bekannt ist, können wir uns auf den Fall $f=g$ beschränken. Nehmen wir nun an, dass durch

$$g_1 \cdot \ldots \cdot g_r \quad = \quad f \quad = \quad h_1 \cdot \ldots \cdot h_s$$

zwei Zerlegungen des primitiven Polynoms $f \in R[x]$ in irreduzible Elemente g_i, h_j des Rings $R[x]$ gegeben sind, alle von positivem Grad. Nach Satz 13.9 (ii) sind die Elemente g_i, h_j auch alle irreduzibel in $K[x]$, wobei K den Quotientenkörper von R bezeichnet. Auf Grund der Eindeutigkeit der Primfaktorzerlegung in $K[x]$ muss $r=s$ gelten, und nach eventueller Umnummerierung ist g_i in $K[x]$ assoziiert zu h_i, für $1 \leq i \leq r$. Wegen Satz 13.9 (i) g_i auch in $R[x]$ jeweils assoziiert zu h_i. Damit ist die Eindeutigkeit der Zerlegung nachgewiesen. □

Wir formulieren noch zwei Kriterien für die Irreduzibilität von Polynomen über Ringen.

Satz 13.11 *(Eisenstein-Kriterium)*
Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f \in R[x]$ ein primitives Polynom vom Grad $n > 0$. Es sei $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ mit $a_0, \ldots, a_n \in R$, und wir setzen voraus, dass die Koeffizienten von f folgende Bedingungen erfüllen.

$$\text{(i)}\ \ p | a_i \text{ für } 0 \leq i < n \qquad \text{(ii)}\ \ p \nmid a_n \qquad \text{(iii)}\ \ p^2 \nmid a_0$$

Dann ist f in $R[x]$ irreduzibel.

Beweis: Angenommen, es gibt Polynome $g, h \in R[x]$ mit $f = gh$. Wir schreiben

$$g \quad = \quad \sum_{i=0}^{r} b_i x^i \quad \text{und} \quad h \quad = \quad \sum_{k=0}^{s} c_k x^k \quad \text{mit} \quad b_i, c_k \in R, \quad b_r, c_s \neq 0.$$

Dann gilt $a_0 = b_0 c_0$, und wegen Bedingung (iii) gilt $p | a_0$, $p^2 \nmid a_0$. Nach eventueller Vertauschung von g und h können wir annehmen, dass $p | b_0$ und $p \nmid c_0$ gilt. Wäre p ein Teiler sämtlicher Koeffizienten von g, dann wäre p auch ein Teiler von $a_n = b_r c_s$, im Widerspruch zur Bedingung (ii). Es gibt also ein minimales $u \in \{1, \ldots, r\}$ mit $p \nmid b_u$. Nun gilt

$$a_u \quad = \quad \sum_{i=0}^{u} b_{u-i} c_i \quad ,$$

und p ist ein Teiler von $b_{u-i}c_i$ für $1 \leq i \leq u$, aber kein Teiler von $b_u c_0$. Folglich ist p auch kein Teiler von a_u, und wegen Bedingung (i) muss $u = n$ gelten. Damit ist $\text{grad}(g) = n = \text{grad}(f)$ und $\text{grad}(h) = 0$. Weil f primitiv ist, muss h in $R^\times$ liegen. Damit ist die Irreduzibilität von f in $R[x]$ bewiesen. □

Beispielsweise sind die Polynome $x^2 - 5$ und $x^3 + 2x + 6$ beide primitiv, weil sie normiert sind. Beim ersten Polynom kann das Eisenstein-Kriterium auf die Primzahl $p = 5$, beim zweiten auf $p = 2$ angewendet werden. Also sind beide Polynome in $\mathbb{Z}[x]$ und nach Satz 13.9 auch in $\mathbb{Q}[x]$ irreduzibel.

Satz 13.12 *(Reduktionskriterium)*
Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $\bar{R} = R/(p)$. Es sei $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ ein primitives Polynom mit $a_n \notin (p)$ und $\bar{f}$ das Bild von f in $\bar{R}[x]$. Ist $\bar{f}$ in $\bar{R}[x]$ irreduzibel, dann auch das Polynom f in $R[x]$.

Beweis: Nehmen wir an, es gibt eine Zerlegung $f = gh$ von f mit $g, h \in R[x]$, wobei wir annehmen, dass weder g noch h eine Einheit in $R[x]$ ist. Weil f primitiv ist, sind dann g und h auch keine konstanten Polynome. Es gilt dann $\bar{f} = \bar{g}\bar{h}$ in $\bar{R}[x]$, wobei $\bar{g}, \bar{h}$ die Bilder von g, h in $\bar{R}[x]$ bezeichnen. Wegen $a_n \notin (p)$ gilt $\text{grad}(f) = \text{grad}(\bar{f})$, und damit muss auch $\text{grad}(g) = \text{grad}(\bar{g})$ und $\text{grad}(h) = \text{grad}(\bar{h})$ gelten.

Insbesondere sind $\bar{g}$ und $\bar{h}$ nicht konstant. Nun ist (p) wegen Proposition 12.17 ein Primideal in R und $\bar{R} = R/(p)$ damit nach Satz 11.12 (i) ein Integritätsbereich. Daraus folgt, dass die Einheiten im Polynomring $\bar{R}[x]$ genau die Einheiten

in $\bar{R}$ sind, siehe Folgerung 11.30. Somit sind $\bar{g}$ und $\bar{h}$ keine Einheiten in $\bar{R}[x]$. Aber dann zeigt die Gleichung $\bar{f} = \bar{g}\bar{h}$, dass $\bar{f}$ in $\bar{R}[x]$ nicht irreduzibel ist. □

Als Anwendung des Reduktionskriteriums zeigen wir, dass $f = x^3 + x + 1$ in $\mathbb{Q}[x]$ irreduzibel ist. Offenbar ist f in $\mathbb{Z}[x]$ ein primitives Polynom. Setzen wir $\mathfrak{p} = (2)$, dann ist $R/\mathfrak{p} \cong \mathbb{F}_2$. Der Leitkoeffizient von f ist gleich 1 und liegt somit nicht in $\mathfrak{p}$. Das Bildpolynom

$$\bar{f} \quad = \quad x^3 + x + \bar{1} \in \mathbb{F}_2[x]$$

hat in $\mathbb{F}_2$ keine Nullstelle (es gilt $\bar{f}(\bar{0}) = \bar{f}(\bar{1}) = \bar{1}$), wegen $\operatorname{grad}(\bar{f}) = 3$ ist es also irreduzibel. Auf Grund des Reduktionskriteriums ist f also in $\mathbb{Z}[x]$ irreduzibel, und mit Satz 13.9 erhalten wir die Irreduzibilität in $\mathbb{Q}[x]$.

§ 14. Kongruenzrechnung und Chinesischer Restsatz

Zusammenfassung. Der *Chinesische Restsatz* ermöglicht unter gewissen Voraussetzungen die Darstellung von Faktorringen R/I als direktes Produkt von Ringen. Eine zahlentheoretische Anwendung dieses Satzes ist die Bestimmung der Lösungsmengen von Systemen von Kongruenzen. Hierbei spielt der bereits in § 11 thematisierte Zusammenhang zwischen Kongruenzen und Faktorringen eine wichtige Rolle. Als weitere Anwendungen untersuchen wir die Nullstellen von Polynomen in Restklassenringen. Außerdem bestimmen wir die Struktur der primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ als direktes Produkt zyklischer Gruppen.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Teilerfremdheit von Idealen	– Chinesischer Restsatz für beliebige Ringe
– Exponent einer Gruppe	– Folgerung: simultane Lösbarkeit von Kongruenzen
– Primitivwurzel modulo einer Primzahl p	– Folgerung: $(\mathbb{Z}/(mn)\mathbb{Z}\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ für $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$
	– Nullstellen von Polynomen in Restklassenringen
	– Einheitengruppen endlicher Körper sind zyklisch.
	– Struktur von $(\mathbb{Z}/p^r\mathbb{Z})^\times$ (p Primzahl, $r \in \mathbb{N}$)

Bereits in der Linearen Algebra haben wir für jede natürliche Zahl $n \in \mathbb{N}$ auf $\mathbb{Z}$ die Kongruenzrelation modulo n definiert. In § 11 haben wir dann die Kongruenzrelation für Ideale in beliebigen Ringen eingeführt. In erster Linie für die Kongruenzen modulo n, teilweise aber auch für die allgemeinen Kongruenzen, werden wir in diesem Kapitel einige Ergebnisse zusammentragen. Wir beginnen mit dem Beweis einiger elementarer Rechenregeln für Kongruenzrelationen.

Proposition 14.1 Seien $m, n \in \mathbb{N}$, außerdem $a, b, c, d \in \mathbb{Z}$ und p eine Primzahl.

(i) Aus $a \equiv c \bmod n$ und $b \equiv d \bmod n$ folgt $a + b \equiv c + d \bmod n$ und $ab \equiv cd \bmod n$.

(ii) Gilt $a \equiv b \bmod n$ und ist m ein Teiler von n, dann folgt $a \equiv b \bmod m$.

(iii) Es gilt $a \equiv b \bmod n$ genau dann, wenn $ma \equiv mb \bmod mn$ erfüllt ist.

(iv) Es gilt $a^p \equiv a \bmod p$. Unter der zusätzlichen Voraussetzung $p \nmid a$ gilt darüber hinaus $a^p \equiv 1 \bmod p$.

Die Aussage (iv) ist auch als *Kleiner Satz von Fermat* bekannt.

Beweis: zu (i) Aus den Voraussetzungen folgt $a + n\mathbb{Z} = c + n\mathbb{Z}$ und $b + n\mathbb{Z} = d + n\mathbb{Z}$. Damit erhalten wir im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ die Gleichungen $(a+b) + n\mathbb{Z} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (c + n\mathbb{Z}) + (d + n\mathbb{Z}) = (c + d) + n\mathbb{Z}$ und ebenso $ab + n\mathbb{Z} = (a + n\mathbb{Z})(b + n\mathbb{Z}) = (c + n\mathbb{Z})(d + n\mathbb{Z}) = cd + n\mathbb{Z}$. Aus diesen Gleichungen wiederum ergeben sich die Kongruenzen $a + b \equiv c + d \bmod n$ und $ab \equiv cd \bmod n$.

zu (ii) Nach Definition ist $a \equiv b \bmod n$ äquivalent dazu, dass $n|(b-a)$ gilt. Es existiert also ein $k \in \mathbb{Z}$ mit $b-a = nk$. Wegen $m \mid n$ gilt außerdem $n = dm$ für ein $d \in \mathbb{N}$. Es folgt $b \equiv a + nk \equiv a + dmk \equiv a \bmod m$.

zu (iii) Für jedes $a \in \mathbb{Z}$ gilt die Äquivalenz

$$a \equiv b \bmod n \quad \Leftrightarrow \quad n \mid (b-a) \quad \Leftrightarrow \quad \exists\, k \in \mathbb{Z} : nk = b-a \quad \Leftrightarrow \quad \exists\, k \in \mathbb{Z} : mnk = mb - ma$$
$$\Leftrightarrow \quad (mn) \mid (mb - ma) \quad \Leftrightarrow \quad ma \equiv mb \equiv mn.$$

zu (iv) Sei $a \in \mathbb{Z}$, und setzen wir zunächst $p \nmid a$ voraus. Dann ist $\bar{a} = a + p\mathbb{Z}$ im Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ein Element ungleich null. Weil p eine Primzahl ist, ist dieser Restklassenring nach Satz 11.7 ein Körper und $\bar{a}$ somit in $(\mathbb{Z}/p\mathbb{Z})^\times$ enthalten. Die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ besteht aus $p-1$ Elementen. Nach dem Satz von Lagrange ist die Ordnung der Untergruppe $\langle \bar{a} \rangle$ von $(\mathbb{Z}/p\mathbb{Z})^\times$, also die Elementordnung $\mathrm{ord}(\bar{a})$, ein Teiler von $p-1$. Es folgt $a^{p-1} + p\mathbb{Z} = (a+p\mathbb{Z})^{p-1} = \bar{a}^{p-1} = \bar{1} = 1 + p\mathbb{Z}$ und somit auch $a^{p-1} \equiv 1 \bmod p$.

Mit Teil (i) erhalten wir auch die Kongruenz $a^p \equiv a^{p-1} \cdot a \equiv 1 \cdot a \equiv a \bmod p$. Ist p ein Teiler von a, dann gilt auch $p \mid a^p$, und es folgt $a^p \equiv 0 \equiv a \bmod p$. Insgesamt ist die Kongruenz $a^p \equiv a \bmod p$ also für alle $a \in \mathbb{Z}$ erfüllt. □

Das Hauptziel dieses Kapitels ist die Herleitung des Chinesischen Restsatzes, eines wichtigen Hilfsmittels bei der Lösung von Kongruenzen. Zur Vorbereitung wird das Konzept der Teilerfremdheit von Ringelementen auf Ideale ausgedehnt.

Definition 14.2 Sei R ein Ring. Zwei Ideale I, J in R werden ***teilerfremd*** genannt, wenn $I + J = (1)$ gilt, wobei (1) wie üblich das Einheitsideal in R bezeichnet.

Diese Bezeichnung wird durch das folgende Lemma gerechtfertigt.

Lemma 14.3 Sei $R = \mathbb{Z}$, und seien $m, n \in \mathbb{N}$. Genau dann sind die Ideale $I = (m)$ und $J = (n)$ teilerfremd, wenn m, n als natürliche Zahlen teilerfremd sind.

Beweis: Sind m und n teilerfremd, dann gibt es nach dem Lemma von Bézout $a, b \in \mathbb{Z}$ mit $am + bn = 1$. Es folgt $1 \in (m) + (n) = I + J$, also $I + J = (1)$. Setzen wir umgekehrt $I + J = (1)$ voraus. Dann liegt 1 in $I + J$, es gibt also $a, b \in \mathbb{Z}$ mit $1 = am + bn$. Ist d ein gemeinsamer Teiler von m und n, dann teilt d auf Grund der Gleichung auch 1. Dies zeigt, dass m und n teilerfremd sind. □

Lemma 14.4 Sei R ein Ring, und seien $I_1, \ldots, I_m, J$ Ideale in R, wobei $I_1, \ldots, I_m$ jeweils teilerfremd zu J sind. Dann ist auch das Produkt $I_1 \cdot \ldots \cdot I_m$ teilerfremd zu J.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über m. Sei zunächst $m = 2$. Dann ist die Gleichung $I_1 I_2 + J = (1)$ zu zeigen. Nun gilt

$$(1) \quad = \quad (1)(1) \quad = \quad (I_1 + J)(I_2 + J) \quad = \quad I_1 I_2 + J I_2 + I_1 J + JJ \quad \subseteq \quad I_1 I_2 + J$$

und somit $I_1 I_2 + J = (1)$. Sei nun die Behauptung für m bereits bewiesen, und seien $I_1, \ldots, I_{m+1}, J$ Ideale, welche die Voraussetzung des Lemmas erfüllen. Nach Induktionsannahme sind die Ideale $I = I_1 \cdot \ldots \cdot I_m$ und I_{m+1} beide teilerfremd zu J. Auf Grund des bereits bewiesenen Falls $m = 2$ ist auch $I I_{m+1} = I_1 \cdot \ldots \cdot I_m \cdot I_{m+1}$ teilerfremd zu J. □

Lemma 14.5 Sei R ein Ring, und seien $I_1, ..., I_m$ Ideale in R, die paarweise teilerfremd sind. Dann gilt $I_1 \cdot ... \cdot I_m = I_1 \cap ... \cap I_m$.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über R und beginnen mit dem Fall $m = 2$. Nach Lemma 10.16 gilt $I_1 I_2 \subseteq I_1$ und $I_1 I_2 \subseteq I_2$, insgesamt also $I_1 I_2 \subseteq I_1 \cap I_2$. Sei nun umgekehrt $r \in I_1 \cap I_2$ vorgegeben. Wegen $I_1 + I_2 = (1)$ gibt es Elemente $a_1 \in I_1$ und $a_2 \in I_2$ mit $a_1 + a_2 = 1$. Es folgt

$$r \quad = \quad r \cdot 1 \quad = \quad r(a_1 + a_2) \quad = \quad ra_1 + ra_2.$$

Die Elemente ra_1 und ra_2 liegen beide in $I_1 I_2$, also gilt dasselbe auch für die Summe. Sei nun die Behauptung für m bereits bewiesen, und seien $I_1, ..., I_{m+1}$ paarweise teilerfremde Ideale. Sei $J = I_1 \cdot ... \cdot I_m$. Nach Lemma 14.4 sind J und I_{m+1} teierfremd. Die Induktionsvoraussetzung liefert also

$$(I_1 \cap ... \cap I_m) \cap I_{m+1} \quad = \quad J \cap I_{m+1} \quad = \quad J I_{m+1} \quad = \quad I_1 \cdot ... \cdot I_m \cdot I_{m+1}. \qquad \square$$

Man beachte, dass die paarweise Teilerfremdheit eine wesentliche Voraussetzung für die Gültigkeit des Lemmas ist. Ist beispielweise $R = \mathbb{Z}$, $I = (2)$ und $J = (6)$, dann gilt $IJ = (12)$, aber aus Satz 10.12 (iii) folgt $I \cap J = (6)$, wegen $\text{kgV}(2, 6) = 6$.

Satz 14.6 *(Chinesischer Restsatz)*

Sei R ein Ring, $I_1, ..., I_m$ paarweise teilerfremde Ideale in R und $I = I_1 \cdot ... \cdot I_m$ Dann gibt es einen Isomorphismus von Ringen

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times ... \times (R/I_m) \qquad \text{mit} \quad \bar{\phi}(a + I) = (a + I_1, ..., a + I_m) \quad \text{für alle} \quad a \in R.$$

Beweis: Sei $\phi : R \to (R/I_1) \times ... \times (R/I_m)$ gegeben durch $\phi(a) = (a + I_1, ..., a + I_m)$. Nach Lemma 14.5 gilt $I = I_1 \cap ... \cap I_m$. Ein Element $a \in R$ liegt genau dann im Kern von ϕ, wenn $a + I_k = I_k \Leftrightarrow a \in I_k$ für $1 \leq k \leq m$ gilt. Dies wiederum ist äquivalent zu $a \in I$. Es gilt also $I = \ker(\phi)$. Nach Proposition 11.8 gibt es einen Homomorphismus

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times ... \times (R/I_m)$$

mit $\bar{\phi}(a + I) = (a + I_1, ..., a + I_m)$, und auf Grund des Homomorphiesatzes für Ringe ist $\bar{\phi}$ ein Isomorphismus, wenn ϕ surjektiv ist. Dies beweisen wir nun durch vollständige Induktion über m.

Sei zunächst $m = 2$ und $(a_1 + I_1, a_2 + I_2) \in (R/I_1) \times (R/I_2)$ vorgegeben. Weil I_1 und I_2 teilerfremd sind, gibt es Elemente $s_1 \in I_1$, $s_2 \in I_2$ mit $s_1 + s_2 = 1$. Es gilt dann $s_1 + I_1 = I_1$, $s_1 + I_2 = (1 - s_2) + I_2 = 1 + I_2$, $s_2 + I_1 = (1 - s_1) + I_1 = 1 + I_1$ und $s_2 + I_2 = I_2$. Bilden wir nun das Element $a = s_2 a_1 + s_1 a_2$, dann folgt

$$a + I_1 \quad = \quad (s_2 + I_1)(a_1 + I_1) + (s_1 + I_1)(a_2 + I_2) \quad = \quad (1 + I_1)(a_1 + I_1) + (0 + I_1)(a_2 + I_1) \quad = \quad a_1 + I_1$$

und ebenso

$$a + I_2 \quad = \quad (s_2 + I_2)(a_1 + I_2) + (s_1 + I_2)(a_2 + I_2) \quad = \quad (0 + I_2)(a_1 + I_2) + (1 + I_2)(a_2 + I_2) \quad = \quad a_2 + I_2$$

insgesamt also $\phi(a) = (a + I_1, a + I_2) = (a_1 + I_1, a_2 + I_2)$. Sei nun $m \in \mathbb{N}$, und setzen wir die Aussage für dieses m voraus. Seien $I_1, ..., I_{m+1}$ teilerfremde Ideale und das Element

$$(a_1 + I_1, ..., a_m + I_m, a_{m+1} + I_{m+1}) \quad \in \quad (R/I_1) \times ... \times (R/I_m) \times (R/I_{m+1})$$

vorgegeben. Nach Induktionsvoraussetzung finden wir ein Element $a' \in R$ mit $a' + I_k = a_k + I_k$ für $1 \leq k \leq m$. Die Ideale $J = I_1 \cdot ... \cdot I_m$ und I_{m+1} sind nach Lemma 14.4 teilerfremd. Wiederum auf Grund der Induktionsvoraussetzung finden wir ein $a \in R$ mit $a + J = a' + J$ und $a + I_{m+1} = a_{m+1} + I_{m+1}$. Die Gleichung $a + J = a' + J$ ist äquivalent zu $a - a' \in J$, und aus $J \subseteq I_k$ für $1 \leq k \leq m$ folgt $a - a' \in I_k$, also $a + I_k = a' + I_k = a_k + I_k$ für $1 \leq k \leq m$. Insgesamt gilt also $a + I_k = a_k + I_k$ für $1 \leq k \leq m + 1$ und $\phi(a) = (a_1 + I_1, ..., a_{m+1} + I_{m+1})$. □

Für die Kongruenzrechnung ergibt sich das dem Chinesischen Restsatz das folgende Resultat.

Satz 14.7 Seien $r \in \mathbb{N}$ mit $r \geq 2$, außerdem $n_1, ..., n_r \in \mathbb{N}$ paarweise teilerfremde natürliche Zahlen und $n = \prod_{j=1}^{r} n_j$. Seien $c_1, ..., c_r \in \mathbb{Z}$. Dann ist die Lösungsmenge $\mathcal{L} \subseteq \mathbb{Z}$ des Kongruenzsystems

$$x \equiv c_1 \bmod n_1 \quad , \quad x \equiv c_2 \bmod n_2 \quad , \quad ... \quad , \quad x \equiv c_r \bmod n_r$$

nicht leer. Ist $a \in \mathcal{L}$ beliebig gewählt, dann gilt $\mathcal{L} = a + n\mathbb{Z}$.

Beweis: Auf Grund des Chinesischen Restsatzes existiert ein Isomorphismus $\bar{\phi} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$ von Ringen mit $\bar{\phi}(c + n\mathbb{Z}) = (c + n_1\mathbb{Z}, ..., c + n_r\mathbb{Z})$ für alle $c \in \mathbb{Z}$. Für jedes $c \in \mathbb{Z}$ gilt die Äquivalenz

$$\begin{aligned} &c \in \mathcal{L} \quad \Leftrightarrow \quad c \equiv c_k \bmod n_k \text{ für } 1 \leq k \leq r \quad \Leftrightarrow \quad c + n_k\mathbb{Z} = c_k + n_k\mathbb{Z} \text{ für } 1 \leq k \leq r \quad \Leftrightarrow \\ &(c + n_1\mathbb{Z}, ..., c + n_r\mathbb{Z}) = (c_1 + n_1\mathbb{Z}, ..., c_r + n_r\mathbb{Z}) \quad \Leftrightarrow \quad \bar{\phi}(c + n\mathbb{Z}) = (c_1 + n_1\mathbb{Z}, ..., c_r + n_r\mathbb{Z}). \end{aligned}$$

Weil $\bar{\phi}$ surjektiv ist, besitzt insbesondere das Element $(c_1 + n_1\mathbb{Z}, ..., c_r + n_r\mathbb{Z})$ der Menge $\mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$ ein Urbild. Die Äquivalenz zeigt somit, dass die Lösungsmenge $\mathcal{L}$ nicht leer ist. Sei nun $a \in \mathcal{L}$ beliebig gewählt. Dann gilt für alle $c \in \mathbb{Z}$ auf Grund der Bijektivität von $\bar{\phi}$ die Äquivalenz

$$c \in \mathcal{L} \quad \Leftrightarrow \quad \bar{\phi}(c + n\mathbb{Z}) = (c_1 + n_1\mathbb{Z}, ..., c_r + n_r\mathbb{Z}) = \phi(a + n\mathbb{Z}) \quad \Leftrightarrow \quad c + n\mathbb{Z} = a + n\mathbb{Z} \quad \Leftrightarrow \quad c \in a + n\mathbb{Z}.$$

Damit ist die Gleichung $\mathcal{L} = a + n\mathbb{Z}$ bewiesen. □

Die Bestimmung einer Lösungsmenge $\mathcal{L}$ eines Kongruenzsystems wie im Satz reduziert sich also auf die Bestimmung einer einzelnen Lösung. Ist das Produkt n klein, dann lässt sich eine solche Lösung am einfachsten dadurch bestimmen, dass man sie aus der Menge $\{0, 1, ..., n-1\}$ durch sukzessive Anwendung der einzelnen Kongruenzen „herausfiltert“. Als konkretes Beispiel betrachten wir das System

$$x \equiv 0 \bmod 2 \quad , \quad x \equiv 2 \bmod 3 \quad , \quad x \equiv 4 \bmod 5.$$

Da es sich bei 2, 3 und 5 um verschiedene Primzahlen handelt, sind die Zahlen insbesondere paarweise teilfremd, und ihr Produkt ist $n = 2 \cdot 3 \cdot 5 = 30$. Die einzigen Zahlen in der Menge $\{0, 1, ..., 29\}$, die die letzte der drei Kongruenzen erfüllen, sind $4, 9, 14, 19, 24, 29$. Unter diese Zahlen erfüllen nur 14 und 29 auch die zweite Kongruenz, und nur 14 auch die erste. Auf Grund des Satzes ist die Lösungsmenge des Systems also durch $\mathcal{L} = 14 + 30\mathbb{Z}$ gegeben.

Ist das Produkt n dagegen groß, dann kommt man durch Anwendung des Euklidischen Algorithmus schneller ans Ziel. Zunächst bemerken wir, dass die Bestimmung einer Lösung für ein System aus r Kongruenzen mit $r > 2$ leicht auf den Fall $r = 2$ zurückgeführt werden kann. Dazu betrachtet man die teilerfremden Zahlen n_1 und $m = n_2 \cdot \ldots \cdot n_r$. Wir setzen voraus, dass b eine Lösung des Systems bestehend aus den $r-1$ Kongruenzen $x \equiv c_j \bmod n_j$ mit $2 \leq j \leq r$ ist. Außerdem sei a eine Lösung des Systems

$$x \equiv c_1 \bmod n_1 \quad , \quad x \equiv b \bmod m.$$

Dann ist a auch eine Lösung des ursprünglichen, r-elementigen Systems. Denn nach Definition ist a zunächst eine Lösung der ersten Kongruenz. Wegen $a \equiv b \bmod m$ gilt außerdem $m \mid (b-a)$, und wegen $n_j \mid m$ auch $n_j \mid (b-a)$, für $2 \leq j \leq r$. Dies wiederum ist äquivalent zu $a \equiv b \equiv c_j \bmod n_j$ für $2 \leq j \leq r$.

Wir können uns also auf die Bestimmung einer Lösung im Fall $r = 2$ konzentrieren. Seien $m, n \in \mathbb{N}$ teilerfremd und $c, d \in \mathbb{Z}$. Gesucht wird eine Lösung des Systems $x \equiv c \bmod m$, $x \equiv d \bmod n$. Hierzu führt man die folgenden Einzelschritte aus.

(1) Bestimme mit Hilfe des Euklidischen Algorithmus Zahlen $u, v \in \mathbb{Z}$ mit $um + vn = \mathrm{ggT}(m, n) = 1$.

(2) Berechne $a_1 = 1 - um$ und $a_2 = 1 - a_1$. (Dann gilt offenbar $a_1 \equiv 1 - 0 \equiv 1 \bmod m$, $a_1 \equiv vn \equiv 0 \bmod n$ und ebenso $a_2 \equiv 1 - (1 - um) \equiv um \equiv 0 \bmod m$ und $a_2 \equiv 1 - (1 - um) \equiv 1 - vn \equiv 1 \bmod n$.)

(3) Setze $a = ca_1 + da_2$. (Dann erhalten wir $a \equiv c \cdot 1 + d \cdot 0 \equiv c \bmod m$ und $b \equiv c \cdot 0 + d \cdot 1 \equiv d \bmod n$. Also ist a eine Lösung des Systems.)

Als konkretes Beispiel betrachten wir das System

$$x \equiv 15 \bmod 59 \quad , \quad x \equiv 20 \bmod 73.$$

Da 59 und 73 Primzahlen sind, gilt $\mathrm{ggT}(59, 73) = 1$, außerdem ist $59 \cdot 73 = 4307$. Mit Hilfe des Euklidischen Algorithmus finden wir für die Gleichung $59u + 73v = 1$ die Lösung $(u, v) = (26, -21)$. Gemäß Schritt (2) berechnen wir $a_1 = 1 - 59u = 1 - 59 \cdot 26 = -1533$ und $a_2 = 1 - a_1 = 1534$. Wie in Schritt (3) erhalten wir durch $a = 15a_1 + 20a_2 = 7685$ eine Lösung des Systems. Die Lösungsmenge des Systems ist also nach Satz 14.7 gegeben durch $\mathcal{L} = 7685 + 4307\mathbb{Z}$. Der eindeutig bestimmte Repräsentant der Nebenklasse $7685 + 4307\mathbb{Z}$ in $\{0, 1, \ldots, 4306\}$ ist 3378. Also kann die Lösungsmenge auch in der Form $\mathcal{L} = 3378 + 4307\mathbb{Z}$ angeschrieben werden.

Als Ergänzung bemerken wir noch, dass der Fall, dass die Zahlen $n_1, \ldots, n_r \in \mathbb{N}$ nicht paarweise teilerfremd sind, auf den teilerfremden Fall zurückgeführt werden kann. Der Einfachheit halber formulieren wir die allgemeine Aussage nur für den Fall $r = 2$.

Satz 14.8 Seien $m, n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Wir betrachten die Lösungsmenge $\mathcal{L} \subseteq \mathbb{Z}$ des Kongruenzsystems

$$x \equiv a \bmod m \quad , \quad x \equiv b \bmod n.$$

(i) Es gilt $\mathcal{L} \neq \emptyset$ genau dann, wenn $a \equiv b \bmod d$ erfüllt ist, mit $d = \mathrm{ggT}(m, n)$.

(ii) Sei $\ell \in \mathbb{Z}$ mit $b = a + \ell d$, außerdem $m' = \frac{m}{d}$ und $n' = \frac{n}{d}$. Sei c eine Lösung des Systems $x \equiv 0 \bmod m'$, $x \equiv \ell \bmod n'$. Dann ist die Lösungsmenge des ursprünglichen Systems gegeben durch $\mathcal{L} = a + dc + \mathrm{kgV}(m, n)\mathbb{Z}$.

Beweis: Zur Vorbereitung bemerken wir: Ist $u \in \mathbb{Z}$ eine Lösung des Kongruenzsystems, dann ist die Lösungsmenge des gesamten Systems gegeben durch $u + \mathrm{kgV}(m,n)\mathbb{Z}$. Ist nämlich $v \in \mathbb{Z}$ eine weitere Lösung, dann gilt $u \equiv a \equiv v \bmod m$ und $u \equiv b \equiv v \bmod n$. Die Differenz $v-u$ ist also eine gemeinsames Vielfaches von m und n, und somit ein Vielfaches von $\mathrm{kgV}(m,n)$. Daraus folgt $v \in u + \mathrm{kgV}(m,n)\mathbb{Z}$. Setzen wir umgekehrt $v \in u + \mathrm{kgV}(m,n)\mathbb{Z}$ voraus, dann ist $v-u$ ein gemeinsames Vielfaches von m und n. Es folgt $v \equiv u \equiv a \bmod m$ und $v \equiv u \equiv b \bmod n$, und somit $v \in \mathcal{L}$.

zu (ii) Auf Grund der Vorbereitung genügt es zu überprüfen, dass $a + dc$ eine Lösung des Systems ist. Nach Voraussetzung gilt $m' \mid c$ und $c \equiv \ell \bmod n'$. Es existieren also $u, v \in \mathbb{Z}$ mit $c = um'$ und $c - \ell = vn'$. Zu zeigen ist, dass $a + dc$ in $\mathcal{L}$ enthalten ist, also eine Lösung des ursprünglichen Kongruenzsystems darstellt. Tatsächlich gilt

$$a + dc \;\equiv\; a + dum' \;\equiv\; a + um \;\equiv\; a \bmod m$$

und ebenso

$$a + dc \;\equiv\; a + d(\ell + vn') \;\equiv\; (a + \ell d) + dvn' \;\equiv\; b + vn \;\equiv\; b \bmod n.$$

zu (i) „⇒“ Sei $c \in \mathcal{L}$ beliebig gewählt. Dann folgt $c \equiv a \bmod m$ und $c \equiv b \bmod n$, wegen $d \mid m$ und $d \mid n$ also auch $a \equiv c \equiv b \bmod d$. „⇐“ Dies folgt direkt aus Teil (ii), denn auf Grund der Voraussetzung $a \equiv b \bmod d$ existiert ein $\ell \in \mathbb{Z}$ mit $b = a + \ell d$, und offenbar ist $a + dc + \mathrm{kgV}(m,n)\mathbb{Z}$ mit dem in (ii) beschriebenen $c \in \mathbb{Z}$ eine nichtleere Menge. □

Bei Teil (ii) von Satz 14.8 beachte man, dass die Zahlen $m', n' \in \mathbb{N}$ teilerfremd sind und somit die Bestimmung einer Lösung dieses Systems mit dem zuvor behandelten Rechenverfahren möglich ist.

Eine weitere Anwendung des Chinesischen Restsatzes besteht in der Lösung von Polynomgleichungen in Restklassenringen.

Satz 14.9 Seien $m, n \in \mathbb{N}$ teilerfremd und $f \in \mathbb{Z}[x]$. Es bezeichne $\mathcal{N}$ die Menge der Nullstellen von f in $\mathbb{Z}/(mn)\mathbb{Z}$, und $\mathcal{N}_m$ bzw. $\mathcal{N}_n$ die Menge der Nullstellen von f in $\mathbb{Z}/m\mathbb{Z}$ bzw. $\mathbb{Z}/n\mathbb{Z}$. Dann existiert eine Bijektion $\psi : \mathcal{N} \to \mathcal{N}_m \times \mathcal{N}_n$ mit $\psi(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$ für alle $a \in \mathbb{Z}$ mit $a + mn\mathbb{Z} \in \mathcal{N}$.

Beweis: Weil es sich bei $\bar{\phi}$ um einen Ringhomomorphismus handelt, gilt $f(\bar{\phi}(\bar{a})) = \bar{\phi}(f(\bar{a}))$ für alle $\bar{a} \in \mathbb{Z}/(mn)\mathbb{Z}$. Stellen wir nämlich f in der Form $f = \sum_{k=0}^{d} a_k x^k$ mit $d \in \mathbb{N}$ und $a_k \in \mathbb{Z}$ für $0 \le k \le d$ dar, dann gilt auf Grund der Homomorphismus-Eigenschaft jeweils

$$f(\bar{\phi}(\bar{a})) \;=\; \sum_{k=0}^{d} a_k \bar{\phi}(\bar{a})^k \;=\; \sum_{k=0}^{d} \bar{\phi}(a_k \cdot \bar{a}^k) \;=\; \bar{\phi}\left(\sum_{k=0}^{d} a_k \bar{a}^k\right) \;=\; \bar{\phi}(f(\bar{a})).$$

Dies zeigt, dass durch die eingeschränkte Abbildung $\psi = \bar{\phi}|_{\mathcal{N}}$ jedenfalls eine Abbildung $\mathcal{N} \to \mathcal{N}_m \times \mathcal{N}_n$ gegeben ist, denn für alle $\bar{a} \in \mathcal{N}$ und $(\bar{b}, \bar{c}) = \psi(\bar{a})$ gilt jeweils

$$(f(\bar{b}), f(\bar{c})) \;=\; f(\bar{b}, \bar{c}) \;=\; f(\psi(\bar{a})) \;=\; f(\bar{\phi}(\bar{a})) \;=\; \phi(f(\bar{a})) \;=\; \phi(\bar{0}) \;=\; (\bar{0}, \bar{0})$$

und somit $(\bar{b}, \bar{c}) \in \mathcal{N}_m \times \mathcal{N}_n$. Nach Definition gilt außerdem $\psi(a + mn\mathbb{Z}) = \bar{\phi}(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$ für alle $a \in \mathbb{Z}$ mit $a + mn\mathbb{Z} \in \mathcal{N}$.

Als Einschränkung einer injektiven Abbildung ist auch ψ injektiv. Zum Nachweis der Surjektivität sei $(\bar{b},\bar{c}) \in \mathcal{N}_m \times \mathcal{N}_n$ vorgegeben. Sei $\bar{a} \in \mathbb{Z}/(mn)\mathbb{Z}$ das eindeutig bestimmte Element mit $\bar{\phi}(\bar{a}) = (\bar{b},\bar{c})$. Wegen $\phi(f(\bar{a})) = f(\phi(\bar{a})) = f(\bar{b},\bar{c}) = (f(\bar{b}), f(\bar{c})) = (\bar{0},\bar{0})$ und der Injektivität folgt $f(\bar{a}) = \bar{0}$, also $\bar{a} \in \mathcal{N}$ und $\psi(\bar{a}) = \bar{\phi}(\bar{a}) = (\bar{b},\bar{c})$. Damit ist die Surjektivität von ψ nachgewiesen. □

Als konkretes Beispiel für die Aussage des Satzes bestimmen wir die Nullstellen des Polynoms $f = x^2 - x \in \mathbb{Z}[x]$ im Restklassenring $\mathbb{Z}/35\mathbb{Z}$. Sei $\bar{\phi} : \mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ der Isomorphismus aus dem Chinesischen Restsatz. Da 5 und 7 Primzahlen sind, handelt es sich bei $\mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/7\mathbb{Z}$ nach Satz 11.7 um Körper. In beiden Körpern sind $\bar{0}$ und $\bar{1}$ offenbar Nullstellen von f, und da ein Polynom vom Grad 2 über einem Körper nach Folgerung 12.5 (ii) nicht mehr als zwei Nullstellen besitzt, sind es die einzigen. Somit ist

$$\mathcal{N}_5 \times \mathcal{N}_7 \quad = \quad \{\, (0+5\mathbb{Z}, 0+7\mathbb{Z}) \,,\, (0+5\mathbb{Z}, 1+7\mathbb{Z}) \,,\, (1+5\mathbb{Z}, 0+7\mathbb{Z}) \,,\, (1+5\mathbb{Z}, 1+7\mathbb{Z}) \,\}\,.$$

Nach Satz 14.9 sind die Nullstellen von f in $\mathbb{Z}/35\mathbb{Z}$ genau die Urbilder von $\mathcal{N}_5 \times \mathcal{N}_7$ unter dem Isomorphismus $\bar{\phi}$. Offenbar ist $\bar{0} = 0 + 35\mathbb{Z}$ das Urbild von $(0+5\mathbb{Z}, 0+7\mathbb{Z})$, und $\bar{1} = 1 + 35\mathbb{Z}$ ist das Urbild von $(1+5\mathbb{Z}, 1+7\mathbb{Z})$. Die eindeutig bestimmte Lösung des Kongruenzsystems $x \equiv 0 \bmod 5$, $x \equiv 1 \bmod 7$ in $\{0, 1, ..., 34\}$ ist 15. Also ist $\overline{15}$ das Urbild von $(0+5\mathbb{Z}, 1+7\mathbb{Z})$. Genauso findet man das Urbild $\overline{21}$ von $(1+5\mathbb{Z}, 0+7\mathbb{Z})$. Insgesamt ist $\mathcal{N} = \{\bar{0}, \bar{1}, \overline{15}, \overline{21}\}$ also die Nullstellenmenge von f in $\mathbb{Z}/35\mathbb{Z}$.

Als weitere Anwendung des Chinesischen Restsatzes bestimmen wir die Struktur der in § 4 eingeführten primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$. Dabei handelt es sich um endliche abelsche Gruppen. Aus § 8 wissen wir bereits, dass solche Gruppen also direkte Produkte endlicher zyklischer Gruppen darstellbar sind. Unser Ziel besteht darin, eine solche Darstellung von $(\mathbb{Z}/n\mathbb{Z})^\times$ für jedes $n \in \mathbb{N}$ explizit anzugeben.

Lemma 14.10 Seien R und S Ringe. Dann gilt

(i) $(R \times S)^\times = R^\times \times S^\times$

(ii) Ist $\phi : R \to S$ ein Isomorphismus von Ringen, dann gilt $\phi(R^\times) = S^\times$. Insbesondere sind die Einheitengruppen $R^\times$ und $S^\times$ also isomorph.

Beweis: zu (i) „$\subseteq$“ Das Einselement des Rings $R \times S$ ist $(1_R, 1_S)$. Ist $(a,b) \in (R \times S)^\times$, dann gibt es nach Definition ein Paar $(c,d) \in R \times S$ mit $(ac, bd) = (a,b)(c,d) = (1_R, 1_S)$. Es gilt also $ac = 1_R$, $bd = 1_S$ und damit $a \in R^\times$, $b \in S^\times$. „$\supseteq$“ Sei $(a,b) \in R^\times \times S^\times$. Dann gibt es Elememte $c \in R$ und $d \in S$ mit $ac = 1_R$ und $bd = 1_S$. Insgesamt erhalten wir $(a,b)(c,d) = (ac, bd) = (1_R, 1_S) = 1_{R\times S}$, also $(a,b) \in (R \times S)^\times$.

zu (ii) Wir beweisen zunächst die Inklusion $\phi(R^\times) \subseteq S^\times$. Sei $a \in \phi(R^\times)$. Dann gibt es ein $b \in R^\times$ mit $\phi(b) = a$. Weil b eine Einheit ist, existiert ein $c \in R^\times$ mit $bc = 1_R$, und es folgt $a\phi(c) = \phi(b)\phi(c) = \phi(bc) = \phi(1_R) = 1_S$. Dies zeigt, dass a eine Einheit in S ist. Wir können nun dasselbe Argument auf den Ringhomomorphismus ϕ^{-1} anwenden und erhalten $\phi^{-1}(S^\times) \subseteq R^\times$. Anwendung von ϕ auf beide Seiten liefert $S^\times \subseteq \phi(R^\times)$. Insgesamt gilt also $\phi(R^\times) = S^\times$. □

Wir erinnern daran, dass die Ordnung der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ gleich $\varphi(n)$ ist, wobei φ die in § 3 definierte Eulersche φ-Funktion bezeichnet. Dort hatten wir bereits (ohne Begründung) die Rechenregeln $\varphi(mn) = \varphi(m)\varphi(n)$ für teilerfremde $m, n \in \mathbb{N}$ und $\varphi(p^r) = p^{r-1}(p-1)$ für $r \in \mathbb{N}$ und Primzahlen p angegeben. Die zweite Gleichung kommt folgendermaßen zu Stande: Nach Definition ist $\varphi(p^r)$ die Anzahl der ganzen Zahlen a mit $0 \le a \le p^r - 1$. Die einzigen Zahlen in diesem Bereich, die *nicht* teilerfremd zu p^r sind, sind die Vielfachen von p, und die Anzahl dieser Vielfachen beträgt p^{r-1}. Es bleiben also genau $p^{r-1}(p-1) = p^r - p^{r-1}$ Zahlen übrig.

Die erste Gleichung kann man einfacher beweisen, indem man die Ringtheorie zur Hilfe nimmt.

Proposition 14.11 Sind m, n teilerfremd und $m, n \geq 2$. Dann gilt für die Eulersche φ-Funktion die Rechenregel $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis: Auf Grund des Chinesischen Restsatzes und Lemma 14.10 gilt

$$(\mathbb{Z}/mn\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Die Menge links enthält $\varphi(mn)$, die Menge rechts $\varphi(m)\varphi(n)$ Elemente. □

Für die weiteren Ausführungen benötigen wir einen neuen Begriff aus der Gruppentheorie. Der ***Exponent*** $\exp(G)$ einer Gruppe G ist die kleinste Zahl $n \in \mathbb{N}$ mit der Eigenschaft $g^n = e$ für alle $g \in G$. Existiert keine natürliche Zahl mit dieser Eigenschaft, dann setzt man $\exp(G) = +\infty$. Ist G eine endliche Gruppe, dann nimmt der Exponent stets einen endlichen Wert an.

Man überzeugt sich leicht davon, dass die Exponenten der symmetrischen Gruppen S_3 und S_4 durch $\exp(S_3) = 6$ und $\exp(S_4) = 12$ gegeben sind. In S_3 gibt es aber kein Element der Ordnung 6, und ebensowenig in S_4 ein Element der Ordnung 12. Für endliche abelsche Gruppen gilt dagegen

Proposition 14.12 Sei G eine endliche abelsche Gruppe vom Exponenten m. Dann existiert in G ein Element der Ordnung m.

Beweis: Nach § 8 ist G als endliche abelsche Gruppe isomorph zu einem direkten Produkt endlicher zyklischer Gruppen ist. Es gibt also $m_1, ..., m_r \in \mathbb{N}$ mit $G \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$. Der Einfachheit halber können wir annehmen, dass G zu dem Produkt auf der rechten Seite nicht nur isomorph ist, sondern damit übereinstimmt. Sei nun m der Exponent von G. Wir zeigen, dass m mit $\ell = \text{kgV}(m_1, ..., m_r)$ übereinstimmt. Nach Definition des Exponenten gilt $mg = 0_G$ für $g \in G$. Insbesondere gilt

$$m(1 + m_1\mathbb{Z}, ..., 1 + m_r\mathbb{Z}) = 0_G \quad \Leftrightarrow \quad (m + m_1\mathbb{Z}, ..., m + m_r\mathbb{Z}) = (m_1\mathbb{Z}, ..., m_r\mathbb{Z}) \quad \Leftrightarrow$$
$$m + m_k\mathbb{Z} = m_k\mathbb{Z} \text{ für } 1 \leq k \leq r \quad \Leftrightarrow \quad m_k | m \text{ für } 1 \leq k \leq r.$$

Also ist m jedenfalls ein gemeinsames Vielfaches von $m_1, ..., m_r$ und damit auch ein Vielfaches von ℓ. Weil ℓ ein Vielfaches von $m_1, ..., m_r$ ist, gilt andererseits für alle $a_1, ..., a_r \in \mathbb{Z}$ und $1 \leq k \leq r$ jeweils $m_k | (\ell a_k)$, also $\ell a_k + m_k\mathbb{Z} = m_k\mathbb{Z}$ und somit

$$\ell(a_1 + m_1\mathbb{Z}, ..., a_r + m_r\mathbb{Z}) \quad = \quad (\ell a_1 + m_1\mathbb{Z}, ..., \ell a_r + m_r\mathbb{Z}) \quad = \quad (m_1\mathbb{Z}, ..., m_r\mathbb{Z}) \quad = \quad 0_G.$$

Nach Definition des Exponenten folgt daraus $\ell \geq m$. Aus $\ell | m$ und $\ell \geq m$ folgt $\ell = m$. Die Rechung von oben zeigt darüber hinaus, dass $(1 + m_1\mathbb{Z}, ..., 1 + m_r\mathbb{Z})$ ein Element der maximalen Ordnung m ist. □

Satz 14.13 Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist U zyklisch. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers immer eine zyklische Gruppe.

Beweis: Sei $n = |U|$ und d der Exponent von U. Nach dem Satz von Lagrange ist $\mathrm{ord}(a)$ für jedes $a \in U$ jeweils ein Teiler von n, also gilt $a^n = 1$ für alle $a \in U$. Dies zeigt, dass $d \leq n$ gilt. Andererseits gilt nach Definition des Exponenten auch $a^d = 1$ für alle $a \in U$. Damit sind alle Elemente aus U Nullstellen des Polynoms $f = x^d - 1 \in K[x]$. Aber ein Polynom vom Grad d über einem Körper kann nach Folgerung 12.5 höchstens d Nullstellen besitzen. Daraus folgt $n \leq d$, insgesamt $n = d$. Nach Proposition 14.12 gibt es in U ein Element der Ordnung n. Also ist U zyklisch. □

Folgerung 14.14 Ist p eine Primzahl, dann gilt $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Beweis: Wie wir bereits festgestellt haben, gilt $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p-1$. Außerdem ist $(\mathbb{Z}/p\mathbb{Z})^\times$ nach Satz 14.13 zyklisch, damit isomorph zu $\mathbb{Z}/(p-1)\mathbb{Z}$. □

Mit den bisherigen Ergebnissen können wir die Struktur der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ bereits in vielen Fällen bestimmen. Beispielsweise gilt

$$(\mathbb{Z}/15\mathbb{Z})^\times \quad \cong \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

und somit insbesondere $\varphi(15) = 8$. Denn nach dem Chinesischen Restsatz und Lemma 14.10 existiert ein Isomorphismus $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. Außerdem gilt $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ nach Folgerung 14.14.

Eine Zahl $a \in \mathbb{Z}$ mit der Eigenschaft $(\mathbb{Z}/p\mathbb{Z})^\times = \langle a + p\mathbb{Z} \rangle$ wird ***Primitivwurzel modulo*** p genannt. Es ist zwar keine Formel bekannt, mit der sich ein solches a bestimmen lässt, aber man kann folgenden Satz aus der Gruppentheorie zur Hilfe nehmen, um es zu finden: Ist G eine zyklische Gruppe der Ordnung n und gilt $g^{\frac{n}{p}} \neq e_G$ für alle Primteiler p von n, dann ist g ein erzeugendes Element, es gilt also $G = \langle g \rangle$.

Beispiel: Wir bestimmen eine Primitivwurzel modulo 43. Die Gruppenordnung von $(\mathbb{Z}/43\mathbb{Z})^\times$ ist $42 = 2 \cdot 3 \cdot 7$, ein Element $\bar{a} \in (\mathbb{Z}/43\mathbb{Z})^\times$ ist also genau dann eine Primitivwurzel, wenn $\bar{a}^m \neq \bar{1}$ für alle $m \in \{\frac{42}{2}, \frac{42}{3}, \frac{42}{7}\} = \{21, 14, 6\}$ gilt. Wegen $\bar{2}^{14} = \bar{1}$ ist $\bar{2}$ keine Primitivwurzel. Es gilt aber $\bar{3}^{21} = \overline{42}$, $\bar{3}^{14} = \overline{36}$ und $\bar{3}^6 = \overline{41}$, also haben wir mit $\bar{a} = \bar{3}$ eine Primitivwurzel modulo 43 gefunden. Tatsächlich erhält man, wenn man die Potenzen $\bar{a}^1$, $\bar{a}^2$, $\bar{a}^3$, ... der Reihe nach aufschreibt, die Elemente

$$\bar{3}, \bar{9}, \overline{27}, \overline{38}, \overline{28}, \overline{41}, \overline{37}, \overline{25}, \overline{32}, \overline{10}, \overline{30}, \bar{4}, \overline{12}, \overline{36}, \overline{22}, \overline{23}, \overline{26}, \overline{35}, \overline{19}, \overline{14}, \overline{42}, \overline{40}, \overline{34}, \overline{16},$$
$$\bar{5}, \overline{15}, \bar{2}, \bar{6}, \overline{18}, \overline{11}, \overline{33}, \overline{13}, \overline{39}, \overline{31}, \bar{7}, \overline{21}, \overline{20}, \overline{17}, \bar{8}, \overline{24}, \overline{29}, \bar{1}$$

und somit die gesamte Gruppe $(\mathbb{Z}/43\mathbb{Z})^\times$.

Das Rechenbeispiel wirft die Frage auf, wie hohe Potenzen von Elementen $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ effizient ausgerechnet werden können. Es gibt hierzu das Verfahren der *schnellen Exponentiation*, dass wir hier kurz am Beispiel der Potenz $\bar{3}^{21}$ im Restklassenring $\mathbb{Z}/43\mathbb{Z}$ erläutern wollen. Zunächst schreibt man den Exponenten als Summe von Zweierpotenzen, in unserem Fall also $21 = 16 + 4 + 1$. Anschließend berechnet man die Elemente $\bar{3}^{2^d}$ für hinreichend großes d. In unserem Fall ist

$$\bar{3}^1 = \bar{3} \quad , \quad \bar{3}^2 = \bar{9} \quad , \quad \bar{3}^4 = (\bar{3}^2)^2 = \bar{9}^2 = \overline{81} = \overline{38} \quad , \quad \bar{3}^8 = (\bar{3}^4)^2 = (\overline{38})^2 = (-\bar{5})^2 = \overline{25} \quad ,$$
$$\bar{3}^{16} = (\bar{3}^8)^2 = (\overline{25})^2 = \overline{625} = \overline{195} = \overline{23}$$

weiter $\overline{38} \cdot \overline{23} = \overline{874} = \overline{14}$ und schließlich $\bar{3}^{21} = \bar{3}^{16} \cdot \bar{3}^4 \cdot \bar{3}^1 = \overline{23} \cdot \overline{38} \cdot \bar{3} = \overline{14} \cdot \bar{3} = \overline{42}$.

Lemma 14.15

(i) Sei p eine ungerade Primzahl und $m \in \mathbb{N}$. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \bmod p^m$ und $(1+p)^{p^{m-1}} \not\equiv 1 \bmod p^{m+1}$.

(ii) Für alle $m \in \mathbb{N}$, $m \geq 2$ gilt $5^{2^{m-2}} \equiv 1 \bmod 2^m$ und $5^{2^{m-2}} \not\equiv 1 \bmod 2^{m+1}$.

Beweis: zu (i) Wir beweisen die Aussage durch vollständige Induktion über m. Für $m = 1$ lautet die Aussage $1 + p \equiv 1 \bmod p$ und $1 + p \not\equiv 1 \bmod p^2$, und sie ist offenbar erfüllt. Sei nun $m \in \mathbb{N}$, und setzen wir die Assuage für m voraus. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \bmod p^m$. Es gilt also $(1+p)^{p^{m-1}} = 1 + kp^m$ für ein $k \in \mathbb{Z}$, aber wegen $(1+p)^{p^{m-1}} \not\equiv 1 \bmod p^{m+1}$ ist p kein Teiler von k. Durch Anwendung des Binomischen Lehrsatzes erhalten wir

$$\begin{aligned}(1+p)^{p^m} &= ((1+p)^{p^{m-1}})^p = (1+kp^m)^p = \\ \sum_{j=0}^{p}\binom{p}{j}(kp^m)^j &= 1 + kp^{m+1} + \sum_{j=2}^{p}\binom{p}{j}k^j p^{jm}.\end{aligned}$$

Für $2 \leq j \leq p-1$ ist $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ durch p teilbar. Also ist der j-te Summand $\binom{p}{j}k^j p^{jm}$ durch p^{mj+1} teilbar, und es gilt $mj + 1 \geq 2m + 1 \geq m + 2$. Der letzte Summand $\binom{p}{p}k^p p^{mp}$ ist durch p^{mp} teilbar, und es gilt $mp \geq 3m \geq m + 2$. Insgesamt ist $\sum_{j=2}^{p}\binom{p}{j}k^j p^{mj}$ also durch p^{m+2} teilbar, und wir erhalten $(1+p)^{p^m} \equiv 1 + kp^{m+1} \bmod p^{m+2}$. Es folgt $(1+p)^{p^m} \equiv 1 \bmod p^{m+1}$ und $(1+p)^{p^m} \not\equiv 1 \bmod p^{m+2}$.

zu (ii) Auch hier beweisen wir die Aussage durch vollständige Induktion über m. Für den Startwert $m = 2$ ist die Aussage wegen $5 \equiv 1 \bmod 4$ und $5 \not\equiv 1 \bmod 8$ erfüllt. Sei nun $m \geq 2$ und die Aussage für dieses m vorausgesetzt. Dann gilt $5^{2^{m-2}} \equiv 1 \bmod 2^m$ und $5^{2^{m-2}} \not\equiv 1 \bmod 2^{m+1}$. Es gibt also ein ungerades $k \in \mathbb{Z}$ mit $5^{2^{m-2}} = 1 + k2^m$. Durch Einsetzen erhalten wir

$$5^{2^{m-1}} = (5^{2^{m-2}})^2 = (1+k2^m)^2 = 1 + k2^{m+1} + k^2 2^{2m}.$$

Wegen $2m \geq m + 2$ folgt $5^{2^{m-1}} \equiv 1 + k2^{m+1} \bmod 2^{m+2}$. Wir erhalten $5^{2^{m-1}} \equiv 1 \bmod 2^{m+1}$ und $5^{2^m} \not\equiv 1 \bmod 2^{m+2}$. □

Satz 14.16

(i) Für jede ungerade Primzahl p und jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}/p^m\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $p^{m-1}(p-1)$.

(ii) Es gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$. Für alle $m \geq 3$ existiert jeweils ein Isomorphismus $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Beweis: zu (i) Wegen Folgerung 14.14 können wir $m \geq 2$ voraussetzen; außerdem gibt es auf Grund dieses Satzes ein $a \in \mathbb{Z}$ mit $\langle a + p\mathbb{Z}\rangle = (\mathbb{Z}/p\mathbb{Z})^\times$. Setzen wir $\bar{a} = a + p^m\mathbb{Z}$ und $r = \mathrm{ord}(\bar{a})$, dann gilt $\bar{a}^r = \bar{1}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$, also $a^r \equiv 1 \bmod p^m$ und erst recht $a^r \equiv 1 \bmod p$. Weil $a + p\mathbb{Z}$ in der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ die Ordnung $p-1$ hat, folgt aus $(a+p\mathbb{Z})^r = 1 + p\mathbb{Z}$, dass $p-1$ ein Teiler von r ist. Sei $k \in \mathbb{N}$ mit $k(p-1) = r$. Auf Grund der Rechenregeln für Elementordnungen aus der Gruppentheorie ist $\bar{b} = \bar{a}^k$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ein Element der Ordnung $p-1$.

Sei nun außerdem $\bar{c} = (1+p) + p^m\mathbb{Z}$. Nach Lemma 14.15 (i) gilt $\bar{c}^{p^{m-2}} \neq \bar{1}$ und $\bar{c}^{p^{m-1}} = \bar{1}$ in $\bar{c}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Dies zeigt, dass $\bar{c}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ein Element der Ordnung p^{m-1} ist. Sei nun die Untergruppen U und V von $G = (\mathbb{Z}/p^m\mathbb{Z})^\times$

gegeben durch $U = \langle \bar{b} \rangle$ und $V = \langle \bar{c} \rangle$. Als Untergruppen einer abelschen Gruppe sind U und V Normalteiler von G. Weil die Ordnungen $|U| = p-1$ und $|V| = p^{m-1}$ der zyklischen Gruppen $U \cong \mathbb{Z}/(p-1)\mathbb{Z}$ und $V \cong \mathbb{Z}/p^{m-1}\mathbb{Z}$ teilerfremd sind, gilt außerdem $U \cap V = \{\bar{1}\}$. Insgesamt ist das Komplexprodukt UV ein inneres direktes Produkt von U und V. Nach Proposition 4.24 aus der Gruppentheorie und dem Chinesischen Restsatz (der auf Grund der Teilerfremdheit von p^{m-1} und $p-1$ angewendet werden kann) folgt

$$UV \quad \cong \quad U \times V \quad \cong \quad \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \quad \cong \quad \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}.$$

Wegen $|G| = \varphi(p^m) = p^{m-1}(p-1)$ folgt $G = UV \cong \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$, also ist $G = (\mathbb{Z}/p^m\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $p^{m-1}(p-1)$.

zu (ii) Die ersten beiden Aussagen sind unmittelbar klar, denn nach Definition gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{1 + 2\mathbb{Z}\}$ und $(\mathbb{Z}/4\mathbb{Z})^\times = \{1+4\mathbb{Z}, 3+4\mathbb{Z}\} = \langle 3+4\mathbb{Z} \rangle$. Sei nun $m \in \mathbb{N}$ mit $m \geq 3$. Nach Lemma 14.15 (ii) gilt $\bar{5}^{2^{m-2}} = \bar{1}$ und $\bar{5}^{2^{m-3}} \neq \bar{1}$ in $(\mathbb{Z}/2^m\mathbb{Z})^\times$. Daraus folgt $\operatorname{ord}(\bar{5}) = 2^{m-2}$. Außerdem ist $-\bar{1}$ ein Element der Ordnung 2 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$, denn es gilt $-\bar{1} \neq \bar{1}$ und $(-\bar{1})^2 = \bar{1}$. Außerdem gilt $-\bar{1} \notin \langle \bar{5} \rangle$. Denn andernfalls würde $-\bar{1} = \bar{5}^k$ und damit $-1 \equiv 5^k \bmod 2^m$ für ein $k \in \mathbb{Z}$ gelten. Daraus wiederum würde wegen $5 \equiv 1 \bmod 4$ dann $-1 \equiv 5^k \equiv 1^k \equiv 1 \bmod 4$ folgen, im Widerspruch zu $-1 \not\equiv 1 \bmod 4$. Wegen $-\bar{1} \notin \langle \bar{5} \rangle$ gilt $\langle \bar{5} \rangle \cap \langle -\bar{1} \rangle = \{\bar{1}\}$, also bilden die Untergruppen $U = \langle \bar{5} \rangle$ und $V = \langle -\bar{1} \rangle$ ein inneres direktes Produkt UV. Wie in Teil (i) liefert der Satz über innere direkte Produkte aus der Gruppentheorie einen Isomorphismus $UV \cong U \times V \cong \mathbb{Z}/2^{m-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Aus $|UV| = |U \times V| = 2^{m-2} \cdot 2 = 2^{m-1} = \varphi(2^m) = |(\mathbb{Z}/2^m\mathbb{Z})^\times|$ gilt außerdem $(\mathbb{Z}/2^m\mathbb{Z})^\times = UV$. □

Beispiel: Das Element $\bar{a} = \bar{2}$ ein Erzeuger der 18-elementigen Gruppe $(\mathbb{Z}/27\mathbb{Z})^\times$. Dies überprüft man mit dem oben angegebenen Kriterium aus der Gruppentheorie durch die Rechung $\bar{2}^9 = \overline{26} \neq \bar{1}$ und $\bar{2}^6 = \overline{10} \neq \bar{1}$. Die Potenzen $\bar{a}^1, \bar{a}^2, \bar{a}^3, \ldots$ sind der Reihe nach gegeben durch

$$\overline{2}\,,\ \overline{4}\,,\ \overline{8}\,,\ \overline{16}\,,\ \overline{5}\,,\ \overline{10}\,,\ \overline{20}\,,\ \overline{13}\,,\ \overline{26}\,,\ \overline{25}\,,\ \overline{23}\,,\ \overline{19}\,,\ \overline{11}\,,\ \overline{22}\,,\ \overline{17}\,,\ \overline{7}\,,\ \overline{14}\,,\ \overline{1} \quad ,$$

also genau die Elemente der 18-elementigen Gruppe $(\mathbb{Z}/27\mathbb{Z})^\times$.

§ 15. *Endliche und algebraische Körpererweiterungen*

Zusammenfassung. In diesem Kapitel untersuchen wir die Körpererweiterungen genauer. Der Begriff des Erzeugendensystems, den wir bereits in der Gruppen- und Ringtheorie kennengelernt haben, besitzt auch hier eine nützliche Funktion. Ist $L|K$ eine Körpererweiterung, dann besitzt L die Struktur eines K-Vektorraums. Die Dimension dieses K-Vektorraums wird der *Grad* $[L : K]$ der Erweiterung genannt. Ist die Dimension endlich, dann spricht man von einer *endlichen* Erweiterung. Beispielsweise ist $[\mathbb{C} : \mathbb{R}] = 2$, und damit endlich, weil $\mathbb{C}$ als $\mathbb{R}$-Vektorraum zweidimensional ist.

Ein Element $\alpha \in L$ wird *algebraisch* über K genannt, wenn es Nullstelle eines Polynoms $f \in K[x]$ mit $f \neq 0_K$ ist. Trifft dies auf alle Elemente von L zu, dann wird auch die Erweiterung $L|K$ als algebraisch bezeichnet. Ist f normiert, und besitzt es unter allen Polynomen ungleich null mit α als Nullstelle einen minimalen Grad, dann nennt man f das *Minimalpolynom* von α über K. Der Grad der Erweiterung ist dann durch $[K(\alpha) : K] = \operatorname{grad}(f)$ gegeben. Die Elemente von $K(\alpha)$ besitzen eine einfache, eindeutige Darstellung, und mit Hilfe dieser Darstellung lassen sich auch die vier Rechenoperationen auf dem Körper $K(\alpha)$, also Addition, Subtraktion, Multiplikation und Division, auf einfache Weise beschreiben.

Wichtige Grundbegriffe

- Zwischenkörper einer Körpererweiterung
- von einer Teilmenge S über einem Grundkörper K erzeugter Teilkörper $K(S)$
- Grad einer Körpererweiterung
- endliche Körpererweiterung
- algebraisches Element in einer Körpererweiterung
- algebraische Körpererweiterung
- Minimalpolynom eines Elements

Zentrale Sätze

- Vektorraumstruktur eines Erweiterungskörpers
- Gradformel
- Erweiterungsgrad $[K(\alpha) : K]$ = Grad des Minimalpolynoms (falls α über K algebraisch ist)
- Rechenregeln für Elemente in algebraischen Erweiterungen
- Klassifikation der quadratischen Erweiterungen des Körpers $\mathbb{Q}$ der rationalen Zahlen

Bereits in § 9 haben wir die Begriffe „Teilkörper“, „Erweiterungskörper“ und „Körpererweiterung“ eingeführt. In der Körpertheorie spielt darüber hinaus der folgende Begriff eine wichtige Rolle.

Definition 15.1 Sei $L|K$ eine Körpererweiterung. Ein ***Zwischenkörper*** von $L|K$ ein Teilkörper von L, der zugleich Erweiterungskörper von K ist.

Beispielsweise ist $\mathbb{C}|\mathbb{Q}$ eine Körpererweiterung, und $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{C}$ sind Zwischenkörper dieser Erweiterung. Bereits bei den Untergruppen, den Idealen und den Teilringen ist uns das Konzept des Erzeugendensystems begegnet. Auch bei den Teilkörpern erweist sich dieses Konzept als sinnvoll.

Satz 15.2 Sei $\tilde{L}|K$ eine Körpererweiterung und $S \subseteq \tilde{L}$ eine Teilmenge. Dann gibt es einen eindeutig bestimmten Zwischenkörper L von $\tilde{L}|K$ mit den Eigenschaften

(i) $L \supseteq S$

(ii) Für jeden weiteren Zwischenkörper L' von $\tilde{L}|K$ mit $L' \supseteq S$ gilt $L' \supseteq L$.

Insgesamt ist L also der *kleinste* Zwischenkörper von $L|K$ mit der Eigenschaft $L \supseteq S$.

Beweis: Zunächst beweisen wir die Existenz. Sei $(L_i)_{i\in I}$ die Familie *aller* Zwischenkörper von $\tilde{L}|K$ mit $L_i \supseteq S$. Wie bei den Teilringen sieht man, dass dann auch $L = \bigcap_{i\in I} L_i$ ein Teilkörper von $\tilde{L}$ ist. Darüber hinaus gilt $L \supseteq L_i$ für alle $i \in I$ und somit $\tilde{L} \supseteq K$, insgesamt ist L also ein Zwischenkörper von $\tilde{L}|K$. Aus $L_i \supseteq S$ für alle $i \in I$ folgt auch $L \supseteq S$. Da L nach Definition in jedem Zwischenkörper L_i von $\tilde{L}|K$ enthalten ist, ist auch die Bedingung (ii) für den Körper L erfüllt.

Sei nun L' ein weiterer Zwischenkörper von $\tilde{L}|K$ mit den Eigenschaften (i) und (ii). Weil L und L' beide die Bedingung (ii) erfüllen, gilt $L' \supseteq L$ und $L \supseteq L'$, insgesamt also $L = L'$. □

Wir bezeichnen den nach Satz 15.2 eindeutig bestimmten Körper mit $K(S)$ und nennen ihn den von der Teilmenge S über K ***erzeugten*** Teilkörper von $\tilde{L}$. Ist S eine endliche Menge, $S = \{a_1, ..., a_n\}$, dann schreibt man statt $K(\{a_1, ..., a_n\})$ auch

$$K(a_1, ..., a_n) \quad ,$$

man lässt also die Mengenklammern weg. Beispielsweise bezeichnet $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ den kleinsten Zwischenkörper von $\mathbb{R}|\mathbb{Q}$, der $\{\sqrt{3}, \sqrt{5}\}$ als Teilmenge enthält. Wir bemerken bereits hier, dass auf Grund der Teilkörper-Eigenschaft von $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ mit $\sqrt{3}$ und $\sqrt{5}$ auch z.B. die Elemente

$$\sqrt{3}+\sqrt{5} \quad , \quad \sqrt{3}-\sqrt{5} \quad , \quad \sqrt{3}\sqrt{5} = \sqrt{15} \quad , \quad 2+7\sqrt{5} \quad , \quad \frac{3+4\sqrt{5}}{\sqrt{3}+\sqrt{5}} \quad , ...$$

in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ enthalten sind. Insgesamt enthält dieser Körper alle Elemente, die mit Hilfe der vier Grundrechenarten $+, -, \cdot$ und $\div$ aus $\sqrt{3}$, $\sqrt{5}$ und beliebigen rationalen Zahlen gebildet werden können.

Proposition 15.3 Sei $\tilde{L}|K$ eine Körpererweiterung, und seien S und T beliebige Teilmengen von $\tilde{L}$. Dann gilt

$$K(S \cup T) \quad = \quad K(S)(T).$$

Beweis: Wir müssen überprüfen, dass $K(S)(T)$ ein Zwischenkörper von $\tilde{L}|K$ ist, der die Bedingungen (i) und (ii) aus Satz 15.2 für die Menge $S \cup T$ erfüllt. Nach Definition ist $K(S)$ ein Zwischenkörper von $\tilde{L}|K$, und $K(S)(T)$ ist ein Zwischenkörper von $\tilde{L}|K(S)$. Aus $K(S)(T) \supseteq K(S)$ und $K(S) \supseteq K$ folgt $K(S)(T) \supseteq K$, also ist $K(S)(T)$ ein Zwischenkörper von $\tilde{L}|K$.

Weiter gilt nach Definition $K(S) \supseteq S$, und $K(S)(T)$ enthält sowohl $K(S)$ als auch T als Teilmengen. Insgesamt gilt damit $K(S)(T) \supseteq S \cup T$. Damit ist Bedingung (i) erfüllt. Zum Nachweis von (ii) sei L' ein beliebiger Zwischenkörper von $\tilde{L}|K$ mit $L' \supseteq S \cup T$. Dann ist L' insbesondere ein Zwischenkörper von $\tilde{L}|K$ mit $L' \supseteq S$. Auf Grund der Eigenschaft (ii) des Körpers $K(S)$ folgt daraus $L' \supseteq K(S)$, somit ist L' ein Zwischenkörper von $\tilde{L}|K(S)$. Zusammen mit $L' \supseteq T$ folgt $L' \supseteq K(S)(T)$. Damit ist insgesamt die Bedingung (ii) für den Körper $K(S)(T)$ nachgewiesen. □

Als nächstes schauen wir uns auch hier Erweiterungen an, die von einem einzelnen Element erzeugt werden.

Proposition 15.4 Sei $\tilde{L}|K$ eine Körpererweiterung und $a \in \tilde{L}$. Dann gilt

$$K(a) \quad = \quad \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in K[x], g(a) \neq 0 \right\}.$$

Dabei sei $K[x]$ der Polynomring über dem Körper K, und $f(a), g(a)$ bezeichnen die Elemente in $\tilde{L}$, die durch Einsetzen von a in f, g zu Stande kommen.

Beweis: Sei $T \subseteq \tilde{L}$ die Teilmenge auf der rechten Seite der Gleichung. Wir überprüfen zunächst, dass T ein Zwischenkörper von $\tilde{L}|K$ ist. Zum Nachweis der Teilkörper-Eigenschaft stellen wir zunächst fest, dass $1 \in T$ gilt, denn setzen wir $f = g = 1$, dann gilt $1 = f(a)/g(a)$. Seien nun $\alpha, \beta \in T$ vorgegeben. Dann gibt es Polynome $f, f_1, g, g_1 \in K[x]$ mit $g(a) \neq 0$, $g_1(a) \neq 0$ und

$$\alpha = \frac{f(a)}{g(a)} \qquad \text{und} \qquad \beta = \frac{f_1(a)}{g_1(a)}.$$

Es folgt

$$\alpha - \beta \quad = \quad \frac{f(a)g_1(a) - f_1(a)g(a)}{g(a)g_1(a)} \quad = \quad \frac{(f g_1 - f_1 g)(a)}{(g g_1)(a)}$$

und

$$\alpha\beta \quad = \quad \frac{f(a)f_1(a)}{g(a)g_1(a)} \quad = \quad \frac{(f f_1)(a)}{(g g_1)(a)}.$$

Somit sind auch die Elemente $\alpha - \beta$ und $\alpha\beta$ in T enthalten. Ist $\alpha \neq 0$, dann gilt $f(a) \neq 0$, und wir erhalten

$$\alpha^{-1} \quad = \quad \frac{g(a)}{f(a)} \quad \in T.$$

Damit ist gezeigt, dass T ein Teilkörper von $\tilde{L}$ ist. Jedes $b \in K$ entsteht durch Einsetzen von a in das konstante Polynom $b \in K[x]$. Dies zeigt $T \supseteq K$, d.h. T ist tatsächlich ein Zwischenkörper der Erweiterung $\tilde{L}|K$. Dieser enthält auch a, denn dieses Element entsteht durch Einsetzen von a in das Polynom $x \in K[x]$.

Sei nun L' ein beliebiger Zwischenkörper von $\tilde{L}|K$ mit $a \in L'$. Wegen $K \subseteq L$ und $a \in L$, und weil L' abgeschlossen unter Addition und Multiplikation ist, liegt $f(a)$ für jedes Polynom $f \in K[x]$ in L'. Ferner ist L' auch abgeschlossen unter Inversenbildung. Ist $g \in K[x]$ und $g(a) \neq 0$, dann gilt $g(a) \in L'$ und somit auch $g(a)^{-1} \in L'$. Ingesamt sind also sämtliche Elemente der Form $f(a)/g(a)$ mit $f, g \in K[x]$ und $g(a) \neq 0$ in L' enthalten. Damit haben wir $T \subseteq L'$ und insgesamt $T = K(a)$ nachgewiesen. □

Im weiteren Verlauf werden wir nun die Körpererweiterungen genauer untersuchen. Wir beginnen mit einem Merkmal, das es ermöglicht, die Größe solcher Erweiterungen miteinander zu vergleichen.

Definition 15.5 Ist $L|K$ eine Körpererweiterung, dann definieren die beiden Abbildungen

$$+ : L \times L \to L \;,\; (\alpha, \beta) \mapsto \alpha + \beta \quad \text{und} \quad \cdot : K \times L \to L \;,\; (a, \alpha) \mapsto a\alpha$$

eine K-Vektorraumstruktur auf L. Dabei bezeichnet man $[L : K] = \dim_K L$ als den ***Grad*** der Körpererweiterung; auch $[L : K] = \infty$ ist als Wert zugelassen. Ist $[L : K]$ endlich, dann nennt man $L|K$ eine ***endliche*** Körpererweiterung.

Beispielsweise gilt $[\mathbb{C} : \mathbb{R}] = 2$, denn jedes Element $\alpha \in \mathbb{C}$ kann auf eindeutige Weise in der Form $\alpha = a + ib$ mit $a, b \in \mathbb{R}$ dargestellt werden. Somit ist $\{1, i\}$ eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.

Satz 15.6 *(Gradformel)*

Seien $L|K$ und $M|L$ endliche Körpererweiterungen. Dann ist auch die Körpererweiterung $M|K$ endlich, und es gilt

$$[M : K] \quad = \quad [M : L] \cdot [L : K].$$

Beweis: Sei $m = [L : K]$, $n = [M : L]$, $\{\alpha_1, ..., \alpha_m\}$ eine Basis von L als K-Vektorraum und $\{\beta_1, ..., \beta_n\}$ eine Basis von M als L-Vektorraum. Wir zeigen, dass dann durch

$$\{\alpha_i \beta_j \mid 1 \leq i \leq m \ , \ 1 \leq j \leq n\}$$

eine mn-elementige Basis von M als K-Vektorraum ist. Daraus folgt dann die gewünschte Gleichung $[M : K] = mn = [L : K][M : L]$. Zunächst rechnen wir nach, dass die Elemente ein Erzeugendensystem bilden. Sei $\gamma \in M$ beliebig vorgegeben. Weil M als L-Vektorraum von $\beta_1, ..., \beta_n$ aufgespannt wird, gibt es $\gamma_1, ..., \gamma_n \in L$ mit $\gamma = \sum_{j=1}^{n} \gamma_j \beta_j$. Weiter finden wir $a_{ij} \in K$ mit $\gamma_j = \sum_{i=1}^{m} a_{ij} \alpha_i$ für $1 \leq j \leq n$. Einsetzen liefert

$$\gamma \quad = \quad \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \alpha_i \right) \beta_j \quad = \quad \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j.$$

Nun beweisen wir noch die lineare Unabhängigkeit. Seien $a_{ij} \in K$ mit $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j = 0$ vorgegeben. Dann gilt

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \alpha_i \right) \beta_j \quad = \quad 0.$$

Die lineare Unabhängigkeit von $\beta_1, ..., \beta_n$ im L-Vektorraum M liefert $\sum_{i=1}^{m} a_{ij} \alpha_i = 0$ für $1 \leq j \leq n$. Da die Elemente $\alpha_1, ..., \alpha_n$ im K-Vektorraum L linear unabhängig sind, folgt daraus wiederum $a_{ij} = 0$ für $1 \leq i \leq m$ und $1 \leq j \leq n$. □

Umgekehrt gilt: Ist $M|K$ eine endliche Erweiterung, dann sind auch $M|L$ und $L|K$ endlich. Wäre $M|L$ unendlich, dann gäbe es für jedes $n \in \mathbb{N}$ ein System $\alpha_1, ..., \alpha_n$ von Elementen aus M, die über L linear unabhängig sind. Diese sind dann erst recht linear unabhängig über K. Wäre $L|K$ unendlich, dann gäbe es beliebig große, endliche Systeme von Elementen in L, die über K linear unabhängig sind. Diese sind dann erst recht in M enthalten.

Für jede Körpererweiterung $L|K$ gilt offenbar $[L : K] = 1$ genau dann, wenn $L = K$ ist. Denn einerseits ist K ein eindimensionaler K-Vektorraum, mit $\{1_K\}$ als Basis, und folglich gilt $[K : K] = 1$. Setzen wir andererseits $[L : K] = 1$ voraus, dann ist jede einelementige Teilmenge von $L \setminus \{0_L\}$ eine Basis von L als K-Vektorraum, insbesondere also $\{1_K\}$. Jedes $\alpha \in L$ kann also in der Form $\alpha = a \cdot 1_K = a$ mit $a \in K$ dargestellt werden; daraus folgt $L = K$.

Mit Hilfe der Gradformel kann zum Beispiel gezeigt werden, dass die Erweiterung $\mathbb{C}|\mathbb{R}$ keinen echten Zwischenkörper, also keine Zwischenkörper K mit $\mathbb{R} \subsetneq K \subsetneq \mathbb{C}$ besitzt. Sei nämlich K ein beliebiger Zwischenkörper von $\mathbb{C}|\mathbb{R}$. Dann erhalten wir durch die Gradformel

$$2 \quad = \quad [\mathbb{C} : \mathbb{R}] \quad = \quad [\mathbb{C} : K] \cdot [K : \mathbb{R}].$$

Da die Erweiterungsgrade natürliche Zahlen sind, folgt $[\mathbb{C} : K] = 1$ oder $[K : \mathbb{R}] = 1$. Auf Grund der Gradformel folgt daraus wiederum $\mathbb{C} = K$ oder $K = \mathbb{R}$.

Kommen wir nun zu einem wichtigen Merkmal der Elemente einer Körpererweiterung.

Definition 15.7 Sei $L|K$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt ***algebraisch*** über K, wenn ein Polynom $f \neq 0$ in $K[x]$ mit der Eigenschaft existiert, dass α eine Nullstelle von f ist. Gibt es ein solches Polynom nicht, dann nennt man α ***transzendent*** über K.

Wir betrachten einige Beispiele für algebraische und transzendente Körperelemente.

(i) Das Element $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, denn es ist Nullstelle des Polynoms $x^2-2 \in \mathbb{Q}[x]$. Weil dieses Polynom auch in $\mathbb{R}[x]$ liegt, ist $\sqrt{2}$ auch algebraisch über $\mathbb{R}$. Alternativ kann zum Nachweis dieser Eigenschaft aber auch das Polynom $x - \sqrt{2} \in \mathbb{R}[x]$ verwendet werden.

(ii) Allgemein gilt: Ist K ein Körper und $a \in K$, dann ist α als Nullstelle von $x - a \in K[x]$ algebraisch über K.

(iii) Die imaginäre Einheit $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, sogar über $\mathbb{Q}$, als Nullstelle des Polynoms $x^2 + 1 \in \mathbb{Q}[x]$.

(iv) Man kann zeigen, dass die Kreiszahl π und die Eulersche Zahl e transzendent über $\mathbb{Q}$ sind. Der Beweis ist leider so aufwändig, dass wir ihn hier nicht durchführen können. Nach (ii) sind beide Elemente aber algebraisch über $\mathbb{R}$ und $\mathbb{C}$.

Definition 15.8 Sei $L|K$ eine Körpererweiterung, und sei $\alpha \in L$ algebraisch über K. Dann gibt es ein eindeutig bestimmtes, normiertes Polynom $f \in K[x]$, $f \neq 0$ minimalen Grades mit $f(\alpha) = 0$. Man nennt f das ***Minimalpolynom*** von α über K. Wir bezeichnen es mit $\mu_{\alpha,K}$.

Beweis: Weil α über K algebraisch ist, gibt es jedenfalls ein Polynom $0 \neq g \in K[x]$ mit der Eigenschaft $g(\alpha) = 0$. Bezeichnet $a_n \in K^\times$ den Leitkoeffizienten von g, dann ist $\tilde{g} = a_n^{-1} g$ ein normiertes Polynom mit $\tilde{g}(\alpha) = 0$. Aus der Menge aller normierten Polynome $f \in K[x]$ mit $f(\alpha) = 0$ können wir eines mit minimalem Grad wählen.

Zum Beweis der Eindeutigkeit seien $f, g \in K[x]$ zwei normierte Polynome minimalen Grades mit $f(\alpha) = g(\alpha) = 0$. Ist $f \neq g$, dann hat das Polynom $h = g - f$ die Eigenschaft $h(\alpha) = g(\alpha) - f(\alpha) = 0 - 0 = 0$ und $\operatorname{grad}(h) < \operatorname{grad}(f)$. Durch Normierung von h erhalten wir also ein normiertes Polynom mit α als Nullstelle, das einen echt kleineren Grad als f hat. Dies aber widerspricht der Minimalität. Somit ist nur $f = g$ möglich. □

Wir betrachten die Körpererweiterung $\mathbb{R}|\mathbb{Q}$. Das Minimalpolynom $\mu_{\sqrt{2},\mathbb{Q}}$ des Elements $\sqrt{2} \in \mathbb{R}$ über $\mathbb{Q}$ ist $f = x^2 - 2$. Denn einerseits gilt $f(\sqrt{2}) = 0$. Gäbe es andererseits ein normiertes Polynom $g \in \mathbb{Q}[x]$ kleineren Grades, also $g = x + a$ mit $g(\sqrt{2}) = 0$, dann würde $a = -\sqrt{2}$ folgen, und $\sqrt{2}$ wäre rational.

Proposition 15.9 Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K und $f \in K[x]$ sein Minimalpolynom, also $f = \mu_{\alpha,K}$. Dann gilt

(i) Das Polynom f ist irreduzibel.

(ii) Ist $g \in K[x]$ mit $g(\alpha) = 0$, dann folgt $f \mid g$.

(iii) Ist $g \in K[x]$ ebenfalls normiert, irreduzibel, mit $g(\alpha) = 0_K$, dann folgt $f = g$.

Beweis: zu (i) Zunächst kann f wegen $f \neq 0$ und $f(\alpha) = 0$ nicht konstant sein. Nehmen wir nun an, f ist reduzibel, und g, h sind nicht-konstante Polynome mit $f = gh$. Wegen $\text{grad}(g) > 0$, $\text{grad}(h) > 0$ und $\text{grad}(f) = \text{grad}(g) + \text{grad}(h)$ gilt $\text{grad}(g) < \text{grad}(f)$ und $\text{grad}(h) < \text{grad}(f)$. Aus $g(\alpha)h(\alpha) = f(\alpha) = 0$ folgt außerdem $g(\alpha) = 0$ oder $h(\alpha) = 0$. Nehmen wir nun o.B.d.A. an, dass $g(\alpha) = 0$ gilt, und sei $\tilde{g}$ das Polynom, das man durch Normierung von g erhält. Dann ist $\tilde{g}$ ein normiertes Polynom mit α als Nullstelle, dass einen echt kleineren Grad als f hat. Dies widerspricht der Voraussetzung $f = \mu_{\alpha,K}$.

zu (ii) Durch Division mit Rest erhalten wir Polynome $q, r \in K[x]$ mit $g = qf + r$ und $r = 0$ oder $\text{grad}(r) < \text{grad}(f)$. Es gilt $r(\alpha) = g(\alpha) - q(\alpha)f(\alpha) = 0 - q(\alpha) \cdot 0 = 0$. Damit ist der Fall $r \neq 0$ ausgeschlossen, denn ansonsten wäre die Normierung von r ein Polynom mit echt kleinerem Grad als f und α als Nullstelle. Somit gilt $g = qf$, d.h. f ist ein Teiler von g.

zu (iii) Sei g ein Polynom mit der angegebenen Eigenschaft. Nach Teil (ii) gilt $f|g$. Es gibt also ein $h \in K[x]$ mit $g = fh$. Weil g irreduzibel ist, muss h konstant sein. Weil f und g beide normiert sind, folgt $h = 1$ und $g = f$. □

Mit Hilfe des Minimalpolynoms können wir nun genauer angeben, wie eine Körpererweiterung aussieht, die von einem einzigen algebraischen Element erzeugt wird.

Satz 15.10 Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K, $f = \mu_{\alpha,K}$ und $n = \text{grad}(f)$. Dann bilden die Elemente $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ eine Basis von $K(\alpha)$ als K-Vektorraum. Insbesondere gilt $[K(\alpha) : K] = n$.

Beweis: Sei U der Untervektorraum von L, der durch $\{1, \alpha, ..., \alpha^{n-1}\}$ aufgespannt wird, also

$$U = \left\{ \sum_{k=0}^{n-1} a_k \alpha^k \;\middle|\; a_0, ..., a_{n-1} \in K \right\} = \left\{ g(\alpha) \;\middle|\; g \in K[x],\ \text{grad}(g) < n \text{ oder } g = 0 \right\}.$$

Wir zeigen, dass U ein Teilkörper von L ist. Durch Einsetzen von α in das konstante Polynom $1 \in K[x]$ sieht man, dass 1 in U liegt. Seien nun $\beta, \gamma \in U$ vorgegeben. Dann gibt es Polynome $g, h \in K[x]$ mit $\beta = g(\alpha)$, $\gamma = h(\alpha)$, wobei g und h entweder Null sind oder jedenfalls einen Grad kleiner als n haben. Mit g und h ist auch $g - h$ ein Polynom mit $g - h = 0$ oder $\text{grad}(g - h) < n$; daraus folgt $\beta - \gamma = g(\alpha) - h(\alpha) = (g - h)(\alpha) \in U$.

Der Nachweis von $\beta\gamma \in U$ ist etwas aufwändiger, weil der Grad des Polynoms gh auch größer als $n - 1$ sein kann. Durch Division von gh durch f mit Rest erhalten wir aber Polynome $q, r \in K[x]$ mit $gh = qf + r$ und $r = 0$ oder $\text{grad}(r) < n$. Es folgt

$$\beta\gamma = g(\alpha)h(\alpha) = (qf + r)(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha).$$

Nach Definition der Menge U ist $r(\alpha)$ in U enthalten. Es bleibt zu zeigen, dass im Fall $\beta \neq 0$ auch β^{-1} in U liegt. Aus $\beta \neq 0$ folgt zunächst $g \neq 0$. Weil f irreduzibel ist, sind die Polynome f und g teilerfremd. Nach dem Lemma von Bézout aus der Ringtheorie gibt es Polynome $a, b \in K[x]$ mit $af + bg = 1$. Es folgt

$$1 \quad = \quad (af + bg)(\alpha) \quad = \quad a(\alpha)f(\alpha) + b(\alpha)g(\alpha) \quad = \quad a(\alpha) \cdot 0 + b(\alpha)g(\alpha) \quad = \quad b(\alpha)g(\alpha)$$

und somit $\beta^{-1} = g(\alpha)^{-1} = b(\alpha)$. Division von b durch f mit Rest liefert weiter Polynome $q, r \in K[x]$ mit $b = qf + r$ und $\text{grad}(r) < n$. Es folgt

$$\beta^{-1} \quad = \quad b(\alpha) \quad = \quad q(\alpha)f(\alpha) + r(\alpha) \quad = \quad q(\alpha) \cdot 0 + r(\alpha) \quad = \quad r(\alpha) \in U.$$

Damit haben wir insgesamt nachgewiesen, dass U tatsächlich ein Teilkörper von $\tilde{L}$ ist. Darüber hinaus gilt $\alpha \in U$. Ist nämlich $n = 1$, dann gilt $K = U$, außerdem $f = x - \alpha \in K[x]$ und damit $\alpha \in K$. Im Fall $n > 1$ ist $g = x$ ein Polynom vom Grad $< n$, und es gilt $\alpha = g(\alpha) \in U$.

Sei nun L ein beliebiger Zwischenkörper von $\tilde{L}$ mit $\alpha \in L$. Auf Grund der Teilkörpereigenschaft ist L abgeschlossen unter Addition und Multiplikation. Damit enthält L sämtliche Elemente der Form $g(\alpha)$ mit $g \in K[x]$ in L, es gilt also $L \supseteq U$. Somit ist U der *kleinste* Zwischenkörper von $L|K$ mit $\alpha \in U$. Nach Definition des erzeugten Zwischenkörpers folgt $U = K(\alpha)$.

Aus der Definition von U folgt unmittelbar, dass $K(\alpha)$ als K-Vektorraum von den Elementen $1, \alpha, ..., \alpha^{n-1}$ aufgespannt wird. Nehmen wir nun an, dass diese Elemente über K linear abhängig sind. Dann gibt es Koeffizienten $a_0, ..., a_{n-1} \in K$, nicht alle gleich Null, mit

$$\sum_{k=0}^{n-1} a_k \alpha^k \quad = \quad 0.$$

Setzen wir $g = \sum_{k=0}^{n-1} a_k x^k$, dann ist $g \in K[x]$ ein Polynom ungleich Null mit den Eigenschaften $g(\alpha) = 0$ und $\text{grad}(g) < n$. Durch Normierung von g erhalten wir ein normiertes Polynom mit kleinerem Grad als f und mit α als Nullstelle. Aber dies ist unmöglich, weil f das Minimalpolynom von α ist. Also sind die Elemente $1, \alpha, ..., \alpha^{n-1}$ linear unabhängig und bilden eine Basis von $K(\alpha)$ als K-Vektorraum. □

Dem Beweis von Satz 15.10 kann entnommen werden, wie die arithmetischen Operationen (Addition, Multiplikation, Berechnung von Negativen und Kehrwerten) in einem algebraischen Erweiterungskörper $K(\alpha)$ von K ausgeführt werden können. Sei $f \in K[x]$ das Minimalpolynom von α und $n = \text{grad}(f)$. Auf Grund des Satzes kann jedes Element aus $K(\alpha)$ auf ***eindeutige Weise*** in der Form $g(\alpha)$ geschrieben werden, wobei $g \in K[x]$ entweder Null oder vom Grad $< n$ ist. Seien $\beta, \gamma \in K(\alpha)$ und $g, h \in K[x]$ Polynome passenden Grades mit $\beta = g(\alpha)$, $\gamma = h(\alpha)$. Unser Ziel besteht darin, die Elemente $\beta + \gamma$, $-\beta$, $\beta\gamma$ und (im Fall $\beta \neq 0$) auch β^{-1} wiederum in dieser eindeutigen Form darzustellen.

(i) ***Addition:***
Es gilt $\beta + \gamma = (g + h)(\alpha)$, außerdem $g + h = 0$ oder $\text{grad}(g + h) < n$.

(ii) ***Negative:***
Es gilt $-\beta = (-g)(\alpha)$ und $-g = 0$ oder $\text{grad}(-g) < n$.

(iii) ***Multiplikation:***
Durch Division mit Rest bestimmen wir Polynome $q, r \in K[x]$ mit $gh = qf + r$ und $r = 0$ oder $\text{grad}(r) < n$. Wie im Beweis von Satz 15.10 gezeigt wurde, gilt $\beta\gamma = r(\alpha)$.

(iv) ***Kehrwerte:***
Hier sei $\beta \neq 0$ vorausgesetzt. Wie im Beweis des Satzes gezeigt wurde, gilt $\mathrm{ggT}(f,g) = 1$. Mit dem Euklidischen Algorithmus können Polynome $a, g \in K[x]$ mit $af + bg = 1$ berechnet werden. Weiter finden wir Polynome $q, r \in K[x]$ mit $b = qf + r$ und $\mathrm{grad}(r) < n$. Im Beweis haben wir bereits nachgerechnet, dass dann $\beta^{-1} = r(\alpha)$ erfüllt ist.

Wir betrachten ein konkretes Anwendungsbeispiel. Sei $\tilde{L}$ ein Erweiterungskörper von $\mathbb{F}_3$ und $\alpha \in L$ ein Element mit $\alpha^2 + \bar{1} = \bar{0}$. Dabei bezeichnen die Elemente $\bar{0}, \bar{1} \in \mathbb{F}_3$ Null- und Einselement des Körpers $\mathbb{F}_3$ und damit zugleich diejenigen des Körpers $\tilde{L}$. Nach Definition ist α eine Nullstelle des Polynoms $f = x^2 + \bar{1} \in \mathbb{F}_3[x]$. Weil f in $\mathbb{F}_3$ keine Nullstellen besitzt, ist es irreduzibel und somit das Minimalpolynom von α. Jedes $\beta \in \mathbb{F}_3(\alpha)$ kann auf eindeutige Weise in der Form

$$\beta = a_0 + a_1\alpha \quad \text{mit} \quad a_0, a_1 \in \mathbb{F}_3$$

dargestellt werden. Weil es für a_0 und a_1 jeweils $|\mathbb{F}_3| = 3$ Auswahlmöglichkeiten gibt, handelt es sich bei $\mathbb{F}_3(\alpha)$ um einen Körper mit 9 Elementen. Wegen $\dim_{\mathbb{F}_3} \mathbb{F}_3(\alpha) = \mathrm{grad}(f) = 2$ ist $\mathbb{F}_3(\alpha)$ ein 2-dimensionaler $\mathbb{F}_3$-Vektorraum.

Sei nun konkret $\beta = \alpha + \bar{1}$ und $\gamma = \alpha - \bar{1}$. Dann ist $\beta = g(\alpha)$ und $\gamma = h(\alpha)$ mit $g = x + \bar{1}$ und $h = x - \bar{1}$. Es folgt $g + h = \bar{2}x$, $g - h = \bar{2}$ und somit

$$\beta + \gamma = (g+h)(\alpha) = \bar{2}\alpha \qquad \text{und} \qquad \beta - \gamma = (g-h)(\alpha) = \bar{2}.$$

Natürlich kann man auch direkt mit den Elementen rechnen: Es gilt

$$\beta + \gamma \quad = \quad (\alpha + \bar{1}) + (\alpha - \bar{1}) \quad = \quad \alpha + \alpha \quad = \quad \bar{2}\alpha$$

und ebenso

$$\beta - \gamma \quad = \quad (\alpha + \bar{1}) - (\alpha - \bar{1}) \quad = \quad \bar{1} + \bar{1} \quad = \quad \bar{2}.$$

Um nach $\beta\gamma$ nach der angegebenen Methode zu berechnen, teilen wir das Polynom $gh = x^2 - \bar{1}$ mit Rest durch f und erhalten $x^2 - \bar{1} = \bar{1} \cdot (x^2 + \bar{1}) + \bar{1}$. Es folgt $\beta\gamma = \bar{1}$, also ist γ im Körper $\mathbb{F}_3(\alpha)$ der Kehrwert von β. Auch hier hätte man statt mit den Polynomen direkte mit den Körperelementen rechnen können. Aus $f(\alpha) = \alpha^2 - \bar{1} = \bar{0} \Leftrightarrow \alpha^2 = -\bar{1}$ folgt

$$(\alpha + \bar{1})(\alpha - \bar{1}) \quad = \quad \alpha^2 - \bar{1} \quad = \quad -\bar{1} - \bar{1} \quad = \quad \bar{1}.$$

Um den Kehrwert es Elements α auszurechnen, bestimmen wir mit dem Euklidischen Algorithmus Polynome $a, b \in K[x]$ mit $ax + bf = \bar{1}$. Wir erhalten $a = \bar{2}x$ und $b = \bar{1}$. Der Kehrwert von α ist also durch $\alpha^{-1} = a(\alpha) = \bar{2}\alpha$ gegeben. Tatsächlich gilt $(\bar{2}\alpha)\alpha = \bar{2}\alpha^2 = \bar{2}(-\bar{1}) = -\bar{2} = \bar{1}$.

Die vollständige Tabelle der Kehrwerte sämtlicher Elemente in $\mathbb{F}_3(\alpha)^\times$ sieht folgendermaßen aus.

β	$\bar{1}$	$\bar{2}$	α	$\alpha+\bar{1}$	$\alpha+\bar{2}$	$\bar{2}\alpha$	$\bar{2}\alpha+\bar{1}$	$\bar{2}\alpha+\bar{2}$
β^{-1}	$\bar{1}$	$\bar{2}$	$\bar{2}\alpha$	$\alpha+\bar{2}$	$\alpha+\bar{1}$	α	$\bar{2}\alpha+\bar{2}$	$\bar{2}\alpha+\bar{1}$

Jeder einzelne Eintrag kann durch Multiplikation von β und β^{-1} unmittelbar verifiziert werden.

Aus den bisherigen Ausführen folgt noch nicht, dass zum Polynom $x^2+\bar{1} \in \mathbb{F}_3[x]$ überhaupt eine Körpererweiterung $\tilde{L}|\mathbb{F}_3$ und ein Element $\alpha \in \tilde{L}$ mit $\alpha^2+1=0$ existieren. Dem Problem der ***Konstruktion*** und der Eindeutigkeit solcher Körpererweiterungen wenden wir uns nun als nächstes zu.

Satz 15.11 Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K und $f = \mu_{\alpha,K}$. Dann gibt es einen Isomorphismus

$$\bar{\phi} : K[x]/(f) \longrightarrow K(\alpha) \quad \text{mit} \quad \phi(g+(f)) = g(\alpha) \text{ für alle } g \in K[x].$$

Dabei bezeichnet $K(\alpha)$ den von α erzeugten Zwischenkörper der Erweiterung $L|K$.

Beweis: Sei $\phi : K[x] \to L$ der auf Grund der universellen Eigenschaft von Polynomringen eindeutig bestimmte Homomorphismus von Ringen mit $\phi(x) = \alpha$ und $\phi|_K = \mathrm{id}_K$. Weil ϕ als Ringhomomorphismus verträglich mit Addition und Multiplikation verträglich ist, gilt $\phi(g) = g(\alpha)$ für alle $g \in K[x]$. Weil der Körper $K(\alpha)$ das Element $g(\alpha)$ für jedes $g \in K[x]$ enthält, ist durch ϕ ein Homomorphismus $K[x] \to K(\alpha)$ gegeben. Nach Satz 15.10 hat jedes Element aus $K(\alpha)$ die Form $g(\alpha)$ mit $g \in K[x]$ und $\mathrm{grad}(g) < n$. Dies zeigt, dass ϕ als Ringhomomorphismus $K[x] \to K(\alpha)$ auch surjektiv ist.

Wir zeigen nun, dass $\ker(\phi) = (f)$ gilt, wobei (f) das vom Element f erzeugte Hauptideal in $K[x]$ bezeichnet. Ist $g \in (f)$, dann gibt es nach Definition ein $h \in K[x]$ mit $g = hf$. Es folgt $\phi(g) = g(\alpha) = h(\alpha)f(\alpha) = h(\alpha) \cdot 0 = 0$, also $\phi \in \ker(\phi)$. Sei umgekehrt $g \in \ker(\phi)$. Dann gilt $g(\alpha) = 0$. Nach Proposition 15.9 ist g ein Vielfaches des Minimalpolynoms f, also $g \in (f)$. Der Homomorphiesatz für Ringe, Teil (ii) von Satz 11.9, liefert nun den angegebenen Isomorphismus. □

Satz 15.12 *(Existenz algebraischer Erweiterungen)*
Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann gibt es eine Körpererweiterung $L|K$ und ein Element $\alpha \in L$ mit $f(\alpha) = 0$.

Beweis: Zunächst bilden wir den Restklassenring $\tilde{L} = K[x]/(f)$. Weil f irreduzibel ist und es sich bei $K[x]$ um einen Hauptidealring handelt, ist das Ideal (f) nach Satz 12.18 ein maximales Ideal, und daraus wiederum folgt, dass der Faktorring $\tilde{L}$ ein Körper ist. Wir überprüfen nun, dass durch die Abbildung $\phi : K \to \tilde{L}$, $a \mapsto a+(f)$ ein Körperhomomorphismus definiert ist. Zunächst gilt $\phi(1_K) = 1_K + (f) = 1_{\tilde{L}}$. Seien nun $a, b \in K$ beliebig vorgegeben. Dann gilt $\phi(a+b) = (a+b)+(f) = (a+(f))+(b+(f)) = \phi(a)+\phi(b)$ und ebenso

$$\phi(ab) \quad = \quad ab+(f) \quad = \quad (a+(f))(b+(f)) \quad = \quad \phi(a)\phi(b).$$

Nach Satz 11.16 gilt: Ist $\phi : R \to S$ ein Monomorphismus von Ringen, dann gibt es einen Erweiterungsring $\hat{S} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{S} \to S$ von Ringen mit $\hat{\phi}|_R = \phi$. Die Anwendung dieses Satzes auf unseren Körperhomomorphismus ϕ liefert uns nun einen Erweiterungsring $L \supseteq K$ und einen Isomorphismus $\hat{\phi} : L \to \tilde{L}$ von Ringen mit $\hat{\phi}|_K = \phi$. Weil $\tilde{L}$ ein Körper und $\hat{\phi}$ ein Isomorphismus ist, ist auch L ein Körper, und somit ist $L|K$ eine Körpererweiterung. Wir zeigen nun, dass das Element $\alpha = \hat{\phi}^{-1}(x+(f))$ eine Nullstelle von f ist. Dazu schreiben wir f in der

Form $f = \sum_{i=0}^{n} a_i x^i$ mit $n \in \mathbb{N}$ und $a_0, ..., a_n \in K$. Es gilt

$$\hat{\phi}(f(\alpha)) = \hat{\phi}\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} \phi(a_i)\hat{\phi}(\alpha)^i = \sum_{i=0}^{n} (a_i + (f))(x + (f))^i =$$

$$\sum_{i=0}^{n} (a_i x^i + (f)) = \left(\sum_{i=0}^{n} a_i x^i\right) + (f) = f + (f) = 0 + (f) = 0_{\tilde{L}} \quad ,$$

und somit $f(\alpha) = \hat{\phi}^{-1}(0_{\tilde{L}}) = 0_L$. □

Definition 15.13 Eine Körpererweiterung $L|K$ wird ***algebraisch*** genannt, wenn jedes Element $\alpha \in L$ algebraisch über K ist.

Die Eigenschaften „endlich“ und „algebraisch“ hängen folgendermaßen miteinander zusammen.

Proposition 15.14 Sei $L|K$ eine Körpererweiterung.

(i) Ist $L|K$ endlich, dann auch algebraisch.

(ii) Sind $\alpha_1, ..., \alpha_n \in L$ algebraisch über K und gilt $L = K(\alpha_1, ..., \alpha_n)$, dann ist die Erweiterung $L|K$ endlich (also insbesondere algebraisch).

Beweis: zu (i) Wir führen den Beweis durch Kontraposition. Ist $L|K$ nicht algebraisch, dann gibt es ein Element $\alpha \in L$, das transzendent über K ist. Dies bedeutet, dass für jedes $n \in \mathbb{N}$ die Elemente $1, \alpha, ..., \alpha^n$ über K linear unabhängig sind. Denn andernfalls gäbe es Elemente $a_0, ..., a_n \in K$, nicht alle gleich Null, mit $\sum_{i=0}^{n} a_i \alpha^i = 0$, und folglich wäre $f = \sum_{i=0}^{n} a_i x^i \in K[x]$ ein Polynom ungleich Null mit $f(\alpha) = 0$. Daraus würde folgen, dass α algebraisch über K ist, im Widerspruch zur Voraussetzung. Aus der linearen Unabhängigkeit der $n+1$ Elemente $1, \alpha, ..., \alpha^n$ folgt $[L : K] = \dim_K L \geq n + 1$. Da n beliebig gewählt war, erhalten wir $[L : K] = \infty$.

zu (ii) Wir beweisen die Aussage durch vollständige Induktion über n. Für $n = 0$ gilt $L = K$ und somit $[L : K] = 1$. Sei nun $n \in \mathbb{N}$ vorgegeben, und setzen wir die Aussage für alle $m \in \mathbb{N}$ mit $m < n$ voraus. Seien $\alpha_1, ..., \alpha_n \in L$ mit $L = K(\alpha_1, ..., \alpha_n)$. Nach Induktionsvoraussetzung ist die Erweiterung $L_0|K$ mit $L_0 = K(\alpha_1, ..., \alpha_{n-1})$ endlich, und nach Proposition 15.3 gilt $L = L_0(\alpha_n)$. Weil α_n über K algebraisch ist, besitzt α_n ein Minimalpolynom über K, erst recht ein Minimalpolynom $f \in L_0[x]$ über L_0. Nach Satz 15.10 gilt $[L : L_0] = \text{grad}(f)$. Weil $L_0|K$ und $L|L_0$ endliche Erweiterungen sind, ist nach Satz 15.6 auch $L|K$ endlich. □

Satz 15.15

(i) Sei $L|K$ eine Körpererweiterung und $T \subseteq L$ die Teilmenge bestehend aus den Elementen, die algebraisch über K sind. Dann ist T ein Teilkörper von L.

(ii) Seien $L|K$ und $M|L$ Körpererweiterungen. Genau dann ist die Erweiterung $M|K$ algebraisch, wenn die Erweiterungen $L|K$ und $M|L$ beide algebraisch sind.

Beweis: zu (i) Zum Nachweis der Teilkörper-Eigenschaft müssen wir zeigen, dass 1_L in T liegt, und mit $\alpha, \beta \in T$ auch die Elemente $\alpha - \beta$ und $\alpha\beta$, im Fall $\alpha \neq 0_L$ auch das Element α^{-1}. Wegen $1_L = 1_K \in K$ ist 1_L algebraisch über K, also in T enthalten. Seien nun $\alpha, \beta \in T$ vorgegeben. Weil α und β algebraisch über T sind, ist $K(\alpha, \beta)|K$ nach Proposition 15.14 (ii) eine endliche Erweiterung. Nach Teil (i) ist $K(\alpha, \beta)|K$ damit auch algebraisch, es gilt also $K(\alpha, \beta) \subseteq T$. Als Teilkörper enthält $K(\alpha, \beta)$ mit α und β auch die Elemente $\alpha - \beta$ und $\alpha\beta$, im Fall $\alpha \neq 0_L$ auch das Element α^{-1}. Damit sind all diese Elemente auch in T enthalten.

zu (ii) „⇒“ Setzen wir voraus, dass $M|K$ algebraisch ist. Dann ist jedes $\alpha \in M$ Nullstelle eines Polynoms $f \in K[x]$ ungleich Null. Dieses Polynom ist auch in $L[x]$ enthalten, folglich ist α auch algebraisch über L. Weil $\alpha \in M$ beliebig gewählt war, folgt daraus, dass die Erweiterung $M|L$ algebraisch ist. Wenn jedes $\alpha \in M$ algebraisch über K ist, dann gilt dies insbesondere für jedes Element aus L. Folglich ist auch $L|K$ algebraisch.

„⇐“ Seien nun $L|K$ und $M|L$ algebraische Erweiterungen und $\alpha \in M$ ein beliebig vorgegebenes Element. Wir müssen zeigen, dass α algebraisch über K ist. Nach Voraussetzung ist α jedenfalls algebraisch über L. Sei $f = \mu_{L,\alpha} \in L[x]$, und seien $a_0, ..., a_n \in L$ die Koeffizienten von f. Jedes a_i ist laut Voraussetzung algebraisch über K. Nach Proposition 15.14 (ii) ist $L_0|K$ mit $L_0 = K(a_0, ..., a_n)$ damit eine endliche Erweiterung. Weil das Polynom f in $L_0[x]$ liegt, ist α algebraisch über L_0. Damit ist auch $L_0(\alpha)|L_0$ endlich. Mit Satz 15.6 können wir schließen, dass $L_0(\alpha)|K$ endlich ist. Aber dies bedeutet nach Proposition 15.14 (i) wiederum, dass $L_0(\alpha)|K$ algebraisch und insbesondere α algebraisch über K ist. □

Folgerung 15.16 Ist $L|K$ eine Körpererweiterung und $S \subseteq L$ eine Teilmenge mit der Eigenschaft, dass jedes $\alpha \in S$ algebraisch über K ist, dann ist $K(S)|K$ eine algebraische Erweiterung.

Beweis: Sei $T \subseteq L$ die Teilmenge der über K algebraischen Elemente von L. Nach Teil (i) von Satz 15.15 ist T ein Zwischenkörper von $L|K$, und es gilt $S \subseteq T$, nach Definition von S und T. Weil T ein Zwischenkörper von $L|K$ ist, folgt $K(S) \subseteq T$. Daraus folgt, dass jedes $\alpha \in K(S)$ über K algebraisch ist. Dies wiederum bedeutet, dass $K(S)|K$ eine algebraische Erweiterung ist. □

Anhang: Die quadratischen Erweiterungen von $\mathbb{Q}$

Eine Körpererweiterung $L|K$ vom Grad $[L : K] = 2$ wird auch *quadratische Erweiterung* genannt. Weil solche Erweiterungen in Beispielen (bzw. Übungsaufgaben) besonders häufig vorkommen, beweisen wir einige allgemeine Eigenschaften. Hierbei konzentrieren wir uns besonders auf den Fall des Grundkörpers $K = \mathbb{Q}$.

Proposition 15.17 Sei K ein Körper mit $\mathrm{char}(K) \neq 2$ und $L|K$ eine Erweiterung mit $[L : K] = 2$. Dann existiert ein $\gamma \in L$ mit $L = K(\gamma)$ und $\gamma^2 \in K$. (Man sagt dazu auch, dass L aus K durch Adjunktion einer ***Quadratwurzel*** entsteht.)

Beweis: Sei α ein beliebiges Element aus $L \setminus K$. Dann ist $K(\alpha)$ ein Zwischenkörper von $L|K$, und auf Grund der Gradformel gilt $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K] = 2$. Wegen $\alpha \notin K$ ist $K(\alpha) \neq K$ und somit $[K(\alpha) : K] > 1$. Weil $[K(\alpha) : K]$ zugleich ein Teiler von 2 ist, muss $[K(\alpha) : K] = 2$ und $[L : K(\alpha)] = 1$, also $L = K(\alpha)$ gelten. Sei $f = \mu_{\alpha,K}$

das Minimalpolynom von α über K. Wegen $\text{grad}(f) = [K(\alpha) : K] = 2$ gibt es $p, q \in K$ mit $f = x^2 + px + q$. Wegen $\text{char}(K) \neq 2$ existiert das multiplikative Inverse von $2_K = 1_K + 1_K$, das wir der Einfachheit halber mit $\frac{1}{2}$ bezeichnen. Ebenso schreiben wir $\frac{1}{4}$ für $\frac{1}{2} \cdot \frac{1}{2}$. Es gilt nun

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \alpha^2 + p\alpha + q = 0 \quad \Leftrightarrow \quad \alpha^2 + p\alpha + \tfrac{1}{4}p^2 = \tfrac{1}{4}p^2 - q \quad \Leftrightarrow \quad (\alpha + \tfrac{1}{2}p)^2 = \tfrac{1}{4}\delta$$

wobei $\delta = p^2 - 4q$ die ***Diskriminante*** des Polynoms f bezeichnet. Setzen wir nun $\gamma = \alpha + \frac{1}{2}p$, dann gilt $K(\alpha) = K(\gamma)$, denn offenbar ist $\gamma = \alpha + \frac{1}{2}p \in K(\alpha)$ und $\alpha = \gamma - \frac{1}{2}p \in K(\gamma)$. Daraus folgt $L = K(\gamma)$. Außerdem gilt $\gamma^2 = \frac{1}{4}\delta \in K$. □

Eine ganze Zahl $a \in \mathbb{Z}$ wird ***quadratfrei*** genannt, wenn keine Primzahl p mit $p^2 \mid a$ existiert.

Folgerung 15.18 Sei $K|\mathbb{Q}$ eine Erweiterung mit $[K : \mathbb{Q}] = 2$. Dann gibt es eine quadratfreie Zahl $m \in \mathbb{Z} \setminus \{0, 1\}$ mit $K = \mathbb{Q}(\sqrt{m})$.

Beweis: Nach Proposition 15.17 gibt es ein $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$ und $r = \alpha^2 \in \mathbb{Q}$. Sei $n \in \mathbb{N}$ so gewählt, dass $nr \in \mathbb{Z}$ gilt. Dann ist auch $K = \mathbb{Q}(n\alpha)$, und außerdem $n^2 r = (n\alpha)^2 \in \mathbb{Z}$. Wir können also α durch $n\alpha$ ersetzen und direkt davon ausgehen, dass $r \in \mathbb{Z}$ gilt. Dabei ist $r \neq 0$, denn andernfalls wäre auch $\alpha = 0$, somit $K = \mathbb{Q}(0) = \mathbb{Q}$ und schließlich $[K : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1$, im Widerspruch zur Voraussetzung. Sei nun $\prod_{i=1}^{t} p_i^{e_i}$ die Primfaktorzerlegung von $|r|$, mit $t \in \mathbb{N}_0$, $e_1, ..., e_t \in \mathbb{N}$ und den verschiedenen Primteilern $p_1, ..., p_t$ von r. Sei $\varepsilon \in \{\pm 1\}$ das Vorzeichen von r, es gelte also $r = \varepsilon|r|$. Wir definieren $e_i' = 0$, falls e_i gerade, und $e_i' = 1$, falls e_i ungerade ist. Setzen wir $m = \varepsilon \prod_{i=1}^{t} p_i^{e_i'}$, dann ist m offenbar quadratfrei. Außerdem unterscheiden sich r und m nur um ein Quadrat, es gibt also ein $n \in \mathbb{N}$ mit $r = n^2 m$. Aus $(\frac{1}{n}\alpha)^2 = (\frac{1}{n})^2 r = m$ folgt $\frac{1}{n}\alpha \in \{\pm\sqrt{m}\}$ und somit $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\frac{1}{n}\alpha) = \mathbb{Q}(\sqrt{m})$. Dabei ist $m = 0$ bereits ausgeschlossen. Wäre $m = 1$, dann würde $K = \mathbb{Q}(1) = \mathbb{Q}$ folgen, was wir weiter oben auch schon ausgeschlossen hatten. □

Satz 15.19 Seien $m, n \in \mathbb{Z} \setminus \{0, 1\}$ zwei verschiedene quadratfreie Zahlen. Dann gilt $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$, $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$, also insbesondere $\mathbb{Q}(\sqrt{m}) \neq \mathbb{Q}(\sqrt{n})$.

Beweis: Offenbar genügt es $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$ zu beweisen, denn der Beweis der anderen Aussage läuft völlig analog. Zunächst zeigen wir, dass $f = x^2 - m$ das Minimalpolynom von $\sqrt{m}$ über $\mathbb{Q}$ ist. Offenbar ist f normiert und erfüllt $f(\sqrt{m}) = 0$. Wäre f reduzibel, dann gäbe es $a, b \in \mathbb{Q}$ mit $x^2 - m = (x - a)(x - b) = x^2 - (a + b)x + ab$, woraus sich $b = -a$ und $m = -ab = a^2$ ergeben würde. Mit $m = a^2$ müsste auch a ganzzahlig sein (denn eine Primzahl p, die den Nenner, aber nicht den Zähler von a teilt, würde auch im Nenner einer Darstellung von a^2 als gekürzter Bruch auftreten). Dann aber steht $m = a^2$ im Widerspruch dazu, dass m eine quadratfreie Zahl ungleich 1 ist. Es gilt also tatsächlich $\mu_{\mathbb{Q},\sqrt{m}} = f$.

Nach Satz 15.10 gilt $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = \text{grad}(f) = 2$, und $\{1, \sqrt{m}\}$ ist eine Basis von $\mathbb{Q}(\sqrt{m})$ als $\mathbb{Q}$-Vektorraum. Nehmen wir nun an, es gilt $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$. Dann existieren also (eindeutig bestimmte) $r, s \in \mathbb{Q}$ mit $\sqrt{n} = r + s\sqrt{m}$. Durch Quadrieren erhalten wir $n = (r + s\sqrt{m})^2 = (r^2 + s^2 m) + 2rs\sqrt{m}$. Weil die Menge $\{1, \sqrt{m}\}$ im $\mathbb{Q}$-Vektorraum $\mathbb{Q}(\sqrt{m})$ linear unabhängig ist, dürfen wir in

$$(r^2 + s^2 m) \cdot 1 + (2rs) \cdot \sqrt{m} \quad = \quad n \cdot 1 + 0 \cdot \sqrt{m}$$

einen Koeffizientenvergleich durchführen. Wir erhalten $r^2 + s^2 m = n$ und $2rs = 0$, also $r = 0$ oder $s = 0$. Betrachten wir zunächst den Fall $s = 0$. Dann ist $r^2 = n$, was aber im Widerspruch dazu steht, dass n eine quadratfreie ganze Zahl ist, siehe oben. Im Fall $r = 0$ ist $s^2 m = n$. Schreiben wir $s = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $\mathrm{ggT}(a, b) = 1$, so erhalten wir $(\frac{a}{b})^2 m = n \Leftrightarrow a^2 m = b^2 n$. Nehmen wir an, die Zahl a besitzt einen Primteiler p. Wegen $\mathrm{ggT}(a, b) = 1$ und $p^2 \mid (a^2 m)$ muss dann $p^2 \mid n$ gelten. Aber dies widerspricht der Quadratfreiheit. Also muss $a^2 = 1$ gelten. Ebenso zeigt man $b^2 = 1$, so dass sich $m = n$ ergibt. Aber auch dies widerspricht unseren Voraussetzungen. Die Annahme $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$ wurde also insgesamt zu einem Widerspruch geführt. □

§ 16. *Fortsetzung von Körperhomomorphismen*

Zusammenfassung. In diesem Abschnitt beschäftigen wir uns mit der Frage, unter welchen Bedingungen ein Homomorphismus $\phi : K \to M$ von Körpern auf eine algebraische Erweiterung $L \supseteq K$ fortgesetzt werden kann, und falls ja, wieviele solcher Fortsetzungen existieren. Für den Fall, dass L von einem Element erzeugt wird, also $L = K(\alpha)$ für ein über K algebraisches Element α gilt, gibt eine einfache Antwort: Die Anzahl ist gleich der Anzahl der Nullstellen des Minimalpolynoms $\mu_{\alpha,K}$ im Körper M.

Wie im weiteren Verlauf deutlich werden wird, spielen Körperhomomorphismen und ihre Fortsetzung beim Studium algebraischer Erweiterungen eine wichtige Rolle. Im folgenden Abschnitt werden wir mit ihrer Hilfe zeigen, dass der algebraische Abschluss eines Körpers und (allgemeiner) Zerfällungskörper beliebiger Polynommengen bis auf Isomorphie eindeutig bestimmt sind. Die *normalen* und *separablen* Erweiterungen, die uns später begegnen werden, lassen sich durch Eigenschaften der Körperhomomorphismen charakterisieren. In der *Galoistheorie*, dem Hauptgegenstand der Vorlesung im nächsten Semester, bildet man Gruppen bestehend aus Körperhomomorphismen, mit deren Hilfe man Informationen über Struktur algebraischer Erweiterungen gewinnen kann.

Wichtige Grundbegriffe	***Zentrale Sätze***
– K-Homomorphismus	– eindeutige Festlegung einer Fortsetzung durch die Bilder der Erzeuger
– K-Automorphismus	– Existenz von Fortsetzungen auf endliche und algebraische Erweiterungen
– Fortsetzung eines Körperhomomorphismus	– Festlegung der Anzahl der Fortsetzungen durch die Nullstellen des Bildpolynoms in der Erweiterung

Zu Beginn des Kapitels legen wir folgende Notation fest.

(i) Sind L und M Körper, dann bezeichnen wir mit $\mathrm{Hom}(L, M)$ die Menge der Körperhomomorphismen $L \to M$. (Wir erinnern daran, dass nach Proposition 9.7 Körperhomomorphismen stets injektiv sind.)

(ii) Ist K ein gemeinsamer Teilkörper von L und M, dann bezeichnet $\mathrm{Hom}_K(L, M)$ die Menge der Körperhomomorphismen $\phi : L \to M$ mit $\phi(a) = a$ für alle $a \in K$. Solche Körperhomomorphismen werden auch ***K-Homomorphismen*** genannt.

(iii) Für jeden Körper L sei $\mathrm{Aut}(L)$ die Menge der Automorphismen von L, also die Menge der bijektiven Homomorphismen $L \to L$. Es ist leicht zu sehen, dass auf $\mathrm{Aut}(L)$ durch die Komposition $(\phi, \psi) \mapsto \phi \circ \psi$ eine Gruppenstruktur definiert ist.

(iv) Ist K ein Teilkörper L, dann bezeichnet $\mathrm{Aut}_K(L)$ die Teilmenge von $\mathrm{Aut}(L)$ bestehend aus den Automorphismen von L, die zugleich K-Homomorphismen sind. Man spricht in diesem Zusammenhang von ***K-Automorphismen***. Offenbar handelt es sich bei $\mathrm{Aut}_K(L)$ um eine Untergruppe von $\mathrm{Aut}(L)$.

Sei $L|K$ eine Körpererweiterung und $\phi : K \to \tilde{K}$ ein Homomorphismus von K in einen weiteren Körper $\tilde{K}$. Ein Homomorphismus $\psi : L \to \tilde{K}$ wird ***Fortsetzung*** von ϕ genannt, wenn $\psi|_K = \phi$ erfüllt ist. Zunächst formulieren wir die zentrale Aussage zur *Eindeutigkeit* von Fortsetzungen

Satz 16.1 Sei $L|K$ eine Körpererweiterung, $S \subseteq L$ eine Teilmenge mit $L = K(S)$ und $\phi : K \to \tilde{K}$ ein Homomorphismus in einen weiteren Körper $\tilde{K}$. Sind dann $\psi_1, \psi_2 : L \to \tilde{K}$ zwei Fortsetzungen von ϕ mit $\psi_1|_S = \psi_2|_S$, dann gilt $\psi_1 = \psi_2$.

Beweis: Wir überprüfen, dass die Teilmenge $M = \{\alpha \in L \mid \psi_1(\alpha) = \psi_2(\alpha)\}$ ein Zwischenkörper von $L|K$ ist, der S als Teilmenge enthält. Zunächst zeigen wir, dass M ein Teilring von L ist. Da ψ_1 und ψ_2 Ringhomomorphismen sind, gilt $\psi_1(1_L) = 1_{\tilde{K}} = \psi_2(1_L)$ und somit $1_L \in M$. Seien nun $\alpha, \beta \in M$ vorgegeben. Dann gilt $\psi_1(\alpha) = \psi_2(\alpha)$ und $\psi_1(\beta) = \psi_2(\beta)$. Es folgt $\psi_1(\alpha-\beta) = \psi_1(\alpha)-\psi_1(\beta) = \psi_2(\alpha)-\psi_2(\beta) = \psi_2(\alpha-\beta)$ und somit $\alpha-\beta \in M$. Durch eine analoge Rechnung erhält man $\alpha\beta \in M$. Damit ist die Teilring-Eigenschaft von M nachgewiesen. Ist $\alpha \neq 0_L$, dann gilt darüber hinaus $\psi_1(\alpha^{-1}) = \psi_1(\alpha)^{-1} = \psi_2(\alpha)^{-1} = \psi_2(\alpha^{-1})$ und somit $\alpha^{-1} \in M$. Also ist M sogar ein Teilkörper von L. Für alle $a \in K$ gilt wegen der Fortsetzungs-Eigenschaft $\psi_1|_K = \psi_2|_K = \phi$ die Gleichung $\psi_1(a) = \phi(a) = \phi_2(a)$ und somit $a \in M$. Somit ist K in M enthalten, und folglich ist M ein Zwischenkörper von $L|K$. Aus der Voraussetzung $\psi_1|_S = \psi_2|_S$ folgt schließlich noch $S \subseteq M$. Insgesamt ist M also ein Zwischenkörper von $L|K$ mit $S \subseteq M$. Wir erhalten $L = K(S) \subseteq M$, also $M = L$. Dies zeigt, dass ψ_1 und ψ_2 auf ganz L übereinstimmen. □

Wir formulieren einen wichtigen Spezialfall dieser Aussage: Gilt $L = K(\alpha)$ für ein $\alpha \in L$ und ist $\beta \in \tilde{K}$, dann gibt es für jeden Homomorphismus $\phi : K \to \tilde{K}$ und jedes $\beta \in \tilde{K}$ höchstens eine Fortsetzung $\psi_\beta : K(\alpha) \to \tilde{K}$ von ϕ mit der Eigenschaft $\psi_\beta(\alpha) = \beta$.

Nun befassen wir uns mit der ***Existenz*** von Fortsetzungen auf algebraische Erweiterungen. Auf Grund der universellen Eigenschaft der Polynomringe gibt es zu jedem Isomorphismus $\phi : K \to \tilde{K}$ von Körpern einen eindeutig bestimmen Homomorphismus $K[x] \to \tilde{K}[x]$ zwischen den Polynomringen gegeben durch $\sum_{i=0}^m a_i x^i \mapsto \sum_{i=0}^m \phi(a_i)x^i$. Offenbar handelt es sich dabei um einen Isomorphismus zwischen $K[x]$ und $\tilde{K}[x]$, den wir ebenfalls mit ϕ bezeichnen.

Satz 16.2 *(Fortsetzungssatz)*
Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern. Seien außerdem $L|K$ und $\tilde{L}|\tilde{K}$ Körpererweiterungen und $\alpha \in L$ ein über K algebraisches Element mit Minimalpolynom $f \in K[x]$. Ist dann $\tilde{\alpha} \in \tilde{L}$ eine Nullstelle von $\tilde{f} = \phi(f) \in \tilde{K}[x]$, dann gibt es eine eindeutig bestimmte Fortsetzung ψ von ϕ auf $K(\alpha)$ mit $\psi(\alpha) = \tilde{\alpha}$. Dieser Homomorphismus ψ definiert einen Isomorphismus zwischen den beiden Körpern $K(\alpha)$ und $\tilde{K}(\tilde{\alpha})$.

Beweis: Die Eindeutigkeit von ψ ist nach Satz 16.1 klar. Zum Nachweis der Existenz verwenden wir Satz 15.11. Dieser liefert uns Isomorphismen

$$\phi_1 : K[x]/(f) \to K(\alpha) \qquad \text{und} \qquad \phi_2 : \tilde{K}[x]/(\tilde{f}) \to \tilde{K}(\tilde{\alpha})$$

mit $\phi_1(x + (f)) = \alpha$ und $\phi_2(x + (\tilde{f})) = \tilde{\alpha}$ sowie $\phi_1(a + (f)) = a$ und $\phi_2(\tilde{a} + (\tilde{f})) = \tilde{a}$ für $a \in K$ und $\tilde{a} \in \tilde{K}$. Wir betrachten nun zusätzlich den Ringhomomorphismus $\rho : K[x] \to \tilde{K}[x]/(\tilde{f})$ gegeben durch $g \mapsto \phi(g) + (\tilde{f})$. Weil

die Abbildungen $\phi : K[x] \to \tilde{K}[x]$ und $\tilde{K}[x] \to \tilde{K}[x]/(\tilde{f})$, $h \mapsto h + (\tilde{f})$ surjektiv sind, ist auch ρ ein surjektiver Ringhomomorphismus. Außerdem ist $\ker(\rho) = (f)$, denn für alle $g \in K[x]$ gilt

$$g \in \ker(\rho) \quad \Leftrightarrow \quad \rho(g) = 0 + (\tilde{f}) \quad \Leftrightarrow \quad \phi(g) \in (\tilde{f}) \quad \Leftrightarrow \quad g \in (f) \quad ,$$

wobei wir im letzten Schritt verwendet haben, dass auf Grund der Isomorphismus-Eigenschaft von ϕ die Vielfachen des Polynoms genau auf die Vielfachen von $\tilde{f} = \phi(f)$ abgebildet werden. Wir können also den Homomorphiesatz für Ringe anwenden und erhalten einen Isomorphismus $\bar{\rho} : K[x]/(f) \to \tilde{K}[x]/(\tilde{f})$ mit $\bar{\rho}(x + (f)) = x + (\tilde{f})$.

Definieren wir nun den Isomorphismus ψ durch $\psi = \phi_2 \circ \bar{\rho} \circ \phi_1^{-1}$, dann gilt $\psi(\alpha) = (\phi_2 \circ \bar{\rho})(x + (f)) = \phi_2(x + (\tilde{f})) = \tilde{\alpha}$. Andererseits gilt für alle $a \in K$ auch $\psi(a) = (\phi_2 \circ \bar{\rho})(a + (f)) = \phi_2(\phi(a) + (\tilde{f})) = \phi(a)$, also $\psi|_K = \phi$. Als Isomorphismus $K(\alpha) \to \tilde{K}(\tilde{\alpha})$ ist ψ auch ein Homomorphismus $K(\alpha) \to \tilde{L}$ von Körpern. □

Häufig benötigt man auch die folgende Umkehrung des soeben bewiesenen Satzes.

Satz 16.3 Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern. Seien außerdem $L|K$ und $\tilde{L}|\tilde{K}$ Körpererweiterungen, $\alpha \in L$ und $f \in K[x]$ ein Polynom mit $f(\alpha) = 0$. Ist dann $\psi : K(\alpha) \to \tilde{L}$ ein Körperhomomorphismus mit $\psi|_K = \phi$, dann ist $\tilde{\alpha} = \psi(\alpha)$ eine Nullstelle von $\tilde{f} = \phi(f)$.

Beweis: Sei $n = \text{grad}(f)$ und $f = \sum_{i=0}^{n} a_i x^i$ mit $a_0, ..., a_n \in K$. Es gilt $\tilde{f} = \sum_{i=0}^{n} \phi(a_i) x^i$, und daraus folgt

$$\begin{aligned} \tilde{f}(\tilde{\alpha}) &= \sum_{i=0}^{n} \phi(a_i)\tilde{\alpha}^i = \sum_{i=0}^{n} \phi(a_i)\psi(\alpha)^i = \sum_{i=0}^{n} \psi(a_i)\psi(\alpha)^i \\ &= \psi\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \psi(f(\alpha)) = \psi(0) = 0. \end{aligned}$$

Dabei wurde im vierten Schritt die Homomorphismus-Eigenschaft von ψ verwendet. □

Insbesondere gilt also: Sind $L, \tilde{L}$ Erweiterungskörper von K, $f \in K[x]$, $\alpha \in L$ eine Nullstelle von f und $\psi : L \to \tilde{L}$ ein K-Homomorphismus, dann ist auch $\psi(\alpha)$ eine Nullstelle von f. Beispielsweise muss jeder $\mathbb{Q}$-Homomorphismus $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ das Element $\sqrt{2}$ auf $\sqrt{2}$ oder $-\sqrt{2}$ abbilden, denn dies sind die einzigen Nullstellen des Polynoms $f = x^2 - 2 \in \mathbb{Q}[x]$.

Folgerung 16.4 Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern. Seien außerdem $L|K$, $\tilde{L}|\tilde{K}$ Körpererweiterungen, $\alpha \in L$ algebraisch über K und $f = \mu_{K,\alpha}$. Dann stimmt die Anzahl der Fortsetzungen $\psi : K(\alpha) \to \tilde{L}$ von ϕ (also die Anzahl der Homomorphismen mit $\psi|_K = \phi$) überein mit der Anzahl der Nullstellen von $\tilde{f} = \phi(f)$ in $\tilde{L}$.

Beweis: Seien $s \in \mathbb{N}$ und $\beta_1, ..., \beta_s$ die verschiedenen Nullstellen von $\tilde{f}$ in $\tilde{L}$. Auf Grund des Fortsetzungssatzes gibt es für jedes $i \in \{1, ..., s\}$ eine eindeutig bestimmte Fortsetzung $\psi_i : K(\alpha) \to \tilde{L}$ von ϕ mit $\psi_i(\alpha) = \beta_i$. Ist umgekehrt $\psi : K(\alpha) \to \tilde{L}$ eine beliebige Fortsetzung von ϕ, dann ist $\psi(\alpha)$ nach Satz 16.3 eine Nullstelle von $\tilde{f}$, also gilt $\psi(\alpha) = \beta_i$ für ein i. Auf Grund der Eindeutigkeitsaussage im Fortsetzungssatz folgt daraus $\psi = \psi_i$. □

Folgerung 16.5 Für jede algebraische Erweiterung $L|K$ gilt $\mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$.

Beweis: Die Inklusion $\mathrm{Aut}_K(L) \subseteq \mathrm{Hom}_K(L,L)$ ist auf Grund der Definitionen trivial. Zum Beweis der umgekehrten Inklusion sei $\phi \in \mathrm{Hom}_K(L,L)$ vorgegeben. Als Körperhomomorphismus ist ϕ injektiv; zu zeigen bleibt die Surjektivität. Für vorgegebenes $\beta \in L$ müssen wir zeigen, dass ein $\alpha \in L$ mit $\phi(\alpha) = \beta$ existiert. Sei $f = \mu_{K,\beta}$ das Minimalpolynom von β über K und $N \subseteq L$ die Menge der Nullstellen von f in L. Nach Folgerung 12.5 handelt es sich bei N um eine endliche Menge; genauer gilt $|N| \leq \mathrm{grad}(f)$. Wir betrachten nun die eingeschränkte Abbildung $\phi|_N$. Als Einschränkung einer injektiven Abbildung ist auch $\phi|_N$ injektiv. Nach Satz 16.3 ist für jedes $\alpha \in N$ auch $\phi(\alpha)$ eine Nullstelle von f, also $\phi(\alpha) \in N$ und somit $\phi(N) \subseteq N$. Weil $\phi|_N : N \to N$ injektiv und die Menge N endlich ist, ist $\phi|_N$ auch surjektiv. Es gibt also ein $\alpha \in N$ mit $\phi(\alpha) = (\phi|_N)(\alpha) = \beta$. Damit ist die Surjektivität nachgewiesen. □

Im Fall einer *endlichen* Erweiterung $L|K$ kann man die Gleichung $\mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$ auch einfacher beweisen: Jeder K-Homomorphismus $\phi : L \to L$ ist verträglich mit der Addition und erfüllt für alle $a \in K$ und $\gamma \in L$ jeweils $\phi(a\gamma) = \phi(a)\phi(\gamma) = a\phi(\gamma)$, ist also ein Endomorphismus des endlich-dimensionalen K-Vektorraums L. Außerdem wissen wir bereits, dass Körperhomomorphismen stets injektiv sind. Aus der Linearen Algebra ist nun bekannt, dass jeder injektive Endomorphismus eines endlich-dimensionalen Vektorraums bijektiv ist; dies war eine Folgerung aus dem Dimensionssatz für lineare Abbildungen. Also ist ϕ in $\mathrm{Aut}_K(L)$ enthalten.

Als Anwendungsbeispiel der bisherigen Sätze zeigen wir, dass es genau drei $\mathbb{Q}$-Homomorphismen $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, aber nur einen einzigen $\mathbb{Q}$-Homomorphismus $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{R}$ gibt. Nach dem Eisenstein-Kriterium (Satz 13.11) ist das Polynom $f = x^3 - 2$ in $\mathbb{Q}[x]$ irreduzibel. Außerdem gilt $f(\sqrt[3]{2}) = 0$, also ist f nach Proposition 15.9 das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$.

Um die beiden nicht-reellen Nullstellen von x^3-2 darzustellen, benötigt man die Zahl $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Wegen $\zeta^3 = 1$ und $\zeta \neq 1$ bezeichnet man diese Zahl als ***primitive dritte Einheitswurzel***; wir werden solche Zahlen zusammen mit ihren Minimalpolynomen über $\mathbb{Q}$, den sogenannten Kreisteilungspolynomen, später systematisch untersuchen. Um die Gleichung $\zeta^3 = 1$ zu verifizieren, bemerken wir zunächst

$$\begin{aligned} \zeta^2 + \zeta + 1 &= \tfrac{1}{4}(-1+\sqrt{-3})^2 - \tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3} + 1 = \tfrac{1}{4}(-1+i\sqrt{3})^2 - \tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3} + 1 \\ &= \tfrac{1}{4}(1-2i\sqrt{3}-3) - \tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3} + 1 = -\tfrac{1}{2} - \tfrac{1}{2}i\sqrt{3} - \tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3} + 1 = 0. \end{aligned}$$

Daraus folgt dann $\zeta^3 - 1 = (\zeta - 1)(\zeta^2 + \zeta + 1) = (\zeta - 1) \cdot 0 = 0$. Mit Hilfe der Gleichung $\zeta^3 = 1$ lässt sich nun leicht überprüfen, dass $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$ die beiden nicht-reellen Nullstellen von f sind: Es gilt $f(\zeta\sqrt[3]{2}) = (\zeta\sqrt[3]{2})^3 = \zeta^3(\sqrt[3]{2})^3 - 2 = 1 \cdot 2 - 2 = 0$ und $f(\zeta^2\sqrt[3]{2}) = (\zeta^2\sqrt[3]{2})^3 - 2 = (\zeta^3)^2(\sqrt[3]{2})^3 - 2 = 1^2 \cdot 2 - 2 = 0$. Dies zeigt, dass $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$ die drei komplexen Nullstellen von f sind.

Die drei Nullstellen entsprechen nun nach Folgerung 16.4 drei verschiedenen Fortsetzungen $\psi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ von $\mathrm{id}_\mathbb{Q}$, also drei verschiedenen $\mathbb{Q}$-Homomorphismen. Wegen $\zeta \notin \mathbb{R}$ ist $\zeta\sqrt[3]{2}$ keine reelle Zahl, und wegen $\zeta^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3} \notin \mathbb{R}$ ist auch $\zeta^2\sqrt[3]{2}$ nicht reell. Dies bedeutet, dass $\sqrt[3]{2}$ die einzige Nullstelle von f in $\mathbb{R}$ ist. Folglich gibt es, wiederum nach Folgerung 16.4, nur einen einzigen $\mathbb{Q}$-Homomorphismus $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{R}$. Es handelt sich um die identische Abbildung $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{R}$, $\alpha \mapsto \alpha$.

Als Ergänzung bemerken wir noch, dass kein $\mathbb{Q}$-Homomorphismus $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}$ existiert, denn das Minimalpolynom $x^3 - 2$ von $\sqrt[3]{2}$ besitzt keine Nullstelle in $\mathbb{Q}$. Alternativ kann man das auch damit begründen, dass $\mathbb{Q}(\sqrt[3]{2})$ als $\mathbb{Q}$-Vektorraum dreidimensional ist und somit keine injektive lineare Abbildung in den eindimensionalen $\mathbb{Q}$-Vektorraum $\mathbb{Q}$ existiert.

Zum Schluss beweisen wir noch eine elementare Aussage zum Verhalten von Erzeugendensystemen unter Körperhomomorphismen, die wir im nachfolgenden Kapitel benötigen werden.

Lemma 16.6 Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern und $L|K$ und $\tilde{L}|\tilde{K}$ Körpererweiterungen. Sei $S \subseteq L$ eine Teilmenge und $\psi : L \to \tilde{L}$ eine Fortsetzung von ϕ. Dann gilt $\psi(K(S)) = \tilde{K}(\psi(S))$.

Beweis: Sei $M = \psi(K(S))$. Nach Definition des erzeugten Teilkörpers $\tilde{K}(\psi(S))$ ist zu zeigen:

(i) M ist ein Zwischenkörper von $\tilde{L}|\tilde{K}$, der $\psi(S)$ enthält.

(ii) Ist L_1 ein weiterer Zwischenkörper von $\tilde{L}|\tilde{K}$ mit $L_1 \supseteq \psi(S)$, dann folgt $L_1 \supseteq M$.

zu (i) Als Bild von $K(S) \subseteq L$ unter einem Körperhomomorphismus nach $\tilde{L}$ ist $\psi(K(S))$ auf jeden Fall ein Teilkörper von $\tilde{L}$. Dieser enthält $\tilde{K} = \phi(K) = \psi(K)$, also $\phi(K(S))$ ein Zwischenkörper von $\tilde{L}|\tilde{K}$. Außerdem ist wegen $S \subseteq K(S)$ auch $\psi(S)$ in $\psi(K(S))$ enthalten.

zu (ii) Es genügt zu zeigen, dass $K(S)$ in $\psi^{-1}(L_1)$ enthalten ist, denn die Anwendung von ψ auf beide Seiten dieser Gleichung liefert $M = \psi(K(S)) \subseteq \psi(\psi^{-1}(L_1)) \subseteq L_1$. Dazu reicht es zu überprüfen, dass $\psi^{-1}(L_1)$ ein Zwischenkörper von $L|K$ ist, der S als Teilmenge enthält.

Zunächst zeigen wir, dass $\psi^{-1}(L_1)$ ein Teilkörper von L ist. Weil L_1 ein Teilkörper von $\tilde{L}$ ist, gilt $\psi(1_L) = 1_{\tilde{L}} \in L_1$ und somit $1_L \in \psi^{-1}(L_1)$. Seien nun $\alpha, \beta \in \psi^{-1}(L_1)$ vorgegeben. Dann gilt $\psi(\alpha), \psi(\beta) \in L_1$. Weil L_1 ein Teilkörper von $\tilde{L}$ ist, liegen auch $\psi(\alpha - \beta) = \psi(\alpha) - \psi(\beta)$ und $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$ in L_1. Daraus folgt $\alpha - \beta \in \psi^{-1}(L_1)$ und $\alpha\beta \in \psi^{-1}(L_1)$. Ist außerdem $\alpha \neq 0_{\tilde{L}}$, dann gilt wegen $\psi(\alpha)\psi(\alpha^{-1}) = \psi(\alpha\alpha^{-1}) = \psi(1_L) = 1_{\tilde{L}}$ und der Teilkörper-Eigenschaft von L_1 auch $\psi(\alpha^{-1}) = \psi(\alpha)^{-1} \in L_1$ und damit $\alpha^{-1} \in \psi^{-1}(L_1)$.

Also ist $\psi^{-1}(L_1)$ tatsächlich ein Teilkörper von L. Wegen $\psi(K) = \phi(K) = \tilde{K} \subseteq L_1$ gilt $K \subseteq \psi^{-1}(L_1)$. Also ist $\psi^{-1}(L_1)$ ein Zwischenkörper von $L|K$. Wegen $\psi(S) \subseteq L_1$ enthält $\psi^{-1}(L_1)$ auch die Menge S. □

§ 17. *Zerfällungskörper und normale Erweiterungen*

Zusammenfassung. Ist $f \in K[x]$ ein nicht-konstantes Polynom, dann bezeichnet man einen minimalen Erweiterungskörper L von K, über dem f in Linearfaktoren zerfällt, als *Zerfällungskörper* von f über K. Ebenso kann jeder beliebigen Menge von nicht-konstanten Polynomen ein Zerfällungskörper zugeordnet werden. Wir zeigen, dass umgekehrt auch für jede Polynommenge ein entsprechender Zerfällungskörper existiert. Auf diese Weise können wir für jeden Körper K einen *algebraischen Abschluss* konstruieren. Dabei handelt es sich um eine Erweiterung $\tilde{K} \supseteq K$ mit der Eigenschaft, dass jedes nicht-konstante Polynom aus $\tilde{K}[x]$ über $\tilde{K}$ in Linearfaktoren zerfällt.

Erweiterungskörper von K, die als Zerfällungskörper zustande kommen, werden auch als *normale* Erweiterungen bezeichnet. Diese Erweiterungen $L|K$ können auch ohne Bezug auf ein bestimmtes Polynom oder eine Polynommenge charakterisiert werden, unter anderem durch die Automorphismengruppe $\mathrm{Aut}_K(L)$. Die normalen Erweiterungen werden sowohl in der Theorie der endlichen Körper als auch in der Galoistheorie eine wichtige Rolle spielen.

Wichtige Grundbegriffe

- Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[x]$, einer Menge von Polynomen
- algebraische Abgeschlossenheit
- algebraischer Abschluss eines Körpers
- normale Körpererweiterungen
- Konjugierte eines Elements

Zentrale Sätze

- Existenz und Eindeutigkeit des Zerfällungskörpers
- Existenz und Eindeutigkeit des algebraischen Abschlusses
- Fortsetzbarkeit von Körperhomomorphismen auf algebraische Erweiterungen
- Charakterisierung normaler Erweiterungen als Zerfällungskörper, durch die Automorphismengruppe

Wir beginnen mit der Definition des Zerfällungskörpers eines Polynoms.

Definition 17.1 Sei $L|K$ eine Körpererweiterung und $f \in K[x]$ ein nicht-konstantes Polynom. Zerfällt f über L in Linearfaktoren, und bezeichnen $\alpha_1, ..., \alpha_r$ die Nullstellen von f in L, dann nennt man $K(\alpha_1, ..., \alpha_r)$ den ***Zerfällungskörper*** von f in L über dem Grundkörper K.

Satz 17.2 Sei K ein Körper. Dann existiert zu jedem nicht-konstanten Polynom $f \in K[x]$ ein Zerfällungskörper von f über K.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über $n = \mathrm{grad}(f)$. Dabei können wir voraussetzen, dass f normiert ist, weil sich an den Nullstellen nichts ändert, wenn wir f mit einem Element $a \in K^\times$ multiplizieren. Im Fall $n = 1$ gilt dann $f = x - \alpha$ für ein $\alpha \in K$. Also ist $L = K(\alpha) = K$ der gesuchte Körper.

Sei nun $n \in \mathbb{N}$ und setzen wir die Aussage für Polynomgrade $m < n$ als gültig voraus. Sei f vom Grad n und $f_1 \in K[x]$ ein irreduzibler Faktor von f. Nach Satz 15.12 über die Existenz algebraischer Erweiterungen gibt es einen Erweiterungskörper M_0 von K und ein Element $\alpha_1 \in M_0$ mit $f(\alpha_1) = f_1(\alpha_1) = 0$. Sei $M = K(\alpha_1)$ und $g \in M[x]$ mit $f = (x - \alpha_1)g$. Wegen $\text{grad}(g) < \text{grad}(f) = n$ können wir die Induktionsvoraussetzung auf $g \in M[x]$ anwenden. Wir erhalten einen Erweiterungskörper L von M, so dass das Polynom g über L in Linearfaktoren zerfällt, $g = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_r)$, und $L = M(\alpha_2, \ldots, \alpha_r)$ gilt. Es folgt

$$f = (x - \alpha_1)(x - \alpha_2) \cdot \ldots \cdot (x - \alpha_r) \qquad \text{und} \qquad L = M(\alpha_2, \ldots, \alpha_r) = K(\alpha_1, \alpha_2, \ldots, \alpha_r). \qquad \square$$

Nach Satz 15.14 ist jeder Zerfällungskörper eines Polynoms $f \in K[x]$ algebraisch über K, weil er von endlich vielen algebraischen Elementen erzeugt wird.

Betrachten wir das bereits in der Einleitung angekündigte Beispiel mit dem Grundkörpers $K = \mathbb{Q}$ und dem Polynom $f = x^3 - 2 \in \mathbb{Q}[x]$. Offenbar ist $\sqrt[3]{2}$ eine Nullstelle von f in $\mathbb{R}$. Allerdings zerfällt f über $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren. Statt dessen besitzt f über diesem Körper die Zerlegung

$$f \quad = \quad (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}).$$

Der quadratische Faktor mit den Koeffizienten $p = \sqrt[3]{2}$ und $q = \sqrt[3]{4}$ besitzt die negative Diskriminante $p^2 - 4q = (\sqrt[3]{2})^2 - 4\sqrt[4]{3} = \sqrt[3]{4} - 4\sqrt[4]{3} = (-3)\sqrt[4]{3}$, hat also keine reellen Nullstellen. Wegen $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ ist somit gezeigt, dass der quadratische Faktor in $\mathbb{Q}(\sqrt[3]{2})$ tatsächlich nicht in Linearfaktoren zerlegt werden kann. Dies kann man auch anhand der drei komplexen Nullstellen von $x^3 - 2$ überprüfen: Wie wir in § 12 gesehen haben, sind dies neben $\sqrt[3]{2}$ die beiden nicht-reellen Zahlen $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$. Letztere müssen zugleich auch die Nullstellen des quadratischen Faktors sein, was auch direkt nachrechnen kann: Wegen $1 + \zeta + \zeta^2 = 0$ gilt

$$(x - \zeta\sqrt[3]{2})(x - \zeta^2\sqrt[3]{2}) \quad = \quad x^2 - (\zeta + \zeta^2)\sqrt[3]{2}x + \zeta^3\sqrt[3]{4} \quad = \quad x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$$

Insgesamt gilt also $x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta\sqrt[3]{2})(x - \zeta^2\sqrt[3]{2})$. Dies zeigt, dass der Zerfällungskörper von f über $\mathbb{Q}$ durch $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ gegeben ist. Für die letzte Gleichung genügt es, die Inklusionen $\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\} \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta)$ und $\{\sqrt[3]{2}, \zeta\} \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})$ zu überprüfen; bei der zweiten Inklusion verwendet man $\zeta = \zeta\sqrt[3]{2}/\sqrt[3]{2}$.

Man beachte, dass das Polynom f in Satz 17.2 auch reduzibel über dem Grundkörper $\mathbb{Q}$ sein darf. Ist beispielsweise $f = (x^2 - 2)(x^2 - 3)(x - 5) \in \mathbb{Q}[x]$ und $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, dann ist K einZerfällungskörper von f über $\mathbb{Q}$, denn die Nullstellen von f sind $\pm\sqrt{2}$, $\pm\sqrt{3}$ und 5, und es gilt

$$K \quad = \quad \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}, 5).$$

Wir erweitern nun die Definition des Zerfällungskörpers nun von *einem* Polynom auf eine beliebige *Menge* von Polynomen.

Definition 17.3 Sei $L|K$ eine Körpererweiterung, und $S \subseteq K[x]$ eine (möglicherweise unendliche) Menge von nicht-konstanten Polynomen, die über L alle in Linearfaktoren zerfallen. Weiter sei $N \subseteq L$ die Menge aller Nullstellen sämtlicher Polynome aus S in L, also

$$N \quad = \quad \{\alpha \in L \mid f(\alpha) = 0 \text{ für ein } f \in S\}.$$

Dann wird $K(N)$ als ***Zerfällungskörper*** von S über dem Grundkörper K bezeichnet.

Auch hier kann man zeigen

Satz 17.4 Ist K ein Körper und $S \subseteq K[x]$ eine Menge nicht-konstanter Polynome, dann existiert ein Zerfällungskörper von S über K.

Ist die Teilmenge $S \subseteq K[x]$ endlich, dann folgt die Aussage direkt aus Satz 17.2. Bezeichnet nämlich $g \in K[x]$ das Produkt aller Polynome aus S, dann ist jeder Zerfällungskörper von g, wie man unmittelbar überprüft, auch ein Zerfällungskörper von S. Für den Beweis im allgemeinen Fall benötigt man nichttriviale Hilfsmittel aus der Mengenlehre, unter anderem das sog. ***Zornsche Lemma***. Aus algebraischer Sicht bietet der Beweis aber wenig Neues, weshalb wir ihn in einen Anhang zu diesem Kapitel verschieben.

Proposition 17.5 Sei K ein Körper und $S \subseteq K[x]$ eine beliebige Menge nicht-konstanter Polynome. Dann ist jeder Zerfällungskörper von S über K eine algebraische Erweiterung von K.

Beweis: Dies ergibt sich direkt aus Folgerung 15.16, weil jeder Zerfällungskörper durch Adjunktion von Nullstellen von Polynomen über K entsteht, also durch Adjunktion von Elementen, die über K algbraisch sind. □

Wir wenden uns nun einem besonders wichtigen Typ von Zerfällungskörpern zu, dem *algebraischen Abschluss* eines Körpers K. Zunächst definieren wir

Definition 17.6 Ein Körper K heißt ***algebraisch abgeschlossen***, wenn jedes nicht-konstante Polynom $f \in K[x]$ in K eine Nullstelle besitzt.

Durch vollständige Induktion über den Polynomgrad $\operatorname{grad}(f)$ zeigt man leicht, dass jedes nicht-konstante Polynom $f \in K[x]$ über K in Linearfaktoren zerfällt, wenn K algebraisch abgeschlossen ist. Wie bereits oben bemerkt, besitzt der Körper $\mathbb{C}$ der komplexen Zahlen die Eigenschaft der algebraischen Abgeschlossenheit.

Definition 17.7 Sei K ein Körper. Ein Erweiterungskörper L von K wird ***algebraischer Abschluss*** von K genannt, wenn $L|K$ algebraisch und L algebraisch abgeschlossen ist.

Unser nächstes Ziel besteht in dem Nachweis, dass jeder Körper K einen algebraischen Abschluss besitzt, und dass dieser „im Wesentlichen“ eindeutig bestimmt ist. Auch für den Zerfällungskörper eines Polynoms $f \in K[x]$ werden wir einen entsprechende Eindeutigkeitsaussage beweisen.

Proposition 17.8 Für jede Erweiterung $L|K$ sind die folgende Aussagen äquivalent.

(i) Der Körper L ist ein algebraischer Abschluss von K.

(ii) Die Erweiterung $L|K$ ist algebraisch, und jedes nicht-konstante Polynom $f \in K[x]$ zerfällt über L in Linearfaktoren.

(iii) Die Erweiterung $L|K$ ist *minimal* mit der Eigenschaft, dass jedes nicht-konstante Polynom $f \in K[x]$ über L in Linearfaktoren zerfällt. Es gibt also abgesehen von L selbst keinen Zwischenkörper von $L|K$ mit dieser Eigenschaft.

Beweis: Die Implikation „(i) ⇒ (ii)“ ist auf Grund der Definitionen trivial. Zum Beweis von „(ii) ⇒ (iii)“ setzen wir voraus, dass $L|K$ algebraisch ist, und dass jedes nicht-konstante Polynom $f \in K[x]$ über L in Linearfaktoren zerfällt. Sei L_1 ein beliebiger Zwischenkörper von $L|K$ mit derselben Eigenschaft; zu zeigen ist $L_1 = L$. Die Inklusion $L_1 \subseteq L$ ist offenbar erfüllt. Für den Beweis der umgekehrten Inklusion sei $\alpha \in L$ vorgegeben. Das Minimalpolynom $f = \mu_{\alpha,K}$ ist nicht-konstant, zerfällt also über L_1 in Linearfaktoren. Weil α eine Nullstelle von f ist, muss α in L_1 liegen.

Nun zeigen wir noch die Implikation „(iii) ⇒ (i)“. Setzen wir voraus, dass $L|K$ die unter (iii) angegebene Minimalitätseigenschaft besitzt. Zunächt zeigen wir, dass $L|K$ algebraisch ist. Sei dazu $T \subseteq L$ die Menge der über K algebraischen Elemente; zu zeigen ist $T = L$. Sei dazu $S_K \subseteq K[x]$ die Menge aller nicht-konstanten Polynome und $N = \{\alpha \in L \mid f(\alpha) = 0 \text{ für ein } f \in S_K\}$. Jedes Polynom aus S_K zerfällt nicht nur über L, sondern bereits über $K(N)$ in Linearfaktoren. Auf Grund der Minimalitätseigenschaft gilt also $L = K(N)$. Nach Satz 15.15 ist T ein Zwischenkörper von $L|K$, der offenbar N enthält. Es folgt $L = K(N) \subseteq T \subseteq L$ und somit $T = L$.

Es bleibt zu zeigen, dass $L|K$ algebraisch abgeschlossen ist. Für ein beliebig vorgegebenes nicht-konstantes Polynom $f \in L[x]$ ist die Existenz einer Nullstelle von f in L nachzuweisen. Sei $\tilde{L} \supseteq L$ ein Zerfällungskörper von f über L und $\alpha \in \tilde{L}$ eine beliebige Nullstelle von f. Mit $L(\alpha)|L$ und $L|K$ ist nach Satz 15.15 auch die Erweiterung $L(\alpha)|K$ algebraisch. Sei $h \in K[x]$ das Minimalpolynom von α über K. Nach Voraussetzung zerfällt h über L in Linearfaktoren. Aus $h(\alpha) = 0$ folgt $\alpha \in L$. □

Folgerung 17.9 Sei $L|K$ eine Körpererweiterung und $S_K \subseteq K[x]$ die Menge aller nicht-konstanten Polynome über K. Genau dann ist L ein algebraischer Abschluss von K, wenn L ein Zerfällungskörper von S_K ist.

Beweis: Als Zerfällungskörper von S_K ist L jedenfalls algebraisch über K. Außerdem zerfällt jedes nicht-konstante Polynom aus $K[x]$ über L in Linearfaktoren. Auf Grund der Richtung „(ii) ⇒ (i)“ in Satz 17.8 ist L damit ein algebraischer Abschluss von K. Setzen wir umgekehrt voraus, dass L ein algebraischer Abschluss von K ist. Dann zerfällt jedes Polynom aus S_K über L in Linearfaktoren. Außerdem wird L über K durch die Menge der Nullstellen der Polynome $f \in S_K$ erzeugt, da jedes $\alpha \in L$ jeweils Nullstelle von $\mu_{\alpha,K} \in S_K$ ist. Also ist L ein Zerfällungskörper von S_K über K. □

Wegen Satz 17.4 ergibt sich aus Folgerung 17.9, dass jeder Körper K einen algebraischen Abschluss besitzt. Außerdem stellen wir fest: Ist K ein Körper und $\tilde{L}$ ein algebraisch abgeschlossener Erweiterungskörper von K, dann ist

$$\tilde{K} \quad = \quad \{\alpha \in \tilde{L} \mid \alpha \text{ algebraisch über } K\}$$

der eindeutig bestimmte algebraische Abschluss von K in $\tilde{L}$. Denn offenbar ist $\tilde{K}$ der Zerfällungskörper der Menge $S_K \subseteq K[x]$ aller nicht-konstanten Polynome. Die Behauptung folgt ist somit eine Konsequenz von Folgerung 17.9. Es ist also gerechtfertigt, von *dem* algebraischen Abschluss eines Körpers K in einem algebraisch abgeschlossenen Erweiterungskörper $\tilde{L} \supseteq K$ zu sprechen.

Ist insbesondere K ein Zwischenkörper $\mathbb{C}|\mathbb{Q}$, dann ist $\tilde{K} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } K\}$ der eindeutig bestimmte algebraische Abschluss von K in $\mathbb{C}$. Man beachte, dass $\mathbb{C}$ selbst kein algebraischer Abschluss von $\mathbb{Q}$ ist, denn dies würde bedeuten, dass $\mathbb{C}|\mathbb{Q}$ eine algebraische Erweiterung ist. Wie wir in § 11 bemerkt haben, gibt es in $\mathbb{C}$ aber Elemente, die über $\mathbb{Q}$ transzendent sind, zum Beispiel e und π.

Unser nächstes Ziel ist der Beweis der Eindeutigkeit des algebraischen Abschlusses eines Körpers K bis auf K-Isomorphie. Dies soll bedeuten: Sind $\tilde{K}_1$ und $\tilde{K}_2$ zwei algebraische Abschlüsse von K, dann gibt es einen K-Isomorphismus $\tilde{K}_1 \to \tilde{K}_2$.

Proposition 17.10 Sei $L|K$ eine algebraische Erweiterung, $\tilde{K}$ ein algebraisch abgeschlossener Körper und $\phi : K \to \tilde{K}$ ein Homomorphismus von Körpern. Dann gibt es eine Fortsetzung ψ von ϕ auf den Körper L, also einen Homomorphismus $\psi : L \to \tilde{K}$ mit $\psi|_K = \phi$.

Beweis: Wir beschränken uns auf den Fall, dass die Erweiterung $L|K$ endlich ist. Den unendlichen Fall bearbeitet man auch hier mit Hilfe des Zornschen Lemmas (siehe Anhang). Der Beweis wird durch vollständige Induktion über $n = [L : K]$ geführt. Ist $n = 1$, dann gilt $L = K$, und wir können einfach $\psi = \phi$ setzen.

Sei nun $n \in \mathbb{N}$, und setzen wird die Aussage für Erweiterungen vom Grad $< n$ voraus. Sei $\alpha \in L \setminus K$ ein beliebiges Element und $f \in K[x]$ das Minimalpolynom von α über K. Weil $\tilde{K}$ algebraisch abgeschlossen ist, besitzt das Polynom $\tilde{f} = \phi(f)$ eine Nullstelle $\tilde{\alpha}$ in $\tilde{K}$. Wir wenden nun den Fortsetzungssatz, Satz 16.2, auf den Isomorphismus $\phi : K \to \phi(K)$ an und erhalten einen (eindeutig bestimmten) Homomorphismus $\hat{\phi} : K(\alpha) \to \tilde{K}$ mit $\hat{\phi}(\alpha) = \tilde{\alpha}$ und $\hat{\phi}|_K = \phi$. Wegen $\alpha \notin K$ ist $[K(\alpha) : K] > 1$, und nach dem Gradsatz gilt

$$[L : K(\alpha)] \quad = \quad \frac{[L : K]}{[K(\alpha) : K]} \quad < \quad [L : K] \quad = \quad n.$$

Wir können somit die Induktionsvoraussetzung auf die Erweiterung $L|K(\alpha)$ anwenden und erhalten einen Homomorphismus $\psi : L \to \tilde{K}$ mit $\psi|_{K(\alpha)} = \hat{\phi}$. Es folgt $\psi|_K = (\psi|_{K(\alpha)})|_K = \hat{\phi}|_K = \phi$. □

Satz 17.11 Sei K ein Körper und $S \subseteq K[x]$ eine Menge bestehend aus nicht-konstanten Polynomen. Sei $\phi : K \to \tilde{K}$ ein Isomorphismus von Körpern und $\tilde{S} = \{\phi(f) \mid f \in S\}$. Sei L ein Zerfällungskörper von S und $\tilde{L}$ ein Zerfällungskörper von $\tilde{S}$. Dann gibt es einen Isomorphismus $\psi : L \to \tilde{L}$ mit $\psi|_K = \phi$.

Beweis: Sei $\hat{L}$ ein algebraischer Abschluss von $\tilde{L}$. Weil der Körper $\hat{L}$ algebraisch abgeschlossen ist, kann ϕ nach 17.10 zu einem Homomorphismus $\psi : L \to \hat{L}$ fortgesetzt werden. Zu zeigen ist $\psi(L) = \tilde{L}$.

Sei N die Menge der Nullstellen aller Polynome $f \in S$ in L, und sei $\tilde{N} \subseteq \tilde{L}$ die entsprechende Menge für $\tilde{S}$. Nach Definition der Zerfällungskörper gilt $L = K(N)$ und $\tilde{L} = \tilde{K}(\tilde{N})$. Für jedes $\alpha \in N$ gibt es ein $f \in S$ mit $f(\alpha) = 0$. Wegen $\phi = \psi|_K$ ist $\psi(\alpha)$ nach Satz 16.3 eine Nullstelle von $\tilde{f} = \phi(f)$. Es folgt $\psi(\alpha) \in \tilde{N}$ und insgesamt $\psi(N) \subseteq \tilde{N}$. Mit Lemma 16.6 erhalten wir

$$\psi(L) \quad = \quad \psi(K(N)) \quad = \quad \tilde{K}(\psi(N)) \quad \subseteq \quad \tilde{K}(\tilde{N}) \quad = \quad \tilde{L}.$$

Nun zeigen wir, dass jedes nicht-konstante Polynom aus $\tilde{S}$ über dem Körper $\psi(L)$ in Linearfaktoren zerfällt. Sei also $\tilde{f} \in \tilde{S}$ vorgegeben und $f \in S$ mit $\tilde{f} = \phi(f)$. Weil L ein Zerfällungskörper von S ist, zerfällt f über L in Linearfaktoren. Es gibt also ein $c \in K$ und $\alpha_1, ..., \alpha_n \in L$ mit $f = c(x - \alpha_1) \cdot ... \cdot (x - \alpha_n)$, wobei $n = \text{grad}(f)$ ist. Anwendung von ψ auf diese Gleichung liefert

$$\tilde{f} \quad = \quad \phi(f) \quad = \quad \psi(f) \quad = \quad \phi(c)(x - \psi(\alpha_1)) \cdot ... \cdot (x - \psi(\alpha_n)) \quad ,$$

und es gilt $\psi(\alpha_i) \in \psi(L)$ für $1 \leq i \leq n$. Dies zeigt, dass die Nullstellen sämtlicher Polynome $\tilde{f} \in \tilde{S}$ in $\tilde{L}$ bereits in $\psi(L)$ enthalten sind. Damit ist $\psi(L)$ ein Zwischenkörper von $\tilde{L}|\tilde{K}$ mit $\psi(L) \supseteq \tilde{N}$. Weil $\tilde{L} = \tilde{K}(\tilde{N})$ nach Definition der *kleinste* Zwischenkörper von $\tilde{L}|\tilde{K}$ mit dieser Eigenschaft ist, folgt $\tilde{L} \subseteq \psi(L)$. Insgesamt ist damit $\psi(L) = \tilde{L}$ nachgewiesen. □

Folgerung 17.12 Sei K ein Körper, und seien L, $\tilde{L}$ algebraische Abschlüsse von K. Dann existiert ein K-Isomorphismus zwischen L und $\tilde{L}$.

Beweis: Nach 17.9 sind L und $\tilde{L}$ beide Zerfällungskörper der Menge S_K aller nicht-konstanten Polynome über K. Somit existiert nach Satz 17.11 ein Isomorphismus $\psi : L \to \tilde{L}$ mit $\psi|_K = \mathrm{id}_K$, also ein K-Isomorphismus. □

Definition 17.13 Eine algebraische Körpererweiterung $L|K$ heißt ***normal***, wenn folgende Bedingung erfüllt ist: Ist $f \in K[x]$ ein irreduzibles Polynom, das in L eine Nullstelle besitzt, dann zerfällt f über L in Linearfaktoren.

Proposition 17.14 Sei $L|K$ eine Körpererweiterung vom Grad 2. Dann ist $L|K$ normal.

Beweis: Sei $f \in K[x]$ ein irreduzibles Polynom, das in L eine Nullstelle α besitzt. Dabei können wir uns auf den Fall beschränken, dass f normiert und somit das Minimalpolynom von α ist. Wegen $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K] = 2$ gilt $\mathrm{grad}(f) = [K(\alpha) : K] \in \{1, 2\}$. Im Fall $\mathrm{grad}(f) = 1$ ist f bereits ein lineares Polynom. Im Fall $\mathrm{grad}(f) = 2$ ist $x - \alpha$ ein Teiler von $f \in L[x]$. Es gibt somit ein Polynom $\mathrm{grad}(g)$ vom Grad 1 mit $f = (x - \alpha)g$. Also zerfällt f auch in diesem Fall über L in Linearfaktoren. □

Wenn wir nach Gegenbeispielen zu normalen Erweiterungen suchen, müssen wir uns also auf solche vom Grad ≥ 3 konzentrieren. Sei etwa $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$, wobei wir beide Körper als Teilkörper von $\mathbb{R}$ betrachten. Dann ist die Erweiterung $L|K$ *nicht* normal. Denn das Polynom $f = x^3 - 2 \in K[x]$ ist nach dem Eisenstein-Kriterium irreduzibel über K, besitzt aber andererseits in L eine Nullstelle, nämlich $\sqrt[3]{2}$. Wäre $L|K$ normal, dann müsste f über $\mathbb{Q}(\sqrt[3]{2})$ in Linearfaktoren zerfallen. Aber wir haben bereits im Abschnitt über Zerfällungskörper gesehen, dass dies nicht der Fall ist.

Durch den folgende Satz wird gezeigt, dass normale Erweiterungskörper nichts weiter als Zerfällungskörper von Polynomen des Grundkörpers sind. Die zusätzliche Charakterisierung über die Körperhomomorphismen werden wir später in der Galoistheorie verwenden.

Satz 17.15 Sei K ein Körper, und seien $\tilde{K} \supseteq L \supseteq K$ Erweiterungen von K, wobei $L|K$ endlich und $\tilde{K}$ algebraisch abgeschlossen ist. Dann sind folgende Aussagen äquivalent:

(i) $L|K$ ist normal.

(ii) Es gibt ein nicht-konstantes Polynom $f \in K[x]$, so dass L der Zerfällungskörper von f über K ist.

(iii) Es gilt $\mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L)$.

Beweis: „(i) ⇒ (ii)“ Da $L|K$ endlich ist, gibt es über K algebraische Elemente $\alpha_1, ..., \alpha_r \in L$ mit $L = K(\alpha_1, ..., \alpha_r)$ (wähle zum Beispiel eine K-Basis von L). Für jedes $i \in \{1, ..., r\}$ sei $f_i \in K[x]$ das Minimalpolynom von α_i und $f = \prod_{i=1}^{r} f_i$. Jedes f_i besitzt offenbar in L eine Nullstelle. Weil $L|K$ normal ist, zerfällt jedes f_i und damit auch das Polynom f über L in Linearfaktoren, und zugleich wird f von den Nullstellen von f erzeugt. Also ist L ein Zerfällungskörper von f.

„(ii) ⇒ (iii)“ Die Inklusion „⊇“ ist auf Grund der Definition von $\mathrm{Hom}_K(L, \tilde{K})$ und $\mathrm{Aut}_K(L)$ klar. Zum Nachweis von „⊆“ sei nun $\phi \in \mathrm{Hom}_K(L, \tilde{K})$ vorgegeben. Außerdem setzen wir voraus, dass L der Zerfällungskörper des nichtkonstanten Polynoms $f \in K[x]$ ist. Dann gilt $L = K(\alpha_1, ..., \alpha_r)$, wobei $\alpha_1, ..., \alpha_r \in L$ die verschiedenen Nullstellen von f sind. Für jedes i ist $\phi(\alpha_i)$ nach Satz 16.3 ebenfalls eine Nullstelle von f und liegt damit in L. Aus

$$\phi(\{\alpha_1, ..., \alpha_r\}) \quad \subseteq \quad \{\alpha_1, ..., \alpha_r\}$$

erhalten wir durch Anwendung von Lemma 16.6 die Inklusion $\phi(L) \subseteq L$, d.h. $\phi(L)$ ist ein Teilkörper von L. Weil ϕ aber injektiv ist, muss der Grad $[\phi(L) : K]$ mit $[L : K]$ übereinstimmen. Es folgt $\phi(L) = L$ und somit $\phi \in \mathrm{Aut}_K(L)$.

„(iii) ⇒ (i)“ Sei $f \in K[x]$ ein irreduzibles Polynom, das in L eine Nullstelle α besitzt. Zu zeigen ist, dass f über L in Linearfaktoren zerfällt. Zumindest zerfällt f über dem Körper $\tilde{K}$, da dieser algebraisch abgeschlossen ist. Sei $\beta \in \tilde{K}$ eine beliebige weitere Nullstelle von f. Auf Grund des Fortsetzungssatzes gibt es einen K-Homomorphismus $\phi : K(\alpha) \to \tilde{K}$ mit $\phi(\alpha) = \beta$. Nach Proposition 16.2 gibt es eine Fortsetzung $\psi : L \to \tilde{K}$ von ϕ auf L. Dieses ψ ist nach Definition in $\mathrm{Hom}_K(L, \tilde{K})$ enthalten. Nach Voraussetzung gilt $\mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L)$, also ist $\beta = \phi(\alpha) = \psi(\alpha)$ in L enthalten. Jede Nullstelle von f liegt also bereits in L, d.h. f zerfällt über L in Linearfaktoren. □

Sei $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \in \mathbb{C}$ und $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$. Dann ist die Erweiterung $L|\mathbb{Q}$ normal, denn wie wir in § 13 gezeigt haben, handelt es sich bei L um den Zerfällungskörper des Polynoms $x^3 - 2 \in \mathbb{Q}[x]$. Nach Satz 17.15 (iii) ist jeder $\mathbb{Q}$-Homomorphismus $\phi : L \to \mathbb{C}$ ein $\mathbb{Q}$-Automorphismus von L.

Definition 17.16 Sei $L|K$ eine normale Erweiterung und $\alpha \in L$. Dann werden die Nullstellen des Minimalpolynoms $\mu_{\alpha,K}$ in L die ***Konjugierten*** des Element α über K genannt.

Zum Beispiel sind die Konjugierten eines Elements $z \in \mathbb{C}$ über $\mathbb{R}$ stets das Element z selbst und das konjugiert-komplexe Element $\bar{z}$.

Auf Grund des Fortsetzungssatzes und wegen Satz 17.15 lassen sich die Konjugierten in einer normalen Erweiterung $L|K$ auch folgendermaßen charakterisieren: Sei $\alpha \in L$ vorgegeben. Ein Element $\beta \in L$ ist genau dann über K zu α konjugiert, wenn ein $\sigma \in \mathrm{Aut}_K(L)$ mit $\sigma(\alpha) = \beta$ existiert. Sei nämlich $\hat{L}$ ein algebraischer Abschluss von L. Ist β eine Nullstelle von $f = \mu_{\alpha,K} \in K[x]$, dann gibt es auf Grund des Fortsetzungssatzes einen K-Homomorphismus $\sigma : L \to \hat{L}$, und wegen Satz 17.15 (iii) ist σ in $\mathrm{Aut}_K(L)$ enthalten. Ist umgekehrt $\beta \in L$ ein Element, für das ein $\sigma \in \mathrm{Aut}_K(L)$ mit $\sigma(\alpha) = \beta$ existiert, dann ist mit α nach Satz 16.3 auch β eine Nullstelle von f. Zum Schluss untersuchen wir noch, wie sich die Eigenschaft „normal“ bei Türmen von Körpererweiterungen verhält.

Proposition 17.17 Ist $L|K$ eine normale Erweiterung und M ein Zwischenkörper von $L|K$, dann ist auch die Erweiterung $L|M$ normal.

Beweis: Sei $f \in M[x]$ ein irreduzibles Polynom und $\alpha \in L$ eine Nullstelle von f. Zu zeigen ist, dass f über L in Linearfaktoren zerfällt. Nach Multiplikation von f mit einem $\alpha \in M^\times$ können wir voraussetzen, dass f normiert ist. Dann ist f das Minimalpolynom von α über M. Das Minimalpolynom $g \in K[x]$ von α über K zerfällt über L in Linearfaktoren, weil die Erweiterung $L|K$ normal ist. Nun ist g auch ein Polynom in $M[x]$ mit $g(\alpha) = 0$ und damit ein Vielfaches des Minimalpolynoms f von α über L. Mit g zerfällt also auch f über L in Linearfaktoren. □

Aus den Voraussetzungen von Proposition 17.17 folgt *nicht*, dass auch die auch die untere Teilerweiterung $M|K$ normal ist. Als Beispiel betrachten wir die Körper

$$K = \mathbb{Q} \quad , \quad M = \mathbb{Q}(\sqrt[3]{2}) \quad \text{und} \quad L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$$

mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Wir haben bereits festgestellt, dass $L|K$ eine normale Erweiterung ist, und auf Grund der Proposition gilt dasselbe für die Erweiterung $L|M$. Aber $M|K$ ist nicht normal, wie wir im Beispiel von oben gesehen haben. Ebenso wenig folgt im Allgemeinen aus der Normalität der beiden Teilerweiterungen $M|K$ und $L|M$, dass die Gesamterweiterung $L|K$ normal ist.

Anhang: Unendliche algebraische Erweiterungen und Zornsches Lemma

In diesem Anhang werden die vollständigen Beweise von Satz 17.4 und Proposition 17.10 nachgeliefert.

Zunächst wiederholen wir einige Grundbegriffe der Mengenlehre, die bereits im ersten Semester eingeführt wurden. Eine Relation $\preceq$ auf einer Menge X heißt ***reflexiv***, wenn $x \preceq x$ für alle $x \in X$ gilt, ***anti-symmetrisch***, wenn für alle $x, y \in X$ aus $x \preceq y$ und $y \preceq x$ jeweils $x = y$ folgt, und ***transitiv***, wenn für alle $x, y, z \in X$ aus $x \preceq y$ und $y \preceq z$ jeweils $x \preceq z$ folgt. Eine Relation auf X, die alle drei Eigenschaften besitzt, wird ***Halbordnung*** genannt. Sind je zwei Elemente $x, y \in X$ vergleichbar, gilt also $x \preceq y$ oder $y \preceq x$, dann spricht man von einer ***Totalordnung***. Zusätzlich definieren wir

Definition 17.18 Sei $(X, \preceq)$ eine Menge mit einer Halbordnung. Eine Teilmenge $T \subseteq X$ heißt ***Kette*** in X, wenn sie nichtleer ist und jeweils zwei Elemente $x, y \in T$ miteinander vergleichbar sind. Dies ist äquivalent dazu, dass die Einschränkung der Relation $\preceq$ auf T eine Totalordnung ist.

Ein Element $s \in X$ heißt ***obere Schranke*** einer Teilmenge $T \subseteq X$, wenn $s \succeq t$ für alle $t \in T$ gilt. Ein Element $x \in X$ wird ***maximal*** genannt, wenn kein $y \in X$ mit $y \succeq x$ und $y \neq x$ existiert.

Satz 17.19 *(Zornsches Lemma)*
Sei X eine nichtleere Menge und $\preceq$ eine Halbordnung auf X mit der Eigenschaft, dass jede Kette in X eine obere Schranke in X besitzt. Dann existiert in X ein maximales Element.

Offenbar genügt es, die Bedingung für nichtleere Ketten zu überprüfen, denn jedes Element in X ist eine obere Schranke der leeren Menge.

Man kann zeigen, dass das Zornsche Lemma äquivalent zum sogenannten ***Auswahlaxiom*** ist, welches besagt, dass für jede Menge $\mathcal{X}$, deren Elemente selbst Mengen sind, eine Menge C existiert, die aus jedem $X \in \mathcal{X}$ genau ein Element enthält, und keine weiteren Elemente. Wir können also eine Menge bilden, indem wir aus jeder Menge $X \in \mathcal{X}$ genau ein Element auswählen. (Die Gültigkeit dieser Aussage wirkt so offensichtlich, dass man sie häufig unbewusst anwendet. Wir hatten sie in § 4 im Zusammenhang mit den Repräsentantensystemen bereits kurz erwähnt.) Dabei bedeutet die Äquivalenz von Auswahlaxiom und Zornschem Lemma folgendes: Setzt man die sog. ZF-Axiome der Mengenlehre voraus, dann kann das Zornsche Lemma aus dem Auswahlaxiom abgeleitet werden und umgekehrt das Auswahlaxiom aus dem Zornschen Lemma. Einen Beweis findet man zum Beispiel im Anhang A von [Hi].

Leider können wir aus Platz- und Zeitgründen auf die Zusammensetzung der ZF-Axiome, benannt nach den Mengentheoretikern *E. Zermelo (1871-1953)* und *A. Fraenkel (1891-1965)*, hier nicht genauer eingehen. Sie stellen unter anderem sicher, dass eine leere Menge, Vereinigungen von Mengen, Potenzmengen und unendliche Mengen existieren, und dass man mit Hilfe prädikatenlogischer Aussagenschemata Teilmengen von Mengen definieren darf. Die ZF-Axiome werden mit dem Auswahlaxiom zum ZFC-Axiomensystem zusammengefasst. Die gesamte heutige Mathematik kann auf den ZFC-Axiomen aufgebaut werden.

Erwähnt werden sollte noch, dass das Zornsche Lemma an vielen Stellen die früher gebräuchliche ***transfinite Induktion*** als Beweisprinzip abgelöst hat. Dabei handelt es sich um eine Verallgemeinerung der vollständigen Induktion, die nicht auf den natürlichen Zahlen, sondern auf den sog. ***Ordinalzahlen*** basiert. Während die vollständige Induktion nur zum Beweis einer abzählbar unendlichen Menge von Aussagen geeignet ist, lassen sich mit der transfiniten Induktion beliebig große Mengen von Aussagen beweisen. Aus diesem Grund kann auch die Anwendung des Zornschen Lemmas als „verallgemeinerte vollständige Induktion“ betrachten.

Wir beginnen mit einer einfachen mengentheoretischen Anwendung des Zornschen Lemmas. Aus dem ersten Semester ist folgendes bekannt: Eine Abbildung $f : X \to Y$ zwischen zwei Mengen X und Y ist genau dann injektiv, wenn eine Abbildung $g : Y \to X$ mit $g \circ f = \mathrm{id}_X$ existiert, und genau dann surjektiv, wenn eine Abbildung $h : Y \to X$ mit $f \circ h = \mathrm{id}_Y$ existiert. Dabei ist die Abbildung g dann offenbar surjektiv, und h ist injektiv. Existiert also zwischen zwei Mengen X und Y eine injektive Abbildung $X \to Y$, dann gibt es auch eine surjektive Abbildung $Y \to X$. Gibt es umgekehrt eine surjektive Abbildung $X \to Y$, dann auch eine injektive Abbildung $Y \to X$. Mit dem Zornschen Lemma kann nun darüber hinaus gezeigt werden

Satz 17.20 Sind X, Y beliebige Mengen, dann gibt es eine injektive Abbildung $X \to Y$ oder eine injektive Abbildung $Y \to X$.

Beweis: Wir orientieren uns an der Darstellung in [Ph] und betrachten die Menge $\mathcal{M}$ aller Paare (A, f) bestehend aus einer Teilmenge $A \subseteq X$ und einer injektiven Abbildung $f : A \to Y$. Diese Menge ist nichtleer, denn das Paar bestehend aus $\emptyset \subseteq X$ und der „leeren“ Abbildung $\emptyset \to Y$ ist offenbar in $\mathcal{M}$ enthalten. Auf $\mathcal{M}$ definieren wir eine Relation $\preceq$ mit der Eigenschaft, dass $(A_1, f_1) \preceq (A_2, f_2)$ genau dann gilt, wenn $A_1 \subseteq A_2$ und $f_2|_{A_1} = f_1$ erfüllt ist, für beliebige $(A_1, f_1), (A_2, f_2) \in \mathcal{M}$. Zunächst weisen wir nach, dass $\preceq$ eine Halbordnung auf $\mathcal{M}$ ist. Die Reflexivität ist offensichtlich, denn für jedes Paar $(A, f) \in \mathcal{M}$ gilt $A \subseteq A$ und $f|_A = f$. Zum Nachweis der Antisymmetrie seien (A_1, f_1) und (A_2, f_2) mit $(A_1, f_1) \preceq (A_2, f_2)$ und $(A_2, f_2) \preceq (A_1, f_1)$ vorgegeben. Dann gilt $A_1 \subseteq A_2$ und $A_2 \subseteq A_1$, also $A_1 = A_2$. Aus $A_1 = A_2$ folgt $f_2|_{A_1} = f_2|_{A_2} = f_2$, und mit $f_2|_{A_1} = f_1$ erhalten wir $f_2 = f_1$. Insgesamt gilt also $(A_1, f_1) = (A_2, f_2)$. Für die Transitivität seien $(A_1, f_1), (A_2, f_2), (A_3, f_3) \in \mathcal{M}$ mit $(A_1, f_1) \preceq (A_2, f_2)$ und $(A_2, f_2) \preceq (A_3, f_3)$ vorgegeben. Dann

gilt $A_1 \subseteq A_2$ und $A_2 \subseteq A_3$, also $A_1 \subseteq A_3$. Aus $f_3|_{A_2} = f_2$ und $f_2|_{A_1} = f_1$ folgt $f_3|_{A_1} = (f_3|_{A_2})|_{A_1} = f_2|_{A_1} = f_1$. Insgesamt ist damit $(A_1, f_1) \preceq (A_3, f_3)$ nachgewiesen.

Nun überprüfen wir, dass die halbgeordnete Menge $(\mathcal{M}, \preceq)$ die Voraussetzungen des Zornschen Lemmas erfüllt. Dass $\mathcal{M}$ nichtleer ist, haben wir bereits festgestellt. Sei nun $\mathcal{T}$ eine nichtleere Kette in $\mathcal{M}$. Zu zeigen ist, dass $\mathcal{T}$ in $\mathcal{M}$ eine obere Schranke besitzt. Dafür sei $A_\mathcal{T} \subseteq X$ die Vereinigung aller Mengen A, für die eine Abbildung $f : A \to Y$ mit $(A, f) \in \mathcal{T}$ existiert. Wir definieren eine Abbildung $f : A_\mathcal{T} \to Y$, indem wir für jedes $a \in A_\mathcal{T}$ ein Paar $(A, f_a) \in \mathcal{T}$ mit $a \in A$ wählen und $f_\mathcal{T}(a) = f_a(a)$ setzen. Das Bild $f_\mathcal{T}(a)$ ist von der Wahl des Paares (A, f_a) unabhängig. Ist nämlich $(A', f') \in \mathcal{T}$ ein weiteres Element mit $a \in A'$, dann gilt $(A, f_a) \preceq (A', f')$ oder $(A', f') \preceq (A, f_a)$, weil $\mathcal{T}$ eine Kette ist. Im ersten Fall gilt $f_a(a) = (f'|_A)(a) = f'(a)$, im zweiten $f'(a) = (f_a|_{A'})(a) = f_a(a)$, in beiden Fällen also $f_a(a) = f'(a)$.

Wir behaupten nun, dass $(A_\mathcal{T}, f_\mathcal{T})$ in $\mathcal{M}$ liegt und eine obere Schranke von $\mathcal{T}$ ist. Für Ersteres müssen wir noch zeigen, dass $f_\mathcal{T}$ injektiv ist. Seien also $a_1, a_2 \in A_\mathcal{T}$ mit $f_\mathcal{T}(a_1) = f_\mathcal{T}(a_2)$ vorgegeben. Auf Grund der Definition von $A_\mathcal{T}$ gibt es Paare $(A_1, f_1), (A_2, f_2) \in \mathcal{T}$ mit $a_1 \in A_1$, $a_2 \in A_2$, und unsere Feststellung aus dem vorherigen Absatz zeigt, dass $f_1(a_1) = f_\mathcal{T}(a_1) = f_\mathcal{T}(a_2) = f_2(a_2)$ gilt. Weil $\mathcal{T}$ eine Kette ist, dürfen wir o.B.d.A. annehmen, dass $(A_1, f_1) \preceq (A_2, f_2)$ gilt. Daraus folgt $A_1 \subseteq A_2$, also $a_1, a_2 \in A_2$, außerdem $f_2|_{A_1} = f_1$ und somit $f_2(a_2) = f_1(a_1) = (f_2|_{A_1})(a_1) = f_2(a_1)$. Die Injektivität von f_2 liefert nun $a_1 = a_2$, wie gewünscht. Damit ist $(A_\mathcal{T}, f_\mathcal{T})$ nachgewiesen. Ist nun $(A, f) \in \mathcal{T}$ beliebig vorgegeben, dann gilt $A_\mathcal{T} \supseteq A$ nach Definition von $A_\mathcal{T}$, und für jedes $a \in A$ ist $f_\mathcal{T}(a) = f(a)$, also $f_\mathcal{T}|_A = f$. Also gilt $(A, f) \preceq (A_\mathcal{T}, f_\mathcal{T})$, und somit ist $(A_\mathcal{T}, f_\mathcal{T})$ in der Tat eine obere Schranke von $\mathcal{T}$.

Nach dem Zornschen Lemma 17.19 existiert in $\mathcal{M}$ nun ein maximales Element $(\tilde{A}, \tilde{f})$. Ist $\tilde{A} = X$, dann ist f eine injektive Abbildung $X \to Y$, und wir sind fertig. Gilt $\tilde{f}(\tilde{A}) = Y$, dann ist $\tilde{f} : \tilde{A} \to Y$ surjektiv, und wir können $\tilde{f}$ zu einer surjektiven Abbildung $X \to Y$ fortsetzen. Wie wir vor dem Beweis angemerkt haben, existiert dann eine injektive Abbildung $Y \to X$. Nehmen wir nun an, dass sowohl $\tilde{A} \subsetneq X$ als auch $\tilde{f}(\tilde{A}) \subsetneq Y$ gilt. Sei $a \in X \setminus \tilde{A}$ und $b \in Y \setminus \tilde{f}(\tilde{A})$. Wir können dann auf $A_1 = \tilde{A} \cup \{a\}$ eine injektive Abbildung $f_1 : A_1 \to Y$ definieren, indem wir $f_1(a) = b$ und $f_1|_{A_1} = \tilde{f}$ festlegen. Aber dann ist (A_1, f_1) in $\mathcal{M}$ ein echt größeres Element als $(\tilde{A}, \tilde{f})$, im Widerspruch zur Maximalität. Also ist der Fall $\tilde{A} \subsetneq X$ und $\tilde{f}(\tilde{A}) \subsetneq Y$ ausgeschlossen. □

Wenden wir uns nun wieder der Körpertheorie zu. Als erstes beweisen wir Proposition 17.10 für beliebige algebraische Erweiterungen. Sei $L|K$ eine solche Erweiterung, $\tilde{K}$ ein algebraisch abgeschlossener Körper und $\phi : K \to \tilde{K}$ ein Homomorphismus von Körpern. Zu zeigen ist, dass ein Homomorphismus $\psi : L \to \tilde{K}$ mit $\psi|_K = \phi$ existiert.

Es sei $\mathcal{F}$ die Menge aller Paare (M, ψ_M) bestehend aus einem Zwischenkörper M von $L|K$ und einer Fortsetzung $\psi_M : M \to \tilde{K}$ von ϕ auf M. Wir definieren eine Relation $\preceq$ auf $\mathcal{F}$, indem wir fordern, dass die Äquivalenz

$$(M_1, \psi_{M_1}) \preceq (M_2, \psi_{M_2}) \quad \Leftrightarrow \quad M_1 \subseteq M_2 \text{ und } \psi_{M_2}|_{M_1} = \psi_{M_1}$$

für alle Paare $(M_1, \psi_{M_1}), (M_2, \psi_{M_2}) \in \mathcal{F}$ gilt. Wegen $(K, \phi) \in \mathcal{F}$ ist die Menge $\mathcal{F}$ nicht leer. Ähnlich wie im Beweis von Satz 17.20 überprüft man, dass durch $\preceq$ eine Halbordnung auf $\mathcal{F}$ definiert ist; der einzige Unterschied besteht darin, dass an Stelle von Abbildungen nun Körperhomomorphismen betrachtet werden.

Nun zeigen wir, dass die halbgeordnete Menge $(\mathcal{F}, \preceq)$ die Voraussetzungen des Zornschen Lemmas erfüllt. Sei $\mathcal{T} \subseteq \mathcal{F}$ eine nichtleere Kette in $\mathcal{F}$. Weiter sei $M_\mathcal{T}$ die Vereinigung aller Zwischenkörper M von $L|K$, für die ein Körperhomomorphismen $\psi_M : M \to \tilde{K}$ mit $(M, \psi_M) \in \mathcal{T}$ existiert. Dann ist auch $M_\mathcal{T}$ ein Zwischenkörper von $L|K$. Zunächst ist das Einselement $1_K = 1_L$ in $M_\mathcal{T}$ enthalten, denn weil M für jedes Element (M, ψ_M) aus $\mathcal{T}$ ein Teilkörper von L ist, gilt jeweils $1_K \in M$. Seien nun $\alpha, \beta \in M_\mathcal{T}$ vorgegeben. Dann gibt es Elemente $(M_\alpha, \psi_{M_\alpha}), (M_\beta, \psi_{M_\beta}) \in \mathcal{T}$ mit $\alpha \in M_\alpha$ und $\beta \in M_\beta$. Weil $\mathcal{T}$ eine Kette ist, können wir o.B.d.A. $(M_\alpha, \psi_{M_\alpha}) \preceq (M_\beta, \psi_{M_\beta})$ annehmen. Dann sind α, β beide in

M_β enthalten. Weil M_β ein Teilkörper von L ist, liegen auch die Elemente $\alpha-\beta$ und $\alpha\beta$ in M_β, im Fall $\alpha \neq 0_K$ auch das Element α^{-1}. Erst recht enthält $M_\mathcal{T}$ all diese Elemente. Damit ist die Teilkörpereigenschaft nachgewiesen.

Außerdem definieren wir eine Abbildung $\psi_\mathcal{T} : M_\mathcal{T} \to \tilde{K}$, indem wir für jedes $\alpha \in M_\mathcal{T}$ ein Element $(M_\alpha, \psi_{M_\alpha})$ mit $\alpha \in M_\alpha$ auswählen und $\psi_\mathcal{T}(\alpha) = \psi_{M_\alpha}(\alpha)$ setzen. Ist $\alpha \in K$, dann gilt $\psi_\mathcal{T}(\alpha) = \psi_{M_\alpha}(\alpha) = \phi(\alpha)$, weil ψ_{M_α} eine Fortsetzung von ϕ ist. Außerdem ist $\psi_\mathcal{T}$ ein Körperhomomorphismus. Dazu bemerken wir zunächst: Ist $\alpha \in M_\mathcal{T}$ und $(M, \psi_M) \in \mathcal{T}$ ein beliebiges Element mit $\alpha \in M$, dann gilt $\psi_\mathcal{T}(\alpha) = \psi_M(\alpha)$. Denn weil $\mathcal{T}$ eine Kette ist, gilt $(M, \psi_M) \preceq (M_\alpha, \psi_{M_\alpha})$ oder $(M_\alpha, \psi_{M_\alpha}) \preceq (M, \psi_M)$. Im ersten Fall gilt $\psi_M(\alpha) = (\psi_{M_\alpha}|_M)(\alpha) = \psi_{M_\alpha}(\alpha) = \psi_\mathcal{T}(\alpha)$, und durch eine ähnliche Rechnung erhält man dasselbe Resultat auch im zweiten Fall. Seien nun $\alpha, \beta \in M_\mathcal{T}$ vorgegeben, und es seien $(M_\alpha, \psi_{M_\alpha}), (M_\beta, \psi_{M_\beta})$ Elemente aus $\mathcal{T}$ wie im vorherigen Absatz. Dann liegen die Elemente $\alpha, \beta, \alpha+\beta$ und $\alpha\beta$ alle in M_β. Weil ψ_{M_β} ein Körperhomomorphismus ist, gilt

$$\psi_\mathcal{T}(\alpha+\beta) \quad = \quad \psi_{M_\beta}(\alpha+\beta) \quad = \quad \psi_{M_\beta}(\alpha)+\psi_{M_\beta}(\beta) \quad = \quad \psi_\mathcal{T}(\alpha)+\psi_\mathcal{T}(\beta)$$

und ebenso $\psi_\mathcal{T}(\alpha\beta) = \psi_\mathcal{T}(\alpha)\psi_\mathcal{T}(\beta)$. Ebenso gilt $\psi_\mathcal{T}(1_K) = \psi_{M_\beta}(1_K) = \phi(1_K) = 1_{\tilde{K}}$, weil ψ_{M_β} eine Fortsetzung von ϕ ist. Nach Konstruktion gilt $M \subseteq M_\mathcal{T}$ und $\psi_\mathcal{T}|_M = \psi_M$ für jedes $(M, \psi_M) \in \mathcal{T}$. Also ist $(M_\mathcal{T}, \psi_\mathcal{T})$ tatsächlich eine obere Schranke von $\mathcal{T}$.

Auf Grund des Zornschen Lemmas, Satz 17.19, existiert nun in $\mathcal{F}$ ein maximales Element $(\tilde{M}, \psi_{\tilde{M}})$. Gilt $\tilde{M} = L$, dann ist $\psi_{\tilde{M}}$ eine Fortsetzung von ϕ auf L, wie gewünscht. Im Fall $\tilde{M} \subsetneq L$ sei $\alpha \in L \setminus \tilde{M}$ beliebig gewählt. Weil α über K und erst recht über $\tilde{M}$ algebraisch ist, handelt es sich bei $\tilde{M}(\alpha)|\tilde{M}$ nach Proposition 15.14 um eine endliche Erweiterung. Da Satz 16.2 für endliche Erweiterungen bewiesen wurde, existiert eine Fortsetzung $\psi_{M_1} : M_1 \to \tilde{K}$ von $\psi_{\tilde{M}}$ auf $M_1 = \tilde{M}(\alpha)$. Es ist dann (M_1, ψ_{M_1}) in $\mathcal{F}$ ein echt größeres Element als $(\tilde{M}, \psi_{\tilde{M}})$. Aber dies widerspricht der Maximalität von $(\tilde{M}, \psi_{\tilde{M}})$. Also muss $\tilde{M} = L$ gelten. □

Um den Beweis von Satz 17.4 über die Existenz von Zerfällungskörpern für beliebige Mengen nicht-konstanter Polynome vorzubereiten, zeigen wir

Lemma 17.21 Sei X eine Menge und $\mathcal{P}(X)$ ihre Potenzmenge. Dann existiert keine surjektive Abbildung $\phi : X \to \mathcal{P}(X)$.

Beweis: Die Argumentation ähnelt dem Cantorschen Diagonalverfahren, mit dem gezeigt wird, dass die reellen Zahlen surjektiv sind. Nehmen wir an, $\phi : X \to \mathcal{P}(X)$ ist eine surjektive Abbildung, und betrachten wir die Menge $D = \{x \in X \mid x \notin \phi(x)\}$. Weil D surjektiv ist, existiert ein $x_D \in X$ mit $\phi(x_D) = D$, und dieses Element muss $x_D \in D$ oder $x_D \notin D$ erfüllen. Betrachten wir den Fall $x_D \in D$. Dann ist die Bedingung $x \notin \phi(x_D)$ nicht erfüllt, und es folgt $x_D \notin D$, ein Widerspruch. Setzen wir nun $x_D \notin D$ voraus. Dann ist die Bedinung $x_D \notin \phi(x_D)$ erfüllt, und nach Definition von D gilt $x_D \in D$. Also ergibt sich auch im zweiten Fall ein Widerspruch. Dies zeigt, dass unsere Annahme, die Abbildung ϕ wäre surjektiv, falsch war. □

Lemma 17.22 Sei K ein Körper.

(i) Es gibt eine Menge Ω_0 mit der Eigenschaft, dass für jede algebraische Erweiterung $L|K$ eine injektive Abbildung $L \to \Omega_0$ existiert. (Dies bedeutet, dass die Menge Ω_0 groß genug ist, um sämtliche algebraischen Erweiterungen von K in sich „aufzunehmen“.)

(ii) Es existiert eine Menge Ω mit der Eigenschaft, dass für keine algebraische Erweiterung $L|K$ eine surjektive Abbildung $L \to \Omega$ existiert.

Beweis: zu (i) Sei $\Omega_0 = K[x] \times \mathbb{N}$ und $L|K$ eine algebraische Erweiterung. Dann erhalten wir folgendermaßen eine injektive Abbildung $\phi : L \to \Omega_0$: Für jedes nicht-konstante, normierte, irreduzible Polynom $f \in K[x]$ wählen wir eine Nummerierung $\alpha_1, ..., \alpha_n$ der Nullstellen von f in L und definieren dann $\phi(\alpha_j) = (f, j)$. Die Abbildung ist wohldefiniert, da f jeweils das (eindeutig bestimmte) Minimalpolynom von α_j über K ist, und außerdem injektiv, da je zwei verschiedene Elemente aus L entweder verschiedene Minimalpolynome haben, oder den Elementen unterschiedlichen Nummern zugeordnet wurden.

zu (ii) Sei $\Omega = \mathcal{P}(\Omega_0)$, die Potenzmenge von Ω_0. Nehmen wir an, es gäbe eine algebraische Erweiterung $L|K$ und eine surjektive Abbildung $L \to \Omega$. Weiter sei $\phi : L \to \Omega_0$ die injektive Abbildung aus Teil (i). Dann können wir mit Hilfe der Umkehrabbildung der Bijektion $\phi : \phi \to \phi(L)$ eine surjektive Abbildung $\phi(L) \to \Omega$ definieren, und jede Fortsetzung dieser Abbildung auf Ω_0 wäre ebenfalls surjektiv. Aber nach Lemma 17.21 existiert keine surjektive Abbildung von Ω_0 auf Ω. □

Nun kann der Beweis von Satz 17.4 durchgeführt werden. Sei K ein Körper und $S \subseteq K[x]$ eine Menge nicht-konstanter Polynome. Zu zeigen ist, dass ein Zerfällungskörper von S über K existiert. Sei dazu Ω eine Menge wie in Lemma 17.22 (ii). Nach Ersetzung von Ω durch $\Omega \cup K$ dürfen wir $\Omega \supseteq K$ annehmen. Es sei nun $\mathcal{F}$ die Menge aller Erweiterungskörper $(L, +_L, \cdot_L)$ von K mit $L \subseteq \Omega$ und der Eigenschaft, dass L Zerfällungskörper einer Teilmenge $T \subseteq S$ ist. Diese Menge ist nichtleer, denn der Körper K mit seiner Addition und Multiplikation ist Zerfällungskörper der Teilmenge $\varnothing \subseteq S$. Wir definieren eine Relation $\preceq$ auf $\mathcal{F}$, indem wir fordern, dass genau dann $(L_1, +_{L_1}, \cdot_{L_1}) \preceq (L_2, +_{L_2}, \cdot_{L_2})$ erfüllt ist, wenn L_1 ein Teilkörper von L_2 ist. Dies bedeutet unter anderem, dass $L_1 \subseteq L_2$ gilt, dass L_1 abgeschlossen unter $+_{L_2}$ und $\cdot_{L_2}$ ist, und dass die Einschränkung von $+_{L_2}$ bzw. $\cdot_{L_2}$ auf L_1 mit $+_{L_1}$ bzw. $\cdot_{L_1}$ übereinstimmt. Um die Notation nicht zu aufwändig werden zu lassen, schreiben wir ab jetzt an Stelle von $(L, +_L, \cdot_L)$ meist einfach L. Es ist aber darauf zu achten, dass für $L_1, L_2 \in \mathcal{F}$ die additiven und multiplikativen Verknüpfungen im Allgemeinen nur auf K übereinzustimmen brauchen, selbst wenn L_1 und L_2 als Teilmengen von Ω gleich sind.

Um das Zornsche Lemma anwenden zu können, überprüfen wir zunächst wieder, dass durch $\preceq$ eine Halbordnung auf $\mathcal{F}$ gegeben ist. Die Relation ist reflexiv, denn jedes $L \in \mathcal{F}$ ist ein Teilkörper von sich selbst. Sind $L_1, L_2 \in \mathcal{F}$ mit $L_1 \preceq L_2$ und $L_2 \preceq L_1$, dann gilt insbesondere $L_1 \subseteq L_2$ und $L_2 \subseteq L_1$, also $L_1 = L_2$. Außerdem müssen (auf Grund der Teilkörper-Eigenschaft) Addition und Multiplikation auf L_1 und L_2 übereinstimmen. Also stimmen L_1 und L_2 als Körper überein, und folglich ist die Relation anti-symmetrisch. Sind $L_1, L_2, L_3 \in \mathcal{F}$ mit $L_1 \preceq L_2$ und $L_2 \preceq L_3$ vorgegeben, dann ist L_1 Teilkörper von L_2 und L_2 Teilkörper von L_3. Aus $L_1 \subseteq L_2$ und $L_2 \subseteq L_3$ folgt $L_1 \subseteq L_3$. Schränkt man die Addition von L_3 auf L_2 ein, so erhält man die Addition des Körpers L_2. Schränkt man diese weiter auf L_1 ein, so erhält man die Addition auf L_1. Also erhält man die Addition von L_1 auch, indem man die Addition von L_3 direkt auf L_1 einschränkt. Dasselbe gilt für die Multiplikation. Insgesamt ist damit gezeigt, dass L_1 ein Teilkörper von L_3 ist und somit $L_1 \preceq L_3$ gilt. Die Relation $\preceq$ ist also auch transitiv, insgesamt eine Halbordnung.

Für die Anwendbarkeit des Zornschen Lemmas muss noch gezeigt werden, dass jede nichtleere Kette $\mathcal{T}$ in $\mathcal{F}$ eine obere Schranke besitzt. Auf der Teilmenge $L_\mathcal{T} = \bigcup_{L \in \mathcal{T}} L$ von Ω definieren wir auf folgende Weise Verknüpfungen $+_\mathcal{T}$ und $\cdot_\mathcal{T}$: Sind $\alpha, \beta \in L_\mathcal{T}$ vorgegeben, dann gibt es einen Körper $L_1 \in \mathcal{T}$ mit $\alpha \in L_1$ und ein $L_2 \in \mathcal{T}$ mit $\beta \in L_2$. Weil $\mathcal{T}$ eine Kette ist, dürfen wir o.B.d.A. $L_1 \preceq L_2$ annehmen. Es gilt dann $L_1 \subseteq L_2$ und somit $\alpha, \beta \in L_2$. Für jedes Paar (α, β) von Elementen in $L_\mathcal{T}$ können wir also einen Körper $L_{(\alpha,\beta)} \in \mathcal{T}$ mit $\alpha, \beta \in L_{(\alpha,\beta)}$ wählen. Bezeichnen $+_{(\alpha,\beta)}$ und $\cdot_{(\alpha,\beta)}$ die Addition und Multiplikation auf $L_{(\alpha,\beta)}$, dann definieren wir

$$\alpha +_\mathcal{T} \beta = \alpha +_{(\alpha,\beta)} \beta \quad , \quad \alpha \cdot_\mathcal{T} \beta = \alpha \cdot_{(\alpha,\beta)} \beta .$$

Zu überprüfen ist nun, dass es sich bei $(L_\mathcal{T}, +_\mathcal{T}, \cdot_\mathcal{T})$ um einen Körper und darüber hinaus um einen Zerfällungskörper einer Teilmenge $T \subseteq S$ handelt. Beim Nachweis der Körperaxiome beschränken wir uns auf den Nachweis

des Assoziativgesetzes der Addition, weil der Nachweis der übrigen Körperaxiome weitgehend analog veräuft. Seien $\alpha, \beta, \gamma \in L_{\mathcal{T}}$ vorgegeben, außerdem $\alpha' = \alpha +_{(\alpha,\beta)} \beta$ und $\gamma' = \beta +_{(\beta,\gamma)} \gamma$. Weil $\mathcal{T}$ eine Kette ist, gibt es unter den Körpern $L_{(\alpha,\beta)}$, $L_{(\beta,\gamma)}$, $L_{(\alpha',\gamma)}$ und $L_{(\alpha,\gamma')}$ ein größtes Element, das wir mit L bezeichnen. Weil in L das Assoziativgesetz gilt und die vier aufgezählten Körper alles Teilkörper von L sind, gilt

$$\begin{aligned}(\alpha +_{\mathcal{T}} \beta) +_{\mathcal{T}} \gamma &= (\alpha +_{(\alpha,\beta)} \beta) +_{\mathcal{T}} \gamma = \alpha' +_{\mathcal{T}} \gamma = \alpha' +_{(\alpha',\gamma)} \gamma \\ = \alpha' +_L \gamma &= (\alpha +_L \beta) +_L \gamma = \alpha +_L (\beta +_L \gamma) = \alpha +_L \gamma' = \alpha +_{(\alpha,\gamma')} \gamma' = \\ &\alpha +_{\mathcal{T}} \gamma' = \alpha +_{\mathcal{T}} (\beta +_{\beta,\gamma} \gamma) = \alpha +_{\mathcal{T}} (\beta +_{\mathcal{T}} \gamma).\end{aligned}$$

Der Nachweis der übrigen Körperaxiome funktioniert nach dem gleichen Schema; dabei stellt man insbesondere fest, dass Null- bzw. Einselement von $L_{\mathcal{T}}$ mit Null- und Einselement des Grundkörpers K übereinstimmen. Darüber hinaus ist jedes $L \in \mathcal{T}$ ein Teilkörper von $L_{\mathcal{T}}$. Ist nämlich $+$ die Addition auf L und sind $\alpha, \beta \in L$ vorgegeben, dann gilt $L \preceq L_{(\alpha,\beta)}$ oder $L_{(\alpha,\beta)} \preceq L$. Dies zeigt, dass $\alpha +_{\mathcal{T}} \beta = \alpha +_{(\alpha,\beta)} \beta$ und $\alpha + \beta$ übereinstimmen. Ebenso stimmt die Multiplikation von $L_{\mathcal{T}}$ mit der Multiplikation von L überein. Weil K ein Teilkörper von L ist, gilt $1_L = 1_K = 1_{L_{\mathcal{T}}}$. Weil L ein Körper ist und die Verknüpfungen von L und $L_{\mathcal{T}}$ übereinstimmen, ist L abgeschlossen unter der Subtraktion und der Multiplikation in $L_{\mathcal{T}}$, für Elemente ungleich 0_K auch unter Inversenbildung.

Zeigen wir nun noch, dass $L_{\mathcal{T}}$ Zerfällungskörper einer Teilmenge $T \subseteq S$ ist, dann ist $L_{\mathcal{T}}$ insgesamt eine obere Schranke von $\mathcal{T}$ in $\mathcal{F}$. Nach Definition von $\mathcal{F}$ existiert für jedes $L \in \mathcal{F}$, erst recht für jedes $L \in \mathcal{T}$ eine Teilmenge $T_L \subseteq S$, so dass L Zerfällungskörper von T_L ist. Wir beweisen jetzt, dass $L_{\mathcal{T}}$ Zerfällungskörper von $T = \bigcup_{L \in \mathcal{T}} T_L$ ist. Jedes $f \in T$ ist in einer Teilmenge T_L enthalten. Also zerfällt f über L, und damit auch über dem Erweiterungskörper $L_{\mathcal{T}}$ von L, in Linearfaktoren. Für jedes $L \in \mathcal{T}$ sei $N_L \subseteq L$ jeweils die Menge aller Nullstellen von Polynomen aus T_L. Dann gilt $L = K(N_L)$, und $N = \bigcup_{L \in \mathcal{T}} N_L$ ist die Menge aller Nullstellen von Polynomen aus T. Wir müssen nun $L_{\mathcal{T}} \subseteq K(N)$ nachweisen. Tatsächlich liegt jedes $\alpha \in L_{\mathcal{T}}$ in L für ein $L \in \mathcal{T}$, und somit in $K(N_L) \subseteq K(N)$.

Ingesamt haben wir damit die Voraussetzungen des Zornschen Lemmas verifiziert, und demnach existiert in $\mathcal{F}$ ein maximales Element $\tilde{L}$. Nehmen wir an, dass $\tilde{L}$ lediglich Zerfällungskörper einer echten Teilmenge T von S ist. Dann gibt es ein $f \in S$, das über $\tilde{L}$ nicht in Linearfaktoren zerfällt. Nach Satz 17.2 existiert ein Zerfällungskörper L_1 von f über $\tilde{L}$. Wenn es eine injektive Abbildung ϕ_1 von $L_1 \setminus \tilde{L}$ nach $\Omega \setminus \tilde{L}$ gibt, so können wir eine injektive Abbildung $\hat{\phi}_1 : L_1 \to \Omega$ definieren, indem wir $\hat{\phi}_1(\alpha) = \alpha$ für $\alpha \in \tilde{L}$ und $\hat{\phi}_1(\alpha) = \phi_1(\alpha)$ für $\alpha \in L_1 \setminus \tilde{L}$ setzen. Mit Hilfe von Satz 11.15 aus der Ringtheorie und der Bijektion $\hat{\phi}_1$ zwischen L_1 und der Bildmenge $\hat{\phi}_1(\tilde{L})$ können wir auf $\hat{\phi}_1(\tilde{L}) \subseteq \Omega$ die Struktur eines zu L_1 isomorphen Körpers definieren. Wegen $\hat{\phi}_1|_{\tilde{L}} = \mathrm{id}_{\tilde{L}}$ handelt es sich dabei um einen Erweiterungskörper von $\tilde{L}$, und mit L_1 ist auch $\hat{\phi}_1(\tilde{L})$ Zerfällungskörper einer echten Obermenge von T. Insgesamt ist $\hat{\phi}_1(\tilde{L})$ damit in $\mathcal{F}$ ein echt größeres Element als $\tilde{L}$, im Widerspruch zur Maximalität.

Betrachten wir nun noch den Fall, dass keine injektive Abbildung von $L_1 \setminus \tilde{L}$ nach $\Omega \setminus \tilde{L}$ existiert. Dann gäbe es nach Satz 17.20 eine injektive Abbildung $\Omega \setminus \tilde{L} \to L_1 \setminus \tilde{L}$ und somit auch eine surjektive Abbildung $L_1 \setminus \tilde{L} \to \Omega \setminus \tilde{L}$. Diese könnte zu einer surjektiven Abbildung $\rho : L_1 \to \Omega$ mit $\rho(\alpha) = \alpha$ für alle $\alpha \in \tilde{L}$ fortgesetzt werden. Aber dies steht im Widerspruch zur Eigenschaft der Menge Ω, keine surjektive Abbildung $L_1 \to \Omega$ von einer algebraischen Erweiterung $L_1|K$ zuzulassen. □

§ 18. *Endliche Körper*

Zusammenfassung. Aus der Zahlentheorie-Vorlesung ist bereits bekannt, dass für jede Primzahl p durch $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen gegeben ist. In diesem Abschnitt wird das Konzept der Zerfällungskörper aus § 17 verwendet, um die endlichen Körper insgesamt zu klassifizieren. Außerdem diskutieren wir die Teilkörperstruktur und die Automorphismen endlicher Körper.

Wichtige Grundbegriffe	*Zentrale Sätze*
– formale Ableitung eines Polynoms	– Klassifikation der Primkörper
– Frobenius-Endomorphismus eines Rings der Charakteristik p	– Die Elementezahl eines endlichen Körpers ist stets eine Primzahlpotenz $p^n > 1$.
	– Existenz und Eindeutigkeit des Körpers mit p^n Elementen bis auf Isomorphie
	– Eindeutigkeit des Körpers $\mathbb{F}_{p^n}$ Elementen als Teilkörper des algebraischen Abschlusses $\mathbb{F}_p^{\text{alg}}$ von $\mathbb{F}_p$
	– Rechenregel $(a+b)^p = a^p + b^p$ in Charakteristik p („Freshman's Dream“)

In diesem Kapitel spielt der in § 9 eingeführte Begriff des Primkörpers eine besondere Rolle. Wir beginnen damit, dass wir alle Körper, die überhaupt die Rolle eines Primkörpers einnehmen können, bis auf Isomorphie beschreiben.

Satz 18.1 Sei K ein Körper und P sein Primkörper.

(i) Ist $\text{char}(K) = 0$, dann gilt $P \cong \mathbb{Q}$.

(ii) Ist $\text{char}(K) = p$ für eine Primzahl p, dann gilt $P \cong \mathbb{F}_p$.

Beweis: Nach Folgerung 9.3 existiert ein eindeutig bestimmter Ringhomomorphismus $\phi : \mathbb{Z} \to K$, gegeben durch die Zuordnungsvorschrift $n \mapsto n \cdot 1_K$. Mit Hilfe dieses Homomorphismus werden wir nun in beiden Fällen den jeweils angegebenen Isomorphismus konstruieren.

zu (i) Im Fall $\text{char}(K) = 0$ ist ϕ injektiv. Wäre nämlich $n \in \mathbb{Z}$, $n \neq 0$ mit $\phi(n) = 0_K$, dann wäre auch $\phi(-n) = -\phi(n) = -0_K = 0_K$. Damit gäbe es auf jeden Fall ein $m \in \mathbb{N}$ mit $m \cdot 1_K = \phi(m) = 0_K$, was aber der Voraussetzung $\text{char}(K) = 0$ widerspricht.

Die Abbildung $\phi : \mathbb{Z} \to K$ kann zu einer Abbildung $\hat{\phi} : \mathbb{Q} \to K$ fortgesetzt werden. Sei dazu $r \in \mathbb{Q}$ und $r = \frac{a}{b}$ eine Darstellung von r als gekürzter Bruch, mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und $\text{ggT}(a,b) = 1$. Auf Grund der Injektivität von ϕ ist $\phi(b) \neq 0$, so dass wir $\hat{\phi}(r) = \phi(a)\phi(b)^{-1}$ definieren können. Wegen $\hat{\phi}(\frac{a}{1}) = \phi(a)\phi(1)^{-1} = \phi(a) \cdot 1_K^{-1} = \phi(a)$ für alle $a \in \mathbb{Z}$ gilt $\hat{\phi}|_{\mathbb{Z}} = \phi$, also ist $\hat{\phi}$ tatsächlich eine Fortsetzung von ϕ auf $\mathbb{Q}$.

Ist $r \in \mathbb{Q}$ und $r = \frac{a}{b}$ eine beliebige Darstellung von r als Bruch (mit $a \in \mathbb{Z}$ und $b \in \mathbb{N}$). Dann gilt $\hat{\phi}(r) = \phi(a)\phi(b)^{-1}$. Ist nämlich $r = \frac{a_1}{b_1}$ die Darstellung von r als gekürzter Bruch wie oben, dann folgt aus $\frac{a}{b} = \frac{a_1}{b_1}$ die Gleichung $ab_1 = a_1 b$ und somit $\phi(a)\phi(b_1) = \phi(a_1)\phi(b)$, woraus sich wiederum

$$\phi(a)\phi(b)^{-1} \quad = \quad \phi(a_1)\phi(b_1)^{-1} \quad = \quad \hat{\phi}(\tfrac{a_1}{b_1}) \quad = \quad \hat{\phi}(r)$$

ergibt. Man überprüft nun leicht, dass durch $\hat{\phi} : \mathbb{Q} \to K$ ein Körperhomomorphismus geben ist: Zunächst gilt nach Definition $\hat{\phi}(1) = \hat{\phi}(\frac{1}{1}) = \phi(1)\phi(1)^{-1} = 1_K \cdot 1_K^{-1} = 1_K$. Seien nun $r, s \in \mathbb{Q}$ vorgegeben, $r = \frac{a}{b}$ und $s = \frac{c}{d}$ mit $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{N}$. Aus den Gleichungen $r + s = \frac{ad+bc}{bd}$ und $rs = \frac{ac}{bd}$ folgt dann

$$\begin{gathered}\hat{\phi}(r+s) \quad = \quad \phi(ad+bc)\phi(bd)^{-1} \quad = \quad \phi(ad)\phi(bd)^{-1} + \phi(bc)\phi(bd)^{-1} \quad = \\ \phi(a)\phi(d)\phi(b)^{-1}\phi(d)^{-1} + \phi(b)\phi(c)\phi(b)^{-1}\phi(d)^{-1} \quad = \quad \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} \\ = \quad \hat{\phi}(\tfrac{a}{b}) + \hat{\phi}(\tfrac{c}{d}) \quad = \quad \hat{\phi}(r) + \hat{\phi}(s)\end{gathered}$$

und

$$\begin{gathered}\hat{\phi}(rs) \quad = \quad \phi(ac)\phi(bd)^{-1} \quad = \quad \phi(a)\phi(c)\phi(b)^{-1}\phi(d)^{-1} \quad = \quad \phi(a)\phi(b)^{-1} \cdot \phi(c)\phi(d)^{-1} \\ = \quad \hat{\phi}(\tfrac{a}{b}) \cdot \hat{\phi}(\tfrac{c}{d}) \quad = \quad \hat{\phi}(r) \cdot \hat{\phi}(s).\end{gathered}$$

Weil Körperhomomorphismen nach Proposition 9.7 stets injektiv sind, definiert $\hat{\phi}$ einen Isomorphismus zwischen $\mathbb{Q}$ und dem Teilkörper $\hat{\phi}(\mathbb{Q})$ von K. Weil P als Primkörper der kleinste Teilkörper von K ist, gilt $\hat{\phi}(\mathbb{Q}) \supseteq P$. Anderseits gilt auch $\hat{\phi}(\mathbb{Q}) \subseteq P$, denn P enthält als Teilring von K mit 1_K auch $\hat{\phi}(n) = n \cdot 1_K$ für alle $n \in \mathbb{Z}$, und als Teilkörper auch $\phi(\frac{a}{b}) = (a \cdot 1_K)(b \cdot 1_K)^{-1}$ für alle $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Insgesamt gilt also $\hat{\phi}(\mathbb{Q}) = P$, und damit ist $\mathbb{Q} \cong P$ nachgewiesen.

zu (ii) Im Fall $\mathrm{char}(K) = p$ gilt $\phi(p) = p \cdot 1_K = 0_K$. Der Kern von ϕ ist damit eine Untergruppe von $(\mathbb{Z}, +)$, die $\langle p \rangle = p\mathbb{Z}$ enthält. Nehmen wir an, es gäbe ein Element $m \in \ker(\phi) \setminus p\mathbb{Z}$. Division mit Rest liefert dann $q, r \in \mathbb{Z}$ mit $m = qp + r$ und $0 \leq r < p$, wobei $r = 0$ wegen $m \notin p\mathbb{Z}$ ausgeschlossen ist. Wegen $r = m - qp$ wäre dann $r \cdot 1_K = m \cdot 1_K - q \cdot (p \cdot 1_K) = m \cdot 1_K = \phi(m) = 0_K$, was wegen $r < p$ aber zur Definition von $\mathrm{char}(K)$ im Widerspruch steht.

Also muss $\ker(\phi) = p\mathbb{Z}$ gelten. Der Homomorphiesatz für Ringe liefert einen Ringisomorphismus $\bar{\phi} : \mathbb{Z}/p\mathbb{Z} \to \phi(\mathbb{Z})$. Wir überprüfen nun, dass $\bar{\phi}(\mathbb{F}_p) = \phi(\mathbb{Z})$ der Primkörper von K ist. Als Bild von $\mathbb{F}_p$ unter dem Isomorphismus $\bar{\phi}$ ist $\bar{\phi}(\mathbb{F}_p)$ jedenfalls ein Teilkörper von K, und folglich gilt $P \subseteq \bar{\phi}(\mathbb{F}_p)$. Andererseits gilt aber auch $P \supseteq \bar{\phi}(\mathbb{F}_p)$, denn als Teilkörper von K enthält P das Element $\bar{\phi}(1 + p\mathbb{Z}) = 1_K$ und damit auch $\bar{\phi}(n + p\mathbb{Z}) = n \cdot 1_K$ für alle $n \in \mathbb{Z}$, also den gesamten Teilkörper $\bar{\phi}(\mathbb{F}_p)$. □

Nach dieser Vorbereitung kann nun bereits eine wichtige Aussage über die mögliche Elementezahl eines endlichen Körpers getroffen werden. Im Gegensatz zu endlichen Gruppen und Ringen, bei denen jede Elementezahl möglich ist, gilt für die Körper

Satz 18.2 Ist K ein endlicher Körper, dann ist $|K|$ eine Primzahlpotenz. Es gilt also $|K| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$.

Beweis: Sei P der Primkörper von K. Nach Satz 18.1 gilt $P \cong \mathbb{Q}$ oder $P \cong \mathbb{F}_p$ für eine Primzahl p. Dabei scheidet die erste Möglichkeit aus, weil $|K|$ und damit $|P|$ endlich ist. Sei also p die Primzahl mit $P \cong \mathbb{F}_p$. Wegen $|K| < \infty$ muss auch der Grad $n = [K : P]$ endlich sein. Als P-Vektorraum ist K damit isomorph zu P^n, und es folgt $|K| = |P|^n = p^n$. □

Als nächstes werden wir zeigen, dass jeder Körper mit p^n Elementen zwangsläufig ein Zerfällungskörper über seinem Primkörper ist. Weil nach § 16 jeder Zerfällungskörper eines Polynoms $f \in K[x]$ bis auf K-Isomorphie eindeutig bestimmt ist, stellt dies einen wichtigen Schritt hin zum Nachweis der Eindeutigkeit dar. Hierzu benötigen wir allerdings ein wenig Vorbereitung.

Definition 18.3 Sei K ein Körper und $f = \sum_{k=0}^{n} a_k x^k \in K[x]$, mit $n \in \mathbb{N}_0$ und $a_0, ..., a_n \in K$. Dann nennt man

$$f' \quad = \quad \sum_{k=1}^{n} k a_k x^{k-1} \qquad \text{die } \textbf{\textit{formale Ableitung}} \text{ von } f\,.$$

Man überprüft unmittelbar, dass die aus der Analysis bekannten Ableitungsregeln $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$ auch für die formale Ableitung gültig sind.

Proposition 18.4 Sei K ein Körper, $f \in K[x]$ ein Polynom vom Grad $n \geq 1$ und $\tilde{L}$ ein Erweiterungskörper von K, über dem f in Linearfaktoren zerfällt. Dann sind die folgenden beiden Aussage äquivalent:

(i) Es gilt $\mathrm{ggT}(f, f') = 1$ in $K[x]$.

(ii) Das Polynom f besitzt in $\tilde{L}$ nur *einfache* Nullstellen, d.h. es ein $a \in K^\times$ und n verschiedene Elemente $\alpha_1, ..., \alpha_n \in L$, so dass $f = a \prod_{i=1}^{n} (x - \alpha_i)$.

Beweis: Sei $\alpha \in \tilde{L}$ eine Nullstelle von f. Wir zeigen zunächst, dass α genau dann eine mehrfache Nullstelle von f ist, wenn $f'(\alpha) = 0$ gilt. Wegen $f(\alpha) = 0$ gibt es ein Polynom $g \in \tilde{L}[x]$ mit $f = (x - \alpha)g$. Auf Grund der Produktregel gilt $f' = g + (x - \alpha)g'$, und α ist genau dann eine mehrfache Nullstelle von f, wenn

$$g(\alpha) = 0 \quad \Leftrightarrow \quad g(\alpha) + (\alpha - \alpha)g'(\alpha) = 0 \quad \Leftrightarrow \quad f'(\alpha) = 0$$

erfüllt ist. Wir beweisen nun die Äquivalenz. Sind die Polynome f und f' *nicht* teilerfremd in $K[x]$, dann haben sie einen gemeinsamen irreduziblen Faktor $p \in K[x]$. Mit f zerfällt auch p über $\tilde{L}$ in Linearfaktoren. Jede Nullstelle von p in $\tilde{L}$ ist eine gemeinsame Nullstelle von f und f' und somit eine mehrfache Nullstelle von f.

Eine mehrfache Nullstelle α von f in $\tilde{L}$ ist umgekehrt eine gemeinsame Nullstelle von f und f'. Würde in $K[x]$ nun $\mathrm{ggT}(f, f') = 1$ gelten, dann gäbe es nach dem Lemma von Bézout Polynome $a, b \in K[x]$ mit $af + bf' = 1$. Dies hätte den Widerspruch

$$0 \quad = \quad a(\alpha)f(\alpha) + b(\alpha)f'(\alpha) \quad = \quad 1$$

zur Folge. Also sind f und f' in $K[x]$ nicht teilerfremd. □

Proposition 18.5 Sei p eine Primzahl, $n \in \mathbb{N}$ und K ein Körper mit p^n Elementen. Dann ist der Primkörper P von K zu $\mathbb{F}_p$ isomorph, und K ist ein Zerfällungskörper von $f_n = x^{p^n} - x \in P[x]$ über dem Körper P.

Beweis: Dass der Primkörper P von K isomorph zu $\mathbb{F}_p$ sein muss, haben wir schon im Beweis von Satz 18.2 festgestellt. Wir zeigen nun, dass K der Zerfällungskörper von f_n über P ist. Die multiplikative Gruppe $K^\times$ hat die Ordnung p^n-1. (Diese Beobachtung ist ganz entscheidend für das Verständnis der endlichen Körper!) Für jedes $\alpha \in K^\times$ gilt deshalb

$$\alpha^{p^n} \quad = \quad \alpha^{p^n-1}\alpha \quad = \quad \alpha \qquad \Leftrightarrow \qquad \alpha^{p^n} - \alpha \quad = \quad 0 \quad ,$$

also ist jedes solche Element Nullstelle von $f_n = x^{p^n} - x$. Zusätzlich gilt offenbar $f_n(0_K) = 0_K$. Da f_n als Polynom vom Grad p^n andererseits höchstens p^n Nullstellen besitzt, kommen wir insgesamt zu dem Ergebnis, dass die Nullstellenmenge N von f_n mit K übereinstimmt. Das Polynom f_n zerfällt also über K in Linearfaktoren, und zugleich wird K wegen $P(N) = P(K) = K$ über dem Grundkörper P von N erzeugt. Also ist K der Zerfällungskörper von f_n. □

Umgekehrt werden wir nun zeigen, dass jeder Zerfällungskörper des Polynoms $x^{p^n} - x$ über einem Körper mit p Elementen aus genau p^n Elementen besteht. Dies ist ein wichtiger Schritt in Richtung des Existenzbeweises.

Proposition 18.6 Sei p eine Primzahl, R ein Ring der Charakteristik p und $n \in \mathbb{N}$.
Dann gilt

$$(a+b)^{p^n} \quad = \quad a^{p^n} + b^{p^n} \qquad \text{für alle} \quad a, b \in R.$$

Beweis: Ist die Aussage für $n = 1$ erst einmal bewiesen, dann erhält man die Gleichung für beliebiges n durch einen einfachen Induktionsbeweis. Wir können uns also auf den Beweis der Gleichung $(a+b)^p = a^p + b^p$ beschränken. Auf Grund des binomischen Lehrsatzes gilt

$$(a+b)^p \quad = \quad \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \quad = \quad a^p + \sum_{k=1}^{n} \binom{p}{k} a^{p-k} b^k + b^p.$$

Die Binomialkoeffizienten $\binom{p}{k}$ sind für $1 \le k \le p-1$ durch p teilbar, denn in

$$\binom{p}{k} \quad = \quad \frac{p!}{k!(p-k)!} \quad = \quad \frac{1}{k!}\left(\prod_{m=p-k+1}^{p} m\right)$$

wird das Produkt rechts von p geteilt, und wegen $k < p$ wird p durch den Vorfaktor $(k!)^{-1}$ nicht weggekürzt. Aufgefasst als Elemente in R sind die Binomialkoeffizienten $\binom{p}{k}$ für $1 \le k \le p-1$ also gleich Null, und wir erhalten $(a+b)^p = a^p + b^p$. □

Definition 18.7 Ist R ein Ring der Charakteristik p, dann bezeichnet man die Abbildung $\varphi : R \to R$, $a \mapsto a^p$ als ***Frobenius-Endomorphismus*** von R.

Wie wir bereits überprüft haben, ist φ verträglich mit der Addition auf R. Außerdem gilt $\varphi(1_R) = 1_R^p = 1_R$ und $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$. Also ist φ tatsächlich ein Endomorphismus des Rings R. Ist K ein endlicher Körper der Charakteristik p, dann ist der Frobenius-Endomorphismus von K sogar ein Automorphismus. Denn als Körperhomomorphismus ist φ injektiv, und als injektive Abbildung der endlichen Menge K nach K ist φ auch surjektiv, insgesamt eine Bijektion. In dieser Situation wird φ dann auch der ***Frobenius-Automorphismus*** von K genannt.

Proposition 18.8 Sei p eine Primzahl, P ein Körper mit p Elementen, $n \in \mathbb{N}$ und K ein Zerfällungskörper von $f_n = x^{p^n} - x \in P[x]$ über P. Dann gilt $|K| = p^n$.

Beweis: Vorweg bemerken wir, dass $\mathrm{char}(K) = p$ gilt und Proposition 18.6 somit anwendbar ist. Denn wegen $|P| = p$ und $1_P \neq 0_P$ muss die Ordnung von $1_K = 1_P$ in der Gruppe $(P,+)$ ebenfalls gleich p sein, also $\mathrm{char}(P) = p$ gelten. Da K als Zerfällungskörper eines Polynoms über P ein Erweiterungskörper von P ist, gilt auch $\mathrm{char}(K) = p$. Sei nun $M \subseteq K$ die Menge der Nullstellen von f_n in K. Wir zeigen zunächst, dass M ein Teilkörper von K ist. Wegen $f_n(1_K) = 1_K^{p^n} - 1_K = 1_K - 1_K = 0_K$ liegt zunächst 1_K in M. Seien nun $a, b \in K$ vorgegeben. Nach Proposition 18.6 gilt

$$(a-b)^{p^n} \quad = \quad (a+(-b))^{p^n} \quad = \quad a^{p^n} + (-1)^{p^n} b^{p^n} \quad = \quad a + (-1)^{p^n} b.$$

Sowohl im Fall $p = 2$ als auch im Fall $p \neq 2$ erhalten wir $(a-b)^{p^n} = a - b$ und somit $a - b \in M$. Ebenso gilt $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$, also $ab \in M$. Im Fall $a \neq 0$ gilt schließlich $(a^{-1})^{p^n} = a^{-p^n} = (a^{p^n})^{-1} = a^{-1}$ und damit auch $a^{-1} \in M$. Damit ist der Nachweis der Teilkörper-Eigenschaft abgeschlossen.

Nun zeigen wir, dass M ein Erweiterungskörper von P ist. Die multiplikative Gruppe $P^\times$ besteht aus $p-1$ Elementen. Für alle $a \in P^\times$ gilt deshalb $a^p = a^{p-1}a = 1 \cdot a = a$, und natürlich ist die Gleichung $a^p = a$ auch für $a = 0_K$ erfüllt. Damit gilt auch $a^{p^n} = a$ für alle $a \in P$, und es folgt $P \subseteq M$. Insgesamt ist M also ein Erweiterungskörper von P, der genau aus den Nullstellen von f_n besteht und insbesondere von diesen erzeugt wird. Damit ist M der Zerfällungskörper von f_n in K. Dies bedeutet, dass $M = K$ gilt.

Nun brauchen wir nur noch überprüfen, dass f_n genau p^n Nullstellen besitzt und für M als Nullstellenmenge somit $|K| = |M| = p^n$ gilt. Die formale Ableitung von f_n ist gegeben durch $f_n' = p^n x^{p^n-1} - 1 = -1$, also ist $\mathrm{ggT}(f_n', f_n) = 1$. Nach Proposition 18.4 besitzt f_n in K damit p^n voneinander *verschiedene* Nullstellen. Wir erhalten $|K| = |M| = p^n$. □

Wir können nun das Hauptergebnis dieses Abschnitts formulieren.

Satz 18.9 Sei p eine Primzahl und $n \in \mathbb{N}$. Dann gibt es einen Körper mit p^n Elementen, und je zwei Körper mit p^n Elementen sind zueinander isomorph.

Beweis: Zunächst beweisen wir die Existenzaussage. Sei K ein Zerfällungskörper des Polynoms $f_n = x^{p^n} - x \in \mathbb{F}_p[x]$. Dann gilt $|K| = p^n$ nach Proposition 18.8. Sei nun $\tilde{K}$ ein beliebiger Körper mit p^n Elementen und $\tilde{P}$ sein Primkörper. Nach Proposition 18.5 gibt es eine Isomorphismus $\phi : \mathbb{F}_p \to \tilde{P}$, und $\tilde{K}$ ist der Zerfällungskörper von $\tilde{f}_n = x^{p^n} - x \in \tilde{P}[x]$. Offenbar gilt $\tilde{f}_n = \phi(f_n)$. Wir können nun Satz 17.11 über die Eindeutigkeit von Zerfällungskörpern auf die Menge $S = \{f_n\}$ anwenden und erhalten einen Isomorphismus $\psi : K \to \tilde{K}$, der ϕ fortsetzt. □

Folgerung 18.10 Sei p eine prim und $\mathbb{F}_p^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$.

(i) Für jedes $n \in \mathbb{N}$ gibt es genau einen Teilkörper $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p^{\mathrm{alg}}$ mit p^n Elementen.

(ii) Für $m, n \in \mathbb{N}$ gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ genau dann, wenn m ein Teiler von n ist.

(iii) Es gilt $\mathbb{F}_p^{\mathrm{alg}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$.

Beweis: zu (i) Sei $\mathbb{F}_{p^n}$ der Zerfällungskörper von $f_n = x^{p^n} - x \in \mathbb{F}_p[x]$ in $\mathbb{F}_p^{\mathrm{alg}}$. Dann gilt $|\mathbb{F}_{p^n}| = p^n$ nach Proposition 18.8. Ist umgekehrt $L \subseteq \mathbb{F}_p^{\mathrm{alg}}$ ein beliebiger Teilkörper mit p^n Elementen, dann ist $\mathbb{F}_p$ der Primkörper von L, und nach Proposition 18.5 ist L der Zerfällungskörper von f_n in $\mathbb{F}_p^{\mathrm{alg}}$. Also stimmen L und $\mathbb{F}_{p^n}$ überein.

zu (ii) Wenn m ein Teiler von n ist, $n = dm$ mit $d \in \mathbb{N}$, dann ist der Zerfällungskörper von f_m im Zerfällungskörper von f_n enthalten. Ist nämlich $\alpha \in \mathbb{F}_p^{\mathrm{alg}}$ eine Nullstelle von f_m, dann gilt $\alpha^{p^m} = \alpha$, und folglich wird α unter der Abbildung $\phi_m(\alpha) = \alpha^{p^m}$ auf sich selbst abgebildet. Durch vollständige Induktion über $k \in \mathbb{N}_0$ sieht man, dass $\phi_m^k(\alpha) = \alpha^{p^{km}}$ gilt, und wir erhalten insbesondere $\alpha^{p^n} = \alpha^{p^{dm}} = \phi_m^d(\alpha) = \alpha$. Dies zeigt, dass α auch Nullstelle von f_n ist.

Seien umgekehrt $m, n \in \mathbb{N}$ mit der Eigenschaft, dass $\mathbb{F}_{p^m}$ ein Teilkörper von $\mathbb{F}_{p^n}$ ist. Setzen wir $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$, dann handelt es sich bei $\mathbb{F}_{p^n}$ also um einen d-dimensionalen $\mathbb{F}_{p^m}$-Vektorraum. Dieser enthält $(p^m)^d = p^{md}$ Elemente, und aus $p^{md} = |\mathbb{F}_{p^n}| = p^n$ folgt $dm = n$.

zu (iii) Die Inklusion „$\supseteq$“ ist auf Grund der Definition der Teilkörper $\mathbb{F}_{p^n}$ offensichtlich. Zum Nachweis von „$\subseteq$“ sei $\alpha \in \mathbb{F}_p^{\mathrm{alg}}$ vorgegeben. Nach Definition von $\mathbb{F}_p^{\mathrm{alg}}$ ist α algebraisch über $\mathbb{F}_p$. Sei $f = \mu_{\alpha,\mathbb{F}_p}$ und $n = \mathrm{grad}(f)$. Dann gilt $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$, somit ist $\mathbb{F}_p(\alpha)$ ein n-dimensionaler $\mathbb{F}_p$-Vektorraum. Als solcher besteht $\mathbb{F}_p(\alpha)$ aus p^n Elementen, und aus der Eindeutigkeitsaussage in Teil (i) folgt $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$; insbesondere gilt $\alpha \in \mathbb{F}_{p^n}$. □

§ 19. *Separable Körpererweiterungen und Galois-Erweiterungen*

Zusammenfassung. Eine Körpererweiterung $L|K$ wird *separabel* genannt, wenn das Minimalpolynom jedes Element von L über K nur einfache Nullstellen hat. Diese Eigenschaft spielt in der Galoistheorie eine wichtige Rolle, weil sie Auswirkung auf die Anzahl der K-Homomorphismen von L in andere Körper hat. Wie wir sehen werden, ist sie immer gegeben, wenn K ein Körper der Charakteristik 0 oder ein endlicher Körper ist.

Eine weitere wichtige Eigenschaft endlicher separabler Erweiterungen kommt im Satz vom *primitiven Element* zum Ausdruck, welcher besagt, dass solche Erweiterungen stets durch ein einziges Element erzeugt werden können. In Anbetracht der Tatsache, dass solche Erweiterungen bei einem Grundkörper wie $\mathbb{Q}$ bereits eine sehr komplizierte Struktur haben können, ist dies eine bemerkenswerte Aussage.

Wichtige Grundbegriffe

- separables Polynom
- separables Element in einer Körpererweiterung
- separable Körpererweiterung
- rationaler Funktionenkörper $\mathbb{F}_p(t)$ über $\mathbb{F}_p$
- Separabilitätsgrad einer endlichen Erweiterung

Zentrale Sätze

- Separabilität von algebraischen Erweiterungen endlicher Körper und von Körpern der Charakteristik 0
- Satz vom primitiven Element
- Endliche separable Erweiterungen haben endlich viele Zwischenkörper.
- Kennzeichnung von separablen Erweiterungen durch die Anzahl von Körperhomomorphismen

Definition 19.1 Sei K ein Körper. Ein irreduzibles Polynom $f \in K[x]$ wird ***separabel*** genannt, wenn $\mathrm{ggT}(f, f') = 1$ gilt.

Nach Proposition 18.4 ist die Separabilität von f gleichbedeutend damit, dass f irreduzibel ist und in jedem Erweiterungskörper L von K nur einfache Nullstellen besitzt.

Definition 19.2 Sei $L|K$ eine Körpererweiterung. Ein Element $\alpha \in L$ wird ***separabel*** über K genannt, wenn es algebraisch über K ist und sein Minimalpolynom $f \in K[x]$ separabel ist. Wir nennen die Erweiterung $L|K$ separabel, wenn jedes $\alpha \in L$ über K separabel ist.

Proposition 19.3 Ist $L|K$ eine Körpererweiterung, $\alpha \in L$ ein über K separables Element und M ein Zwischenkörper von $L|K$, dann ist α auch separabel über M.

Beweis: Sei $f \in K[x]$ das Minimalpolynom von α über K und $g \in M[x]$ das Minimalpolynom von α über M. Da f auch in $M[x]$ liegt und $f(\alpha) = 0$ gilt, ist g als Minimalpolynom ein Teiler von f. Sei $\tilde{L}$ nun ein algebraischer Abschluss von L. Da α über K separabel ist, besitzt f in $\tilde{L}$ keine mehrfachen Nullstellen. Dasselbe gilt dann auch für den Teiler g von f. Also ist das Minimalpolynom $g \in M[x]$ separabel und α damit separabel über M. □

Satz 19.4 Ist K ein Körper der Charakteristik 0, dann ist jede algebraische Erweiterung $L|K$ separabel.

Beweis: Sei $\alpha \in L$ und $f \in K[x]$ sein Minimalpolynom. Ist $n = \text{grad}(f)$, dann ist $n \in \mathbb{N}$, und f' ist vom Grad $n-1$. (Dies ist für Polynome über Körpern positiver Charakteristik falsch, wie man anhand des Polynoms $x^p - 1$ über dem Körper $\mathbb{F}_p$ sieht.) Weil $\text{ggT}(f, f')$ ein Teiler von f' gilt, ist auch $\text{ggT}(f, f')$ höchstens vom Grad $n-1$. Andererseits ist f irreduzibel und $\text{ggT}(f, f')$ auch ein Teiler von f. Deshalb muss $\text{ggT}(f, f')$ entweder konstant oder ein konstantes Vielfaches von f sein. Wegen $\text{ggT}(f, f') \leq n-1$ bleibt nur die erste Möglichkeit. Also sind f und f' teilerfremd, das Polynom f ist also separabel, und damit ist auch α separabel über K. □

Satz 19.5 Ist K ein endlicher Körper, dann ist jede algebraische Erweiterung $L|K$ separabel.

Beweis: Sei $|K| = q$, $q = p^r$ mit einer Primzahl p und einem $r \in \mathbb{N}$, und sei $\alpha \in L$ ein beliebiges Element. Dann gilt $|K(\alpha)| = q^n = p^{rn}$, wobei $n = [K(\alpha) : K]$ ist. Das Element α ist damit Nullstelle des Polynoms $g = x^{p^{rn}} - x \in K[x]$, und wegen $g' = -1$ besitzt dieses im algebraischen Abschluss $\tilde{L}$ von L nur einfache Nullstellen. Das Minimalpolynom $f \in K[x]$ von α ist ein Teiler von g, also hat auch f in $\tilde{L}$ nur einfache Nullstellen, und es folgt $\text{ggT}(f, f') = 1$ nach Proposition 18.4. □

In Anbetracht von Satz 19.4 und Satz 19.5 drängt sich die Frage auf, ob es überhaupt Körper mit nicht-separablen algebraischen Erweiterungen gibt. Sei p eine Primzahl und $K = \mathbb{F}_p(t)$ der ***rationale Funktionenkörper*** über $\mathbb{F}_p$. Dabei handelt es sich um den Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$, dessen Elemente durch

$$\mathbb{F}_p(t) \quad = \quad \left\{ \frac{g}{h} \;\middle|\; g, h \in \mathbb{F}_p[t],\ h \neq \bar{0} \right\}$$

gegeben sind. Außerdem sei $u = \sqrt[p]{t}$ eine Nullstelle des Polynoms $f = x^p - t \in K[x]$ in einem Erweiterungskörper von K, also ein Element u mit $u^p = t$. Dann ist dieses Element nicht separabel über K, die Erweiterung $L|K$ mit dem Körper $L = K(u) = K(\sqrt[p]{t})$ also eine nicht-separable algebraische Erweiterung.

Um dies zu sehen, bemerken wir zunächst, dass das Polynom $f = x^p - t$ über L in Linearfaktoren zerfällt, denn wegen $\text{char}(L) = p$ gilt $f = x^p - u^p = (x-u)^p$. Wäre f über K reduzibel, dann hätte ein Teiler von f die Form $(x-u)^m$ mit $1 \leq m < p$. Insbesondere müsste der konstante Term $(-1)^m u^m$ des Teilers und somit auch das Element u^m in K liegen. Aber dies ist nicht der Fall. Denn andernfalls gäbe es $g, h \in \mathbb{F}_p[t]$ mit

$$u^m = \frac{g(t)}{h(t)} = \frac{g(u^p)}{h(u^p)} \quad \Leftrightarrow \quad g(u^p) \cdot u^m = h(u^p).$$

Das Element u wäre damit eine Nullstelle des Polynoms $F \in \mathbb{F}_p[x]$ gegeben durch $F = g(x^p) \cdot x^m - h(x^p)$, und es ist $F \neq \bar{0}$, weil die Polynome $g(x^p) \cdot x^m$ und $h(x^p)$ von unterschiedlichem Grad sind; der Grad von $h(x^p)$ ist im Gegensatz zum Grad des Polynoms $g(x^p) \cdot x^m$ durch p teilbar. Die Gleichung $F(u) = \bar{0}$ zeigt dann, dass das Element $u \in L$ über $\mathbb{F}_p$ algebraisch ist. Dann wäre auch $t = u^p$ über $\mathbb{F}_p$ algebraisch, also Nullstelle eines Polynoms $F_1 \in \mathbb{F}_p[x]$. Aber dies ist unmöglich, denn mit F_1 ist auch $F_1(t) \in \mathbb{F}_p[t]$ ein Polynom ungleich null.

Der Widerspruch zeigt, dass eine Zerlegung von $f \in K[x]$ der oben angegebenen Form nicht existiert und f somit irreduzibel ist. Insgesamt ist damit f das Minimalpolynom von u über K, also $f = \mu_{u,K}$. Da u aber eine p-fache

Nullstelle von f ist, ist das Minimalpolynom f ein nicht-separables Polynom, und folglich ist das Element u über dem Grundkörper K nicht separabel.

Wir kommen nun zur Formulierung eines zentralen Resultats über separable Erweiterungen.

Definition 19.6 Eine Körpererweiterung $L|K$ wird ***einfach*** genannt, wenn ein Element $\alpha \in L$ mit $L = K(\alpha)$ existiert. In diesem Fall nennt man α eine ***primitives Element*** der Erweiterung.

Satz 19.7 *(Satz vom primitiven Element)*
Jede endliche, separable Erweiterung $L|K$ ist einfach.

Beweis: Ist K ein endlicher Körper, dann ist auch L endlich. Aus der Zahlentheorie-Vorlesung ist bekannt, dass $L^\times$ als multiplikative Gruppe eines endlichen Körpers zyklisch ist. Ist $\alpha \in L^\times$ ein Erzeuger der Gruppe, dann gilt offenbar $L = K(\alpha)$, also ist $L|K$ einfach. Von nun an gehen wir davon aus, dass der Körper K unendlich ist.

Da es sich bei $L|K$ um eine endliche Erweiterung handelt, gibt es Elemente $\alpha_1, ..., \alpha_r$ mit $L = K(\alpha_1, ..., \alpha_r)$. (Man kann zum Beispiel eine Basis von L als K-Vektorraum nehmen.) Wir beweisen nun durch vollständige Induktion über r, dass eine solche Erweiterung einfach ist. Für $r = 1$ folgt die Aussage direkt aus der Definition. Sei nun $r > 1$, und setzen wir die Aussage für alle $s < r$ voraus. Nach Induktionsvoraussetzung ist $L_0 = K(\alpha_1, ..., \alpha_{r-1})$ einfach. Es gibt also ein $\alpha \in L_0$ mit $L_0 = K(\alpha)$. Setzen wir $\beta = \alpha_r$, dann gilt also $L = K(\alpha, \beta)$. Es bleibt zu zeigen, dass die Erweiterung $L|K$ von einem einzigen Element erzeugt wird.

Sei $\tilde{L}$ ein algebraischer Abschluss von L, $f \in K[x]$ das Minimalpolynom von α über K und $g \in K[x]$ das Minimalpolynom von β über K. Dann zerfallen f und g über $\tilde{L}$ in Linearfaktoren, d.h. es gibt $\alpha_1, ..., \alpha_m \in \tilde{L}$ und $\beta_1, ..., \beta_n$ mit

$$f \quad = \quad \prod_{i=1}^{m}(x-\alpha_i) \qquad \text{und} \qquad g \quad = \quad \prod_{j=1}^{n}(x-\beta_j) \quad ,$$

wobei wir $\alpha_1 = \alpha$ und $\beta_1 = \beta$ annehmen können. Ferner sind die Elemente $\alpha_1, ..., \alpha_m$ und $\beta_1, ..., \beta_n$ jeweils verschieden voneinander, weil α und β über K separabel und f und g damit separable Polynome sind. Für jedes $c \in K^\times$ sei nun $\gamma_c = \alpha + c\beta$ und $M_c = K(\gamma_c)$. Wir werden zeigen, dass c so gewählt werden kann, dass $M_c = K(\alpha, \beta)$ erfüllt ist. Dazu betrachten wir das Polynom $h_c = f(\gamma_c - cx) = \prod_{i=1}^{m} h_{c,i} \in M_c[x]$ mit den Linearfaktoren

$$h_{c,i} \quad = \quad (\gamma_c - cx) - \alpha_i \quad = \quad \gamma_c - (\alpha_i + cx) \qquad \text{in } \tilde{L}[x].$$

Das Polynom h_c ist so konstruiert, dass es $\beta = \beta_1$ auf jeden Fall als Nullstelle besitzt, denn nach Definition gilt $h_{c,1}(\beta) = \gamma_c - (\alpha_1 + c\beta) = \gamma_c - (\alpha + c\beta) = \gamma_c - \gamma_c = 0$ und somit $h_c(\beta_1) = h_c(\beta) = 0$. Andererseits kann das Element c so gewählt werden, dass $\beta_2, ..., \beta_n$ nicht als Nullstellen von h_c auftreten. Für $1 \le i \le m$ und $2 \le j \le n$ gelten nämlich ie Gleichungen

$$h_{c,i}(\beta_j) \quad = \quad \gamma_c - (\alpha_i + c\beta_j) \quad = \quad (\alpha + c\beta) - (\alpha_i + c\beta_j) \quad = \quad (\alpha - \alpha_i) + c(\beta - \beta_j)$$

und somit die Äquivalenzen

$$h_{c,i}(\beta_j) \neq 0 \qquad \Leftrightarrow \qquad (\alpha-\alpha_i)+c(\beta-\beta_j) \neq 0 \qquad \Leftrightarrow \qquad c \neq -\frac{\alpha-\alpha_i}{\beta-\beta_j}.$$

Weil K unendlich ist, können wir c so wählen, dass diese Ungleichungen alle erfüllt sind und somit $h_c(\beta_j) \neq 0$ für $2 \leq j \leq n$ gilt. In diesem Fall ist dann $x-\beta$ der einzige Linearfaktor von g, der auch das Polynom h_c teilt, es gilt also $x-\beta \quad = \quad \mathrm{ggT}(g,h_c)$. Aber der größte gemeinsame Teiler von zwei Polynomen $g,h_c \in M_c[x]$ ist wiederum in $M_c[x]$ enthalten. Es folgt $\beta \in M_c$ und damit auch $\alpha = \gamma_c - c\beta \in M_c$. Aus $\alpha,\beta \in M_c$ erhalten wir $K(\alpha,\beta) \subseteq M_c = K(\gamma_c)$. Da andererseits $\gamma_c = \alpha + c\beta$ in $K(\alpha,\beta)$ liegt, erhalten wir insgesamt die gewünschte Gleichung $K(\alpha,\beta) = K(\gamma_c)$. □

Satz 19.8 Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann gilt $|\mathrm{Hom}_K(L,\tilde{K})| \leq [L:K]$ mit Gleichheit genau dann, wenn die Erweiterung $L|K$ separabel ist.

Beweis: Wir beweisen die Ungleichung und die „⇐“-Richtung der Implikation durch vollständige Induktion über $n = [L:K]$. Genauer gesagt zeigen wir etwas allgemeiner: Ist $\phi : K \to \tilde{K}$ ein beliebiger Körperhomomorphismus, so gibt es $\leq [L:K]$ Fortsetzungen von ϕ auf L; bei einer separablen Erweiterung $L|K$ gibt es genau $[L:K]$ solche Fortsetzungen. Im Fall $n = 1$ ist nichts zu zeigen, denn dann gilt $L = K$, die Erweiterung ist separabel (weil jedes Minimalpolynom $\mu_{K,\alpha}$ eines Elements $\alpha \in K$ vom Grad 1 und somit separabel ist), und die einzige Fortsetzung von ϕ auf K ist offenbar ϕ selbst.

Sei nun $n = [L:K] > 1$, und setzen wir die Aussage für Erweiterungen kleinen Grades voraus. Sei $\alpha \in L \setminus K$, $f = \mu_{K,\alpha}$, $m = \mathrm{grad}(f) = [K(\alpha):K]$ und $\tilde{f} = \phi(f)$. Nach Folgerung 16.4 ist die Anzahl m_1 der Fortsetzungen von ϕ zu einem Homomorphismus $K(\alpha) \to \tilde{K}$ gleich der Anzahl der verschiedenen Nullstellen von $\tilde{f}$ in $\tilde{K}$. Wir bezeichnen diese Anzahl mit m_1. Weil $\tilde{f}$ als Polynom über einem Körper nicht mehr als $m = \mathrm{grad}(\tilde{f})$ Nullstellen in $\tilde{K}$ haben kann, gilt $m_1 \leq m$ mit Gleichheit genau dann, wenn das Polynom $\tilde{f}$ separabel ist. Letzteres wiederum ist genau dann der Fall, wenn f separabel ist (denn die Bedingung $\mathrm{ggT}(f,f') = 1$ bleibt unter dem Körperhomomorphismus ϕ erhalten), und dies wiederum ist äquivalent zur Separabilität von α über K. Ist nun die Erweiterung $L|K$ separabel, dann insbesondere das Element α über K, und dann folgt $m_1 = m$. In jedem Fall bezeichnen wir mit $\psi_1,\ldots,\psi_{m_1}$ die verschiedenen Fortsetzungen von ϕ auf den Körper $K(\alpha)$.

Wegen $K \subsetneq K(\alpha)$ gilt $[K(\alpha):K] > 1$. Für den Erweiterungsgrad $r = [L:K(\alpha)]$ gilt dann auf Grund der Gradformel $r = [L:K(\alpha)] = \frac{[L:K]}{[K(\alpha):K]} < [L:K] = n$. Nach Induktionsvoraussetzung besitzt jedes ψ_i höchstens r Fortsetzungen auf L. Weil jede Fortsetzung von ϕ auf L durch Fortsetzung eines ψ_i auf L zu Stande kommt, ist die Anzahl der Fortsetzungen von ϕ auf L durch $m_1 r \leq mr = [K(\alpha):K]\cdot[L:K(\alpha)] = [L:K] = n$ begrenzt. Ist nun $L|K$ separabel, dann ist jedes $\beta \in L$ nach Proposition 19.3 auch separabel über $K(\alpha)$, die Erweiterung $L|K(\alpha)$ also separabel. Nach Induktionsvoraussetzung besitzt jedes ψ_i dann genau r Fortsetzungen, und insgesamt existieren dann genau $n = mr$ Fortsetzungen von ϕ auf L. Damit ist der Induktionsschritt abgeschlossen.

Beweisen wir nun noch die Richtung „⇒“ der Äquivalenz und nehmen dazu an, dass $L|K$ nicht separabel ist. Dann gibt es ein Element $\alpha \in L$, das nicht separabel über K ist. Wie bereits oben bemerkt, ist die Anzahl m_1 der K-Homomorphismen $K(\alpha) \to \tilde{K}$, also die Anzahl der Fortsetzungen der identischen Abbildung $K \to \tilde{K}$, $a \mapsto a$, dann kleiner als $m = [K(\alpha):K]$. Für jeden solchen K-Homomorphismus wiederum gibt es höchstens $r = [L:K(\alpha)]$ Fortsetzungen von $K(\alpha)$ auf L. Die Gesamtzahl der K-Homomorphismen $L \to \tilde{K}$ ist damit beschränkt durch $m_1 r$, insbesondere ist die Anzahl kleiner als $mr = [L:K]$. □

Definition 19.9 Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann nennt man

$$[L:K]_{\text{sep}} \quad = \quad |\text{Hom}_K(L,\tilde{K})|$$

den ***Separabilitätsgrad*** der Erweiterung $L|K$.

Der Separabilitätsgrad ist von der Wahl des algebraisch abgeschlossenen Erweiterungskörpers $\tilde{K}$ unahängig. Denn zunächst einmal ist jedes $\sigma \in \text{Hom}_K(L,\tilde{K})$ ein K-Isomorphismus von L auf sein Bild $\sigma(L)$, und dieses damit eine endliche und insbesondere algebraische Erweiterung von K. Das Bild $\sigma(L)$ ist also im algebraischen Abschluss von K innerhalb des Körper $\tilde{K}$ enthalten, so dass sich $\text{Hom}_K(L,\tilde{K})$ nicht ändert, wenn wir $\tilde{K}$ durch diesen algebraischen Abschluss ersetzen. Außerdem existiert nach Folgerung 17.12 zwischen je zwei algebraischen Abschlüssen $\tilde{K}_1$ und $\tilde{K}_2$ ein K-Isomorphismus ϕ, so dass zwischen $\text{Hom}_K(L,\tilde{K}_1)$ und $\text{Hom}_K(L,\tilde{K}_2)$ durch $\sigma \mapsto \phi \circ \sigma$ eine Bijektion gegeben ist.

Der Satz vom primitiven Element hat auch Auswirkungen auf die Anzahl der Zwischenkörper einer algebraischen Erweiterung. Diesen Zusammenhang sehen wir uns als nächstes an. Als Vorbereitung beweisen wir

Lemma 19.10 Sei $L|K$ eine einfache algebraische Erweiterung, also $L = K(\alpha)$ für ein $\alpha \in L$. Sei M ein Zwischenkörper von $L|K$ und

$$f \quad = \quad x^n + \sum_{i=0}^{n-1} a_i x^i \quad \in M[x]$$

das Minimalpolynom von α über M. Dann gilt $M = K(a_0,\ldots,a_{n-1})$.

Beweis: Sei $M_0 = K(a_0,\ldots,a_{n-1})$. Dann ist M_0 jedenfalls in M enthalten, denn jedes der Elemente a_i liegt nach Voraussetzung in M. Wir betrachten nun die Erweiterung $L|M_0$. Wegen $L = K(\alpha)$ gilt erst recht $L = M_0(\alpha)$, und das Polynom f ist irreduzibel in $M_0[x]$, weil es sogar in $M[x]$ irreduzibel ist. Also ist f auch das Minimalpolynom von α über M_0, und wir erhalten

$$[L:M] \quad = \quad \text{grad}(f) \quad = \quad [L:M_0].$$

Der Gradsatz liefert nun

$$[M_0:K] \quad = \quad \frac{[L:K]}{[L:M_0]} \quad = \quad \frac{[L:K]}{[L:M]} \quad = \quad [M:K].$$

Zusammen mit $M_0 \subseteq M$ erhalten wir $M_0 = M$. □

Satz 19.11 Eine endliche Erweiterung $L|K$ besitzt genau dann nur endlich viele Zwischenkörper, wenn sie einfach ist.

Beweis: Ist K ein endlicher Körper, dann ist auch L endlich. Weil es in L nur endlich viele Teilmengen gibt, kann es auch nur endlich viele Zwischenkörper gegeben. Andererseits ist $L^\times$ als multiplikative Gruppe eines endlichen

Körpers zyklisch, und ist α ein Erzeuger dieser Gruppe, dann gilt $L = K(\alpha)$. Die Äquivalenz ist im Fall endlicher Körper also richtig, weil beide Teilaussagen immer erfüllt sind. Wir setzen von nun an voraus, dass K unendlich ist.

„⇐“ Sei $\alpha \in L$ ein Element mit $L = K(\alpha)$ und $f \in K[x]$ das Minimalpolynom von α über K. Sei außerdem M ein Zwischenkörper von $L|K$ und $g \in M[x]$ das Minimalpolynom von α über M. Da f in $M[x]$ liegt und $f(\alpha) = 0$ gilt, ist f ein Vielfaches von $g[x]$. Außerdem wird M nach Lemma 19.10 von den Koeffizienten von g erzeugt. Jedem Zwischenkörper kann also ein normierter Teiler von f zugeordnet werden, und diese Zuordnung ist injektiv. Da f nur endlich viele normierte Teiler besitzt, kann es auch nur endlich viele Zwischenkörper geben.

„⇒“ Da $L|K$ eine endliche Erweiterung ist, gibt es Elemente $\alpha_1, ..., \alpha_r \in L$ mit $L = K(\alpha_1, ..., \alpha_r)$. Wir zeigen nun durch vollständige Induktion über r, dass jede algebraische Erweiterung $L|K$, die nur endlich viele Zwischenkörper besitzt und von r Elementen $\alpha_1, ..., \alpha_r$ erzeugt wird, eine einfache Erweiterung ist.

Für $r = 1$ ist nichts zu zeigen. Sei nun $r > 1$, und setzen wir die Aussage für alle $s < r$ als gültig voraus. Setzen wir $L_0 = K(\alpha_1, ..., \alpha_{r-1})$, dann hat mit $L|K$ auch die Erweiterung $L_0|K$ nur endlich viele Zwischenkörper. Nach Induktionsvoraussetzung gibt es ein $\alpha \in L_0$ mit $L_0 = K(\alpha)$. Es gilt dann $L = K_0(\beta) = K(\alpha, \beta)$ mit $\beta = \alpha_r$. Da $L|K$ nur endlich viele Zwischenkörper besitzt, der Körper K nach Voraussetzung aber unendlich ist, gibt es Elemente $c, d \in K$, $c \neq d$, so dass

$$K(\alpha + c\beta) \quad = \quad K(\alpha + d\beta) \qquad \text{gilt.}$$

Setzen wir $M = K(\alpha + c\beta)$, dann liegen also die Elemente $\alpha + c\beta$ und $\alpha + d\beta$ beide in M. Es folgt $(\alpha + c\beta) - (\alpha + d\beta) = (c - d)\beta \in M$ und wegen $(c - d) \in K^\times$ auch $\beta \in M$. Dies wiederum bedeutet, dass auch $\alpha = (\alpha - c\beta) + c\beta$ in M liegt. Aus $\alpha, \beta \in M$ folgt $K(\alpha, \beta) \subseteq M$, und wegen $\alpha + c\beta \in K(\alpha, \beta)$ folgt umgekehrt $M \subseteq K(\alpha, \beta)$. Also ist $L|K$ eine einfache Erweiterung. □

Folgerung 19.12 Jede endliche, separable Erweiterung $L|K$ besitzt nur endlich viele Zwischenkörper.

Beweis: Nach dem Satz vom primitiven Element ist $L|K$ einfach, und nach Satz 19.11 besitzt $L|K$ deshalb nur endlich viele Zwischenkörper. □

§ 20. *Kreisteilungspolynome und Quadratisches Reziprozitätsgesetz*

Zusammenfassung. Die *Kreisteilungskörper* verdanken ihren Namen der Eigenschaft, von den sog. *Einheitswurzeln* erzeugt zu werden, die als Punkte in der komplexen Ebene den Einheitskreis gleichmäßig unterteilen. Die Minimalpolynome der Einheitswurzeln bezeichnet man als *Kreisteilungspolynome*. Die Nullstellen des n-ten Kreisteilungspolynom sind dabei gerade die *primitiven* n-ten Einheitswurzeln. Wir werden zeigen, dass es sich dabei um ganzzahlige Polynome handelt, und geben eine Rekursionsformel für ihre Berechnung an. Besonderen Aufwand erfordert der Beweis, dass die Polynome, die durch die Formel definiert werden, tatsächlich über $\mathbb{Q}$ irreduzibel sind. Hier kommen unter anderem die Ergebnisse aus § 13 zur Anwendung.

Mit dem *Quadratischen Reziprozitätsgesetz* (QRG) lässt sich die Frage nach der Lösbarkeit von Kongruenzen der Form $x^2 \equiv a \bmod p$ für eine vorgegebene Primzahl p und ein vorgegebenes $a \in \mathbb{Z}$ schnell und effizient beantworten. Der Beweis des QRG durch Gauß in seinen *Disquisitiones Arithmeticae* gilt als ein Höhepunkt der Elementaren Zahlentheorie. Die Bemühungen, dieses Gesetz auf höhere Potenzen zu verallgemeinern, hatten einen entscheidenden Einfluss auf die Entwicklung der *Algebraischen Zahlentheorie* zu einem eigenständigen Teilgebiet der Mathematik.

Wichtige Grundbegriffe	***Zentrale Sätze***
– n-te Einheitswurzel, primitive n-Einheitswurzel	– Rekursionsformel für Kreisteilungspolynome
– Gruppe μ_n der Einheitswurzeln	– Irreduzibilität der Kreisteilungspolynome über $\mathbb{Q}$
– n-tes Kreisteilungspolynom	– der Isomorphismus $\mathrm{Gal}(\mathbb{Q}(\zeta_n)\|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$
– quadratischer Rest, Legendre- und Jacobisymbol	– Quadratisches Reziprozitätsgesetz und Ergänzungssätze

Wir beginnen mit der Definition der Einheitswurzeln.

Definition 20.1 Sei $n \in \mathbb{N}$. Eine ***n-te Einheitswurzel*** in $\mathbb{C}$ ist ein Element $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$.

Wie man leicht nachrechnet, bilden die n-ten Einheitswurzeln eine Untergruppe von $\mathbb{C}^\times$, die wir mit μ_n bezeichnen. Es gilt $\mu_n = \left\{ e^{2\pi i k/n} \;\middle|\; 0 \le k < n \right\}$, denn nach Definition sind die n-ten Einheitswurzeln genau die Nullstellen von $x^n - 1 \in \mathbb{Z}[x]$ in $\mathbb{C}$, und da $x^n - 1$ ein Polynom vom Grad n ist, kann es höchstens n verschiedene Nullstellen in $\mathbb{C}$ geben. Andererseits sind durch die Elemente auf der rechten Seite der Gleichung wegen $\left(e^{2\pi i k/n}\right)^n = e^{2\pi i k} = 1$ offenbar n verschiedene Nullstellen des Polynoms gegeben. Das Element $\zeta_n = e^{2\pi i/n}$ ist ein Erzeuger der Gruppe μ_n, es gilt also $\mu_n = \langle \zeta_n \rangle$.

Lemma 20.2 Sei $k \in \mathbb{Z}$. Genau dann gilt $\mu_n = \langle \zeta_n^k \rangle$, wenn $\mathrm{ggT}(k,n) = 1$ ist.

Beweis: Sei G eine zyklische Gruppe der endlichen Ordnung n und g ein Erzeugendes Element. Nach Teil (i) von Satz 3.9 ist g^k genau dann von Ordnung n, und somit ebenfalls ein Erzeuger von G, wenn $\mathrm{ggT}(k,n) = 1$ ist. Das Lemma ist ein Spezialfall dieser Aussage. □

Definition 20.3 Sei $n \in \mathbb{N}$, $n \geq 2$. Eine ***primitive*** n-te Einheitswurzel ist ein Element $\zeta \in \mu_n$ mit $\mu_n = \langle \zeta \rangle$. Wir bezeichnen mit $\mu_n^\times \subseteq \mu_n$ die Menge der primitiven n-ten Einheitswurzeln. Das Polynom $\Phi_n \in \mathbb{C}[x]$ gegeben durch

$$\Phi_n \quad = \quad \prod_{\zeta \in \mu_n^\times} (x - \zeta)$$

wird das n-te ***Kreisteilungspolynom*** genannt.

Aus technischen Gründen setzen wir $\Phi_1 = x-1$, obwohl wir für $n = 1$ keine primitiven n-ten Einheitswurzeln definiert haben. Nach Lemma 20.2 gilt für alle $n \geq 2$ jeweils

$$|\mu_n^\times| \quad = \quad |\{k \in \mathbb{Z} \mid 0 \leq k < n, \mathrm{ggT}(k,n) = 1\}| \quad = \quad \varphi(n) \quad ,$$

also ist $\varphi(n)$ auch der Grad des Polynoms Φ_n. Unser nächstes Ziel besteht in dem Nachweis, dass jedes Kreisteilungspolynom nicht nur über $\mathbb{C}$, sondern über den ganzen Zahlen definiert ist.

Lemma 20.4 Für alle $n \in \mathbb{N}$ gilt $x^n - 1 = \prod_{d|n} \Phi_d$, wobei d die natürlichen Teiler von n durchläuft.

Beweis: Nach Definition sind die Nullstellen von $x^n - 1$ genau die Elemente $\zeta \in \mathbb{C}^\times$ mit $\zeta^n = 1$. Die Ordnung $d = \mathrm{ord}(\zeta)$ von ζ in $\mathbb{C}^\times$ ist dann ein Teiler von n. Also erzeugt ζ erzeugt in diesem Fall die Gruppe μ_d, ist also eine primitive d-te Einheitswurzel und somit eine Nullstelle von Φ_d. Sei umgekehrt ζ eine Nullstelle von Φ_d für einen Teiler d von n. Ist $k \in \mathbb{N}$ mit $n = kd$, dann gilt $\zeta^n = (\zeta^d)^k = 1^k = 1$, also ist ζ eine Nullstelle von $x^n - 1$.

Somit haben wir gezeigt, dass die Nullstellenmengen der beiden Polynome auf der linken und rechten Seite der Gleichung übereinstimmen. Beide Polynome haben darüber hinaus nur einfache Nullstellen, also sind sie gleich. □

Satz 20.5 Es gilt $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$.

Beweis: Erneut führen wir den Beweis durch vollständige Induktion über n. Für $n = 1$ ist die Aussage wegen $\Phi_1 = x - 1$ klar. Sei nun $n > 1$, und setzen wir $\Phi_d \in \mathbb{Z}[x]$ für alle $d < n$ voraus. Nach Lemma 20.4 gilt

$$x^n - 1 \quad = \quad \prod_{d|n} \Phi_d \quad .$$

Sei nun $S = \{d \in \mathbb{N} \mid d|n, d < n\}$ und $g = \prod_{d\in S} \Phi_d$. Dann gilt also $x^n - 1 = g \cdot \Phi_n$, wobei das Polynom g nach Induktionsvoraussetzung in $\mathbb{Z}[x]$ liegt; darüber hinaus ist es normiert. Wir zeigen nun zunächst, dass Φ_n in $\mathbb{Q}[x]$ enthalten ist. Weil $\mathbb{Q}[x]$ ein euklidischer Ring ist, gibt es Polynome $q, r \in \mathbb{Q}[x]$ mit $g \cdot \Phi_n = x^n - 1 = qg + r$ und $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$. Durch Umformen erhalten wir $(\Phi_n - q)g = r$, und auf Grund des Grades von g bleibt $r = 0$ als einzige Möglichkeit. Es gilt also $g \cdot \Phi_n = gq$ und somit $\Phi_n = q \in \mathbb{Q}[x]$, da $\mathbb{Q}$ ein Integritätsbereich ist, in dem die Kürzungsregel angewendet werden kann.

Also ist g ein normierter Teiler von $x^n - 1$ im Ring $\mathbb{Q}[x]$, wobei g und $x^n - 1$ beide in $\mathbb{Z}[x]$ liegen. Nach Satz 13.9 folgt daraus, dass g auch ein Teiler von $x^n - 1$ im Ring $\mathbb{Z}[x]$ ist. Es gibt also ein eindeutig bestimmtes, normiertes Polynom $h \in \mathbb{Z}[x]$ mit $x^n - 1 = gh$. Aus $gh = x^n - 1 = g \cdot \Phi_n$ folgt $\Phi_n = h \in \mathbb{Z}[x]$. □

Die Produktformel $x^n - 1 = \prod_{d|n} \Phi_d$ kann verwendet werden, um die Kreisteilungspolynome für die einzelnen natürlichen Zahlen n rekursiv zu berechnen. Ist p zum Beispiel eine Primzahl, dann gilt

$$x^p - 1 \quad = \quad \Phi_1 \Phi_p \quad = \quad (x-1)\Phi_p$$

und somit

$$\Phi_p \quad = \quad \frac{x^p - 1}{x - 1} \quad = \quad x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Ist $q \in \mathbb{N}$ eine Primzahlpotenz, $q = p^r$ mit einer Primzahl p und $r \in \mathbb{N}$, $r \geq 2$, dann gilt

$$x^{p^r} - 1 \quad = \quad \prod_{d|p^r} \Phi_d \quad = \quad \left(\prod_{d|p^{r-1}} \Phi_d \right) \Phi_{p^r} \quad = \quad \left(x^{p^{r-1}} - 1 \right) \Phi_{p^r}$$

also

$$\begin{aligned} \Phi_{p^r} \quad = \quad \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \quad = \quad \frac{(x^{p^{r-1}})^p - 1}{x^{p^{r-1}} - 1} \quad = \quad & \left(x^{p^{r-1}} \right)^{p-1} + \left(x^{p^{r-1}} \right)^{p-2} + \ \ldots \ + \left(x^{p^{r-1}} \right)^1 + \left(x^{p^{r-1}} \right)^0 \\ = \quad & x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \ \ldots \ + x^{p^{r-1}} + 1. \end{aligned}$$

Das sechste Kreisteilungspolynom berechnet man durch

$$\Phi_6 \quad = \quad \frac{x^6 - 1}{\Phi_1 \Phi_2 \Phi_3} \quad = \quad \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)} \quad = \quad x^2 - x + 1 \quad ,$$

und das zwölfte Kreisteilungspolynom erhält man durch die Rechnung

$$\Phi_{12} \quad = \quad \frac{x^{12} - 1}{\Phi_1 \Phi_2 \Phi_3 \Phi_4 \Phi_6} \quad = \quad \frac{x^{12} - 1}{(x-1)(x+1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)} \quad = \quad x^4 - x^2 + 1.$$

Wir zeigen nun, dass die Kreisteilungspolynome über $\mathbb{Q}$ irreduzibel sind. Zur Vorbereitung bemerken wir

Lemma 20.6 Für jedes Polynom $f \in \mathbb{F}_p[x]$ gilt $f^p = f(x^p)$.

Beweis: Wir können $f \neq 0$ voraussetzen. Sei $f = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in \mathbb{F}_p$. Auf Grund der allgemeinen Rechenregel $(a + b)^p = a^p + b^p$ in Ringen der Charakteristik p und der Gleichung $a^p = a$ für alle $a \in \mathbb{F}_p$ (siehe Algebra-Skript, Abschnitt endliche Körper) gilt

$$f^p \quad = \quad \left(\sum_{k=0}^{n} a_i x^p \right)^p \quad = \quad \sum_{k=0}^{n} a_i^p x^{ip} \quad = \quad \sum_{k=0}^{n} a_i x^{ip} \quad = \quad f(x^p). \qquad \square$$

Satz 20.7 Für jedes $n \in \mathbb{N}$ ist das Kreisteilungspolynom Φ_n in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel.

Beweis: Wir gehen davon aus, dass $n > 1$ ist, denn für $n = 1$ ist die Aussage offensichtlich. Wäre das Kreisteilungspolynom in $\mathbb{Q}[x]$ reduzibel, dann nach Satz 13.9 (ii) auch in $\mathbb{Z}[x]$. Es gibt dann normierte Polynome $f, g \in \mathbb{Z}[x]$ mit $\Phi_n = f\,g$ und $\text{grad}(f), \text{grad}(g) > 1$, wobei wir voraussetzen, dass f in $\mathbb{Z}[x]$ (und damit auch in $\mathbb{Q}[x]$) irreduzibel ist. Wir zeigen nun:

Ist p eine Primzahl mit $p \nmid n$ und $\zeta \in \mathbb{C}$ eine Nullstelle von f, dann gilt auch $f(\zeta^p) = 0$.

Angenommen, es gilt $f(\zeta^p) \neq 0$. Wegen $\Phi_n(\zeta) = 0$ und $\Phi_n = f\,g$ muss dann $g(\zeta^p) = 0$ gelten. Dies bedeutet, dass ζ eine Nullstelle des Polynoms $g(x^p)$ ist. Weil aber f das Minimalpolynom von ζ ist, teilt f das Polynom $g(x^p)$ in $\mathbb{Q}[x]$. Darüber hinaus ist f normiert, insbesondere primitiv, und nach Satz 13.9 (i) ist f damit auch im Ring $\mathbb{Z}[x]$ ein Teiler von $g(x^p)$.

Seien nun $\bar{f}$, $\bar{g}$ die Bilder von f, g im Polynomring $\mathbb{F}_p[x]$. Dann ist $\bar{f}$ ein Teiler von $\bar{g}(x^p)$, nach Lemma 20.6 also ein Teiler von $\bar{g}^p$. Sei $\bar{f}_1$ ein irreduzibler Teiler von $\bar{f}$. Dann ist $\bar{f}_1$ wegen $\bar{f}\,|\,\bar{g}^p$ auch ein Teiler von $\bar{g}$. Wegen $\Phi_n = f\,g$ und $\Phi_n \mid (x^n - 1)$ ist $\bar{f}\,\bar{g}$ ein Teiler von $x^n - \bar{1}$, und wegen $\bar{f}_1|\bar{f}$ und $\bar{f}_1|\bar{g}$ folgt daraus $\bar{f}_1^2|(x^n - \bar{1})$. Insbesondere hat $x^n - \bar{1}$ im algebraischen Abschluss $\mathbb{F}_p^{\text{alg}}$ von $\mathbb{F}_p$ mehrfache Nullstellen. Andererseits zeigt die Gleichung

$$\text{ggT}(x^n - \bar{1}, (x^n - \bar{1})') \quad = \quad \text{ggT}(x^n - \bar{1}, nx^{n-1}) \quad = \quad \bar{1} \quad ,$$

dass dies *nicht* der Fall ist. Auf Grund dieses Widerspruchs ist die Annahme falsch und die Behauptung bewiesen.

Jede Nullstelle von Φ_n, also jede primitive n-te Einheitswurzel, kann in der Form ζ^m dargestellt werden, wobei $m \in \mathbb{N}$ eine zu n teilerfremde Zahl bezeichnet. Ist $m > 1$, dann ist m ein Produkt $p_1 \cdots p_r$ bestehend aus Primzahlen p_k mit $p_k \nmid n$ für $1 \leq k \leq r$. Durch mehrfache Anwendung der soeben bewiesenen Behauptung erkennt man, dass mit ζ auch die Elemente ζ^{p_1}, $\zeta^{p_1 p_2}$, $\zeta^{p_1 p_2 p_3}$, ..., ζ^m Nullstellen von f sind. Insgesamt sind also alle $\varphi(m)$ verschiedenen Linearfaktoren von Φ_n Teiler von f. Daraus folgt $\Phi_n | f$ und $f = \Phi_n$, insgesamt also die Irreduzibilität von Φ_n. □

Definition 20.8 Sei p eine Primzahl und $a \in \mathbb{Z}$. Man nennt a einen ***quadratischen Rest*** modulo p, wenn eine Zahl $c \in \mathbb{Z}$ mit $a \equiv c^2 \bmod p$ existiert. Andernfalls spricht man von einem ***quadratischen Nichtrest***.

Eine alternative Formulierung lautet: Die Zahl a ist quadratischer Rest modulo p genau dann, wenn das Bild $\bar{a} = a + p\mathbb{Z}$ in $\mathbb{F}_p$ ein Quadrat ist. Anhand dieser Formulierung sieht man, dass die Eigenschaft einer Zahl, quadratischer (Nicht-)Rest zu sein, nur von ihrer Restklasse modulo p abhängt. Für die Formulierung der nachfolgenden Aussagen ist die Einführung der folgenden Notation sinnvoll.

Definition 20.9 Sei p eine ungerade Primzahl und $a \in Z$. Das ***Legendre-Symbol*** modulo p ist definiert durch

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

Man beachte, dass durch p teilbare Zahlen a auf jeden Fall quadratische Reste sind, denn für sie gilt jeweils $a \equiv 0^2 \bmod p$. Für die Primzahl 2 wäre die Definition des Legendre-Symbols zwar auch möglich, aber wenig sinnvoll, denn jede ganze Zahl (gerade oder ungerade) ist auf Grund der Kongruenzen $0^2 \equiv 0 \bmod 2$ und $1^2 \equiv 1 \bmod 2$ ein quadratischer Rest modulo 2.

Lemma 20.10 Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$. Dann gelten für das Legendre-Symbol die folgenden Rechenregeln:

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ *(Eulersches Kriterium)*

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

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

Beweis: zu (i) Im Fall $p \mid a$ ist $\left(\frac{a}{p}\right) = 0$, und aus $a \equiv 0 \bmod p$ folgt $a^{(p-1)/2} \equiv 0 \bmod p$. Andernfalls sei $\bar{a}$ das Bild von a in $\mathbb{F}_p^\times$ und $\bar{c} = \bar{a}^{(p-1)/2}$. Wegen $|\mathbb{F}_p^\times| = p-1$ gilt $\bar{c}^2 = (\bar{a}^{(p-1)/2})^2 = \bar{a}^{p-1} = \bar{1}$. Das Element $\bar{c}$ ist also eine Nullstelle des Polynoms $x^2 - \bar{1} = (x - \bar{1})(x + \bar{1})$, und daraus folgt $\bar{c} \in \{\pm 1\}$. Offenbar gilt $\left(\frac{a}{p}\right) = 1$ genau dann, wenn $\bar{a}$ in $\mathbb{F}_p$ ein Quadrat ist. Wir müssen also zeigen, dass dies genau dann der Fall ist, wenn $\bar{c} = \bar{1}$ gilt.

Ist $\bar{a} = \bar{u}^2$ für ein $\bar{u} \in \mathbb{F}_p$, dann folgt $\bar{c} = \bar{u}^{p-1} = \bar{1}$. Setzen wir nun umgekehrt voraus, das $\bar{a}^{(p-1)/2} = \bar{1}$ gilt. Sei η ein erzeugendes Element von $\mathbb{F}_p^\times$ und $\ell \in \mathbb{Z}$ mit $\bar{a} = \eta^\ell$. Durch Einsetzen erhalten wir $\eta^{\ell(p-1)/2} = \bar{1}$, und weil η von Ordnung $p-1$ ist, folgt daraus $\ell(p-1)/2 = k(p-1)$ für ein $k \in \mathbb{Z}$. Wir erhalten $\ell = 2k$ und $\bar{a} = \eta^{2k}$. Also ist $\bar{a}$ ein Quadrat in $\mathbb{F}_p$.

zu (ii) Aus $a \equiv b \bmod p$ folgt $a^{(p-1)/2} \equiv b^{(p-1)/2} \bmod p$, und somt $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$. Weil die Legendre-Symbole nur die Wert -1, 0 oder 1 annehmen können und $p > 2$ ist, folgt daraus $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

zu (iii) Durch Teil (i) erhalten wir in dieser Situation

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p \quad ,$$

und wiederum folgt aus der Kongruenz modulo p die Gleichheit. □

Satz 20.11 *(Ergänzungssätze zum Quadratischen Reziprozitätsgesetz)*
Für jede ungerade Primzahl p gilt

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

und

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

Beweis: Den zweiten Teil jeder der beiden Gleichungen überprüft man unmittelbar dadurch, dass man die Fälle einzeln durchgeht. Ist $p \equiv 1 \bmod 4$, dann ist $\frac{1}{2}(p-1)$ gerade und folglich $(-1)^{(p-1)/2} = 1$. Ist dagegen $p \equiv 3 \bmod 4$, dann ist $\frac{1}{2}(p-1)$ ungerade, und wir erhalten $(-1)^{(p-1)/2} = -1$. Ist $p \equiv 1 \bmod 8$ oder $p \equiv 7 \bmod 8$, dann ist p modulo 16 kongruent zu einer der Zahlen $-7, -1, 1$ oder 7. In jedem Fall gilt dann $p^2 \equiv 1 \bmod 16$, also ist $\frac{1}{8}(p^2-1)$ gerade und $(-1)^{(p^2-1)/8} = 1$. Ist $p \equiv 3 \bmod 8$ oder $p \equiv 5 \bmod 8$, dann gilt $p \equiv a \bmod 16$ für ein $a \in \{-5, -3, 3, 5\}$ und $p^2 \equiv 9 \bmod 16$. In diesem Fall ist $\frac{1}{8}(p^2-1)$ ungerade und $(-1)^{(p^2-1)/8} = -1$.

Auf Grund der Eulerschen Gleichung gilt $(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \bmod p$. Weil auf beiden Seiten der Kongruenz nur die Werte ± 1 möglich sind und wegen $p > 2$ folgt aus der Kongruenz modulo p Gleichheit. Zum Beweis des ersten Teils der zweiten Gleichung rechnen wir im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen. Weil der Faktorring $\mathbb{Z}[i]/(p)$ ein Ring der Charakteristik p ist, gilt $(\alpha+\beta)^p \equiv \alpha^p + \beta^p \bmod p$. Auf Grund der Eulerschen Gleichung und wegen $2 = (-i)(1+i)^2$ erhalten wir

$$\left(\frac{2}{p}\right) \quad \equiv \quad 2^{(p-1)/2} \quad \equiv \quad (-i)^{(p-1)/2}(1+i)^{p-1} \quad \equiv \quad \frac{(-i)^{(p-1)/2}}{1+i}(1+i)^p \quad \equiv$$

$$\frac{(-i)^{(p-1)/2}(1-i)}{(1+i)(1-i)}(1+i^p) \quad \equiv \quad \left(\tfrac{1}{2}(-i)^{(p-1)/2} + \tfrac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p)$$

Gehen wir nun die einzelnen möglichen Fälle durch. Weil p ungerade ist, gilt $p \equiv 1$, 3, 5 oder 7 modulo 8. Im Fall $p \equiv 1 \bmod 8$ gilt $\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) = (\frac{1}{2} - \frac{1}{2}i)(1+i) = 1$. Im Fall $p \equiv 3 \bmod 8$ ist

$$\left(\tfrac{1}{2}(-i)^{(p-1)/2} + \tfrac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) \quad = \quad (\tfrac{1}{2}(-i) - \tfrac{1}{2})(1-i) \quad = \quad -1.$$

Ist $p \equiv 5 \bmod 8$, dann erhalten wir

$$\left(\tfrac{1}{2}(-i)^{(p-1)/2} + \tfrac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) \quad = \quad (-\tfrac{1}{2} + \tfrac{1}{2}i)(1+i) \quad = \quad -1 \quad ,$$

und im letzten Fall $p \equiv 7 \bmod 8$ gilt $\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) = (\frac{1}{2}i + \frac{1}{2})(1-i) = 1$. Also ist die Kongruenz $(\frac{2}{p}) \equiv (-1)^{(p^2-1)/8} \bmod p$ in jedem der vier Fälle erfüllt. Da auf beiden Seite der Kongruenz nur die Werte ± 1, folgt aus der Kongruenz modulo p wiederum Gleichheit. □

Das entscheidende Hilfsmittel zur Berechnung des Legendre-Symbol ist nun das berühmte, auf C. F. Gauß zurückgehende Gesetz.

Satz 20.12 *(Quadratisches Reziprozitätsgesetz)*

Für zwei beliebige voeinander verschiedene ungerade Primzahlen p, q gilt

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

Der Beweis, den wir weiter unten angeben werden, basiert auf der Darstellung im Lehrbuch [5]. Zuerst aber zeigen wir anhand eines Beispiels, wie das Quadratische Reziprozitätsgesetz zur Berechnung des Legendre-Symbols verwendet werden kann. Die Zahl 5209 ist eine Primzahl. Mit Hilfe der uns zur Verfüg stehenden Rechenregeln erhalten wir

$$\left(\frac{8498}{5209}\right) \overset{(1)}{=} \left(\frac{3289}{5209}\right) \overset{(2)}{=} \left(\frac{11\cdot 13\cdot 13}{5209}\right) \overset{(3)}{=} \left(\frac{11}{5209}\right)\left(\frac{13}{5209}\right)\left(\frac{23}{5209}\right) \overset{(4)}{=}$$

$$\left(\frac{5209}{11}\right)\left(\frac{5209}{13}\right)\left(\frac{5209}{23}\right) \overset{(5)}{=} \left(\frac{6}{11}\right)\left(\frac{9}{13}\right)\left(\frac{11}{23}\right) \overset{(6)}{=} \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)\left(\frac{3}{13}\right)^2\left(\frac{11}{23}\right) \overset{(7)}{=}$$

$$(-1)\cdot\left(\frac{3}{11}\right)\cdot 1\cdot\left(\frac{11}{23}\right) \overset{(8)}{=} -\left(\frac{3}{11}\right)\left(\frac{11}{23}\right) \overset{(9)}{=} -(-1)\left(\frac{11}{3}\right)\cdot(-1)\left(\frac{23}{11}\right)$$

$$\overset{(10)}{=} -\left(\frac{2}{3}\right)\left(\frac{1}{11}\right) \overset{(11)}{=} -\left(\frac{2}{3}\right) \overset{(12)}{=} -(-1) \quad = \quad 1.$$

Dabei kommt die Gleichung (1) durch $8498 \equiv 3289 \bmod 5209$ zu Stande. In Schritt (4) wird zum ersten Mal das Quadratische Reziprozitätsgesetz angewendet, und zwar auf jeden der drei Faktoren. Wegen $5209 \equiv 1 \bmod 4$ kommt es dabei zu keinem Vorzeichenwechsel. Gleichung (5) ist wegen $5209 \equiv 6 \bmod 11$, $5209 \equiv 9 \bmod 13$ und $5209 \equiv 11 \bmod 23$ erfüllt. In Schritt (7) wurde auf den ersten Faktor der Zweite Ergänzungssatz angewendet; wegen $11 \equiv 3 \bmod 8$ gilt $\left(\frac{2}{11}\right) = -1$. Außerdem ist zu beachten, dass das Legendre-Symbol $\left(\frac{3}{13}\right)$ wegen $13 \nmid 3$ gleich 1 oder -1, das Quadrat also gleich 1 ist. In Schritt (9) wird noch das Quadratische Reziprozitätsgesetz angewendet, auf beide Faktoren. Wegen $3 \equiv 3 \bmod 4$, $11 \equiv 3 \bmod 4$ und $23 \equiv 3 \bmod 4$ entsteht dabei jeweils ein Vorzeichenwechsel. Gleichung (10) gilt wegen $11 \equiv 2 \bmod 3$ und $23 \equiv 1 \bmod 11$. Schließlich wird Schritt (12) noch einmal der Zweite Ergänzungssatz angewendet. Insgesamt ergibt unsere Rechnung, dass 8498 ein quadratischer Rest modulo der Primzahl 5209 ist. Durch aufwändiges Probieren findet man tatsächlich die Kongruenz $8498 \equiv 2046^2 \bmod 5209$.

Man beachte, dass die erste Anwendung des Quadratischen Reziprozitätsgesetzes unter (4) nur möglich war, weil wir zuvor die Zahl 3289 in das Produkt $11\cdot 13\cdot 23$ von Primzahlen zerlegt haben. Die Berechnung einer solchen Primfaktorzerlegung ist natürlich bei großen Zahlen sehr aufwändig (sogar so aufwändig, dass unter anderem die Sicherheit der RSA-Verschlüsselung darauf beruht). Um das Quadratische Reziprozitätsgesetz in dieser Hinsicht praktikabler zu machen, werden wir es später durch das Jacobi-Symbol verallgemeinern.

Wir werden nun einen Beweis für das Quadratische Reziprozitätsgesetz entwickeln, der auf dem Rechnen mit Einheitswurzeln basiert. Für jede ungerade Primzahl p sei $\zeta_p = e^{2\pi i/p}$. Wir erinnern daran, dass die Nullstellen des Kreisteilungspolynoms Φ_p durch ζ_p^m gegeben sind, wobei m die ganzen Zahlen mit $1 \leq m \leq p-1$ durchläuft.

Lemma 20.13 [20.13] Seien p und q zwei verschiedene ungerade Primzahlen. Weiter sei

$$\zeta_p = e^{2\pi i/p} \in \mathbb{C}^\times \quad , \quad R = \mathbb{Z}[\zeta_p] \quad \text{und} \quad (q) = qR\,,$$

das von q in R erzeugte Hauptideal. Dann gilt $(q) \cap \mathbb{Z} = q\mathbb{Z}$ und

$$R \quad = \quad \{a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2} \mid a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}\}.$$

Beweis: Die Gleichung für R zeigen wir ähnlich wie in den Beispielen aus § 9. Sei $S \subseteq \mathbb{C}$ die Teilmenge auf der rechten Seite der Gleichung. Zunächst überprüfen wir, dass es sich dabei um einen Teilring von $\mathbb{C}$ handelt. Offenbar gilt $1 \in S$ (setze $a_0 = 1$ und $a_j = 0$ für $1 \leq j \leq p-2$), und auch dass für vorgegebene $\alpha, \beta \in S$ jeweils auch $\alpha - \beta \in S$ liegt, ist offensichtlich. Um zu zeigen, dass auch $\alpha\beta$ in S liegt, bemerken wir zunächst, dass das Produkt die Form $\sum_{j=0}^{2p-4} u_j\zeta_p^j$ besitzt, mit $u_0, \ldots, u_{2p-4} \in \mathbb{Z}$. Es genügt damit zu überprüfen, dass die Potenzen ζ_p^j für $0 \leq j \leq 2p-4$ in S liegen. Weil es keinen zusätzlichen Aufwand bereitet, zeigen wir die Aussage $\zeta_p^j \in S$ für alle $j \in \mathbb{N}_0$, durch vollständige Induktion über j. Für $j \leq p-2$ ist die Aussage auf Grund der Definition von S erfüllt. Sei nun $j > p-2$, und setzten wir die Aussage für kleinere Werte von j voraus. Weil ζ_p eine Nullstelle des p-ten Kreisteilungspolynoms Φ_p ist, gilt

$$\zeta_p^j \quad = \quad \zeta_p^{j-p+1} \cdot \zeta_p^{p-1} \quad = \quad \zeta_p^{j-p+1} \cdot \left(\sum_{k=0}^{p-2} (-\zeta_p^k) \right) \quad = \quad \sum_{k=0}^{p-2} (-\zeta_p^{j-p+k+1}).$$

Die Aussage $\zeta_p^j \in S$ folgt nun durch Anwendung der Induktionsvoraussetzung und der Tatsache, dass S abgeschlossen unter Addition und Subtraktion ist. Damit ist die Teilring-Eigenschaft nachgewiesen. Offenbar gilt auch $\mathbb{Z} \cup \{\zeta_p\} \subseteq S$. Ist nun R' ein beliebiger Teilring von $\mathbb{C}$ mit $R' \supseteq \mathbb{Z} \cup \{\zeta_p\}$, dann folgt unmittelbar aus der Abgeschlossenheit von R' unter Addition und Multiplikation, dass jedes Element aus S in R' enthalten ist.

Kommen wir nun zum Beweis der Gleichung $(q) \cap \mathbb{Z} = q\mathbb{Z}$. Die Inklusion „$\supseteq$“ ist offensichtlich, weil $q\mathbb{Z}$ sowohl in $(q) = qR$ als auch in $\mathbb{Z}$ enthalten ist. Zum Nachweis von „$\subseteq$“ sei $a \in (q) \cap \mathbb{Z}$ vorgegeben. Dann existiert ein $\alpha \in R$ mit $a = q\alpha$. Das Element α kann in der Form $\alpha = \sum_{j=0}^{p-2} a_j\zeta_p^j$ mit $a_0, \ldots, a_{p-2} \in \mathbb{Z}$ dargestellt werden. Durch Einsetzen erhalten wir die Gleichung

$$a \cdot 1 \quad = \quad q\alpha \quad = \quad \sum_{j=0}^{p-2} q a_j \cdot \zeta_p^j.$$

Weil $\Phi_p \in \mathbb{Z}[x]$ auf Grund der Irreduzibilität das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist, handelt es sich bei $\{\zeta_p^j \mid 0 \leq j \leq p-1\}$ nach § 15 um eine Basis von $\mathbb{Q}(\zeta_p^j)$ als $\mathbb{Q}$-Vektorraum. Jedes Element aus diesem Körper kann also auf *eindeutige* Weise als Linearkombination dieser Menge dargestellt werden. Daraus folgt $qa_0 = a$ und $a_j = 0$ für $1 \leq j \leq p-2$. Damit ist $a \in q\mathbb{Z}$ nachgewiesen. □

Definition 20.14 Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist die ***Gaußsche Summe*** $g_{a,p} \in \mathbb{Z}[\zeta_p]$ gegeben durch

$$g_{a,p} \quad = \quad \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{na}.$$

Für jede ungerade Primzahl p setzen wir $p^* = p$, falls $p \equiv 1 \bmod 4$ und $p^* = -p$, falls $p \equiv 3 \bmod 4$ ist. Offenbar gilt $p^* = (-1)^{(p-1)/2} p$, was auf Grund des ersten Ergänzungssatzes 20.11 auch in der Form $p^* = (\frac{-1}{p})p$ geschrieben werden kann.

Lemma 20.15 Für die Gaußschen Summen gelten die folgenden Rechenregeln. Es seien p, q zwei verschiedene ungerade Primzahlen und $a \in \mathbb{Z}$ mit $p \nmid a$.

$$\text{(i)} \;\; g_{a,p} = \left(\frac{a}{p}\right) g_{1,p} \qquad \text{(ii)} \;\; g_{1,p}^2 = \left(\frac{-1}{p}\right) p = p^* \qquad \text{(iii)} \;\; g_{1,p}^q \equiv g_{q,p} \bmod (q)$$

wobei unter (iii) die Kongruenz im Ring $\mathbb{Z}[\zeta_p]$ gemeint ist.

Beweis: zu (i) Wegen $p \nmid a$ durchläuft mit n auch na die Restklassen in $\mathbb{Z}/p\mathbb{Z}$ ungleich $\bar{0}$, und ζ_p^{na} durchläuft die von 1 verschiedenen ganzzahligen Potenzen von ζ_p. Damit erhalten wir

$$\left(\frac{a}{p}\right) g_{a,p} \quad = \quad \sum_{n=1}^{p-1} \left(\frac{a}{p}\right)\left(\frac{n}{p}\right) \zeta_p^{na} \quad = \quad \sum_{n=1}^{p-1} \left(\frac{na}{p}\right) \zeta_p^{na} \quad = \quad \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{n} \quad = \quad g_{1,p}.$$

Wegen $(\frac{a}{p}) \in \{\pm 1\}$ folgt daraus $g_{a,p} = (\frac{a}{p}) g_{1,p}$.

zu (ii) Dasselbe Argument wie unter (i) erlaubt es im dritten Schritt der folgenden Rechnung in der zweiten Summe n durch mn zu ersetzen. Damit erhalten wir

$$\begin{aligned} g_{1,p}^2 \quad &= \quad \left(\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m\right)\left(\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n\right) \quad = \quad \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n \quad = \quad \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta_p^m \sum_{n=1}^{p-1} \left(\frac{mn}{p}\right) \zeta_p^{mn} \\ &= \quad \sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \left(\frac{m^2 n}{p}\right) \zeta_p^{m+mn} \quad = \quad \sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{m(1+n)} \quad = \quad \sum_{n=1}^{p-1}\sum_{m=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{m(1+n)} \quad = \quad \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \sum_{m=1}^{p-1} \zeta_p^{m(1+n)} \\ &= \quad \sum_{n=1}^{p-2} \left(\frac{n}{p}\right) \sum_{m=1}^{p-1} \zeta_p^{m(1+n)} + \left(\frac{p-1}{p}\right) \sum_{m=1}^{p-1} \zeta_p^{mp} \quad \overset{(*)}{=} \quad \sum_{n=1}^{p-2} \left(\frac{n}{p}\right)(-1) + \left(\frac{-1}{p}\right)(p-1). \end{aligned}$$

Dabei wurde an der Stelle (*) verwendet, dass wegen $p \nmid (n+1)$ mit ζ_p^m auch $\zeta_p^{m(1+n)}$ alle von 1 verschiedenen Potenzen von ζ_p durchläuft, und dass sich diese Potenzen zu -1 addieren.

Im Beweis von 20.10 haben wir festgestellt: Ist c eine Primitivwurzel mod p, dann sind die verschiedenen quadratischen Reste modulo p ungleich 0 gegeben durch c^{2k} mit $0 \le k < \frac{1}{2}(p-1)$, und die quadratischen Nichtreste durch c^{2k+1} mit $0 \le k < \frac{1}{2}(p-1)$. Für $1 \le n \le p-1$ nimmt das Legendre-Symbol $(\frac{n}{p})$ deshalb $\frac{1}{2}(p-1)$-mal den Wert 1 und

genauso oft den Wert -1 an. Daraus folgt $\sum_{n=1}^{p-1}(\frac{n}{p}) = 0$ und $\sum_{n=1}^{p-2}(\frac{n}{p})(-1) = (\frac{p-1}{p}) = (\frac{-1}{p})$. Setzen wir dies in das Ergebnis unserer Rechnung ein, so erhalten wir $g_{1,p}^2 = (\frac{-1}{p})p = p^*$ wie gewünscht.

zu (iii) Weil $\mathbb{Z}[\zeta_p]/(q)$ ein Ring der Charakteristik q ist, gilt $(\alpha+\beta)^q \equiv \alpha^q + \beta^q \bmod (q)$, und dieselbe Kongruenz gilt auch für eine beliebig große endliche Anzahl von Summanden. (Diese Rechenregel haben wir in der Körpertheorie unter dem Namen „Freshman's Dream" kennengelernt.) Damit erhalten wir

$$g_{1,p}^q \equiv \left(\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta_p^n\right)^q \equiv \sum_{n=1}^{p-1}\left(\left(\frac{n}{p}\right)\zeta_p^n\right)^q \equiv \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)^q\zeta_p^{nq} \equiv \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta_p^{nq} \equiv g_{q,p} \bmod (q). \quad \square$$

Mit Hilfe dieser Lemmata können wir nun das Quadratische Reziprozitätsgesetz erneut beweisen. Seien p, q ungerade Primzahlen. Durch aufeinanderfolgende Anwendung der Rechenregeln (i) und (iii) und mit dem Eulerschen Kriterium **??** erhalten wir zunächst die Kongruenz

$$\left(\frac{q}{p}\right)g_{1,p} \equiv g_{q,p} \equiv g_{1,p}^q \equiv g_{1,p}\cdot(g_{1,p}^2)^{(q-1)/2} \equiv g_{1,p}\cdot(p^*)^{(q-1)/2} \equiv g_{1,p}\left(\frac{p^*}{q}\right) \bmod (q).$$

Multiplizieren wir diese Kongruenz mit $g_{1,p}$, so erhalten wir mit Regel (ii)

$$\left(\frac{q}{p}\right)p^* \equiv \left(\frac{q}{p}\right)g_{1,p}^2 \equiv \left(\frac{p^*}{q}\right)g_{1,p}^2 \equiv \left(\frac{p^*}{q}\right)p^* \bmod (q).$$

Weil q und p^* teilerfremd sind, gibt es nach dem Lemma von Bézout Zahlen $k, \ell \in \mathbb{Z}$ mit $kq + \ell p^* = 1$. Multiplizieren wir die soeben erhaltene Kongruenz mit ℓ, so kürzt sich der Faktor p^* wegen $\ell p^* \equiv 1 \bmod (q)$ weg, und wir erhalten $(\frac{q}{p}) \equiv (\frac{p^*}{q}) \bmod (q)$.

Wir bemerken jetzt, dass damit auch die Kongruenz $(\frac{q}{p}) \equiv (\frac{p^*}{q}) \bmod q$ im Ring $\mathbb{Z}$ gilt. Denn die Kongruenz beider Seiten modulo (q) im $\mathbb{Z}[\zeta_p]$ bedeutet, dass die Differenz beider Seiten im Hauptideal (q) enthalten ist. Damit liegt die Differenz auch in $(q) \cap \mathbb{Z}$, denn die Legendre-Symbole sind ganze Zahlen. Dieser Durchschnitt stimmt mit dem Hauptideal $q\mathbb{Z}$ in $\mathbb{Z}$ überein: Die Inklusion $q\mathbb{Z} \subseteq (q) \cap \mathbb{Z}$ ist unmittelbar klar. Setzen wir umgekehrt $\alpha \in (q) \cap \mathbb{Z}$ voraus. Weil Φ_p das Minimalpolynom von ζ_p ist, wissen wir aus der Körpertheorie, dass unser α wie jedes Element aus $\mathbb{Q}(\zeta_p)$ eine eindeutige Darstellung der Form $a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}$ mit $a_0, \ldots, a_{p-2} \in \mathbb{Q}$ besitzt. Aus $\alpha \in (q)$ und **??** folgt $a_k \in \mathbb{Z}$ und $q \mid a_k$ für $0 \le k \le p-2$. Wegen $\alpha \in \mathbb{Z}$ gilt außerdem $a_1 = \ldots = a_{p-2} = 0$. Ingesamt ist damit $\alpha = a_0 \in q\mathbb{Z}$ nachgewiesen.

Mit Hilfe der Kongruenz $(\frac{q}{p}) \equiv (\frac{p^*}{q}) \bmod q$ in $\mathbb{Z}$ erhalten wir nun das Quadratische Reziprozitätsgesetz. Es gilt

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

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

Weil auf beiden Seiten jeweils eine Zahl der Menge $\{\pm 1\}$ steht und $-1 \not\equiv 1 \bmod q$ gilt, folgt aus der Kongruenz der beiden Seiten die Gleichheit.

Wie oben bereits angekündigt, behandeln wir nun noch eine leichte Verallgemeinerung des Quadratischen Reziprozitätsgesetzes, bei dem die Zerlegung in Primfaktoren vor jeder Anwendung entfällt.

Definition 20.16 Sei $n \in \mathbb{N}$ ungerade und $n = p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von n, wobei wir auch das mehrfache Auftreten derselben Primzahl zulassen (und die Anzahl r der Faktoren im Fall $n = 1$ gleich Null ist). Sei $a \in \mathbb{Z}$. Dann ist das ***Jacobi-Symbol*** von a modulo n definiert durch

$$\left(\frac{a}{n}\right) \quad = \quad \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right)$$

Unmittelbar aus der Definition folgt $(\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})$ für alle $a \in \mathbb{Z}$ und ungerade $m, n \in \mathbb{N}$. Aus 20.10 kann leicht $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$ für alle $a, b \in \mathbb{Z}$ und ungerades $n \in \mathbb{N}$ abgeleitet werden, und $(\frac{a}{n}) = (\frac{b}{n})$ falls $a \equiv b \bmod n$. Ist nämlich $n = p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von n, dann gilt

$$\left(\frac{ab}{n}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{ab}{p_i}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{a}{p_i}\right)\prod_{i=1}^{r}\left(\frac{b}{p_i}\right) \quad = \quad \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Aus $a \equiv b \bmod n$ folgt $a \equiv b \bmod p_i$ für $1 \le i \le r$ und somit

$$\left(\frac{a}{n}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{a}{p_i}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{b}{p_i}\right) \quad = \quad \left(\frac{b}{n}\right).$$

Darüber hinaus gilt

Satz 20.17 Der Erste und Zweite Ergänzungssatz sowie das Quadratische Reziprozitätsgesetz gelten unverändert auch für das Jacobi-Symbol.

Beweis: Da das Jacobi-Symbol, wie wir bereits festgestellt haben, in der unteren Komponente multiplikativ ist, müssen wir zeigen, dass sich auch die „rechten Seiten“ unserer drei Rechenregeln multiplikativ verhalten. Wir beweisen für alle ungeraden $m_1, m_2, n_1, n_2 \in \mathbb{N}$ die Gleichungen

$$(-1)^{\frac{n_1-1}{2}} \cdot (-1)^{\frac{n_2-1}{2}} = (-1)^{\frac{n_1 n_2 - 1}{2}} \qquad , \qquad (-1)^{\frac{n_1^2-1}{8}} \cdot (-1)^{\frac{n_2^2-1}{8}} = (-1)^{\frac{(n_1 n_2)^2-1}{8}}$$

und

$$(-1)^{\frac{m_1-1}{2}\cdot\frac{n_1-1}{2}} \cdot (-1)^{\frac{m_2-1}{2}\cdot\frac{n_1-1}{2}} \quad = \quad (-1)^{\frac{m_1 m_2-1}{2}\cdot\frac{n_1-1}{2}} \quad , \quad (-1)^{\frac{m_1-1}{2}\cdot\frac{n_1-1}{2}} \cdot (-1)^{\frac{m_1-1}{2}\cdot\frac{n_2-1}{2}} \quad = \quad (-1)^{\frac{m_1-1}{2}\cdot\frac{n_1 n_2-1}{2}}.$$

Die erste Gleichung ist äquivalent zu $(-1)^{\frac{n_1-1}{2}+\frac{n_2-1}{2}} = (-1)^{\frac{n_1 n_2-1}{2}}$. Weil allgemein $(-1)^a$ für $a \in \mathbb{Z}$ nur von der Restklasse von a modulo 2 abhängt, ist dies wiederum äquivalent zu

$$\frac{n_1-1}{2} + \frac{n_2-1}{2} \equiv \frac{n_1 n_2 - 1}{2} \bmod 2 \quad \Leftrightarrow \quad (n_1-1)+(n_2-1) \equiv n_1 n_2 - 1 \bmod 4 \quad \Leftrightarrow$$
$$n_1 n_2 - n_1 - n_2 + 1 \equiv 0 \bmod 4 \quad \Leftrightarrow \quad (n_1-1)(n_2-1) \equiv 0 \bmod 4.$$

Die letzte Äquivalenz ist offenbar erfüllt, weil die Faktoren n_1-1 und n_2-1 beide durch 2 teilbar sind. Entsprechend beweist man die zweite Gleichung durch die Äquivalenzumformung

$$(-1)^{\frac{n_1^2-1}{8}}\cdot(-1)^{\frac{n_2^2-1}{8}}=(-1)^{\frac{(n_1n_2)^2-1}{8}} \quad\Leftrightarrow\quad \tfrac{1}{8}(n_1^2-1)+\tfrac{1}{8}(n_2^2-1)\equiv\tfrac{1}{8}((n_1n_2)^2-1) \bmod 2 \quad\Leftrightarrow$$

$$(n_1^2-1)+(n_2^2-1)\equiv(n_1n_2)^2-1 \bmod 16 \quad\Leftrightarrow\quad (n_1n_2)^2-n_1^2-n_2^2+1\equiv 0 \bmod 16 \quad\Leftrightarrow$$

$$(n_1^2-1)(n_2^2-1)\equiv 0 \bmod 16 \quad\Leftrightarrow\quad (n_1-1)(n_1+1)(n_2-1)(n_2+1)\equiv 0 \bmod 16.$$

Wieder sind alle vier Faktoren durch 2 teilbar und die letzte Kongrenz somit erfüllt. Die dritte Gleichung folgt aus der ersten durch die Rechnung

$$(-1)^{\frac{m_1-1}{2}\cdot\frac{n_1-1}{2}}\cdot(-1)^{\frac{m_2-1}{2}\cdot\frac{n_1-1}{2}} = \left((-1)^{\frac{m_1-1}{2}}\cdot(-1)^{\frac{m_2-1}{2}}\right)^{\frac{n_1-1}{2}} = ((-1)^{\frac{m_1m_2-1}{2}})^{\frac{n_1-1}{2}} = (-1)^{\frac{m_1m_2-1}{2}\cdot\frac{n_1-1}{2}}.$$

Der Beweis der vierten Gleichung verläuft weitgehend analog. Seien nun ungerade natürliche Zahlen $m,n\in\mathbb{N}$ vorgegeben, mit zugehörigen Primfaktorzerlegungen $m=p_1\cdot\ldots\cdot p_r$ und $n=q_1\cdot\ldots\cdot q_s$. Den Ersten Ergänzungssatz erhält man nun mit Hilfe der ersten Gleichung von oben durch die Rechnung

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i-1)/2} = (-1)^{(p_1\cdot\ldots\cdot p_r-1)/2} = (-1)^{(m-1)/2},$$

den Zweiten Ergänzungssatz mit der zweiten Gleichung durch

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{r}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i^2-1)/8} = (-1)^{(p_1^2\cdot\ldots\cdot p_r^2-1)/8} = (-1)^{(m^2-1)/8}$$

und das Quadratische Reziprozitätsgesetz für das Jacobi-Symbol schließlich unter Verwendung der dritten und vierten Gleichung durch

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\left(\frac{p_i}{n}\right)\left(\frac{n}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$$

$$= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}} = \prod_{j=1}^{s}(-1)^{\frac{p_1\cdot\ldots\cdot p_r-1}{2}\cdot\frac{q_j-1}{2}} = (-1)^{\frac{p_1\cdot\ldots\cdot p_r-1}{2}\cdot\frac{q_1\cdot\ldots\cdot q_s-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}. \qquad \square$$

Man beachte, dass am Jacobi-Symbol $\left(\frac{a}{n}\right)$, im Gegensatz zum Legendre-Symbol, *nicht* abgelesen werden kann, ob a ein quadratischer Rest modulo n ist. Beispielsweise ist 2 kein quadratischer Rest modulo 15, denn wäre dies der Fall, dann müsste 2 sowohl ein quadratischer Rest modulo 3 als auch ein quadratischer Rest modulo 5 sein. Ist nämlich $2\equiv c^2 \bmod 15$ für ein $c\in\mathbb{Z}$ erfüllt, dann folgt daraus auch $2\equiv c^2 \bmod 3$ und $2\equiv c^2 \bmod 5$. Aber wie man durch Ausprobieren leicht überprüft, ist 2 weder modulo 3 noch modulo 5 ein quadratischer Rest, also erst recht kein quadratischer Rest moduldo 15. Andererseits gilt

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

Das Jacobi-Symbol ermöglicht aber eine effizientere Berechnung von Legendre-Symbolen, weil es vor der Anwendung des Reziprozitätsgesetzes nicht mehr nötig ist, die obere Zahl in ihre Primfaktoren zu zerlegen. So vereinfacht sich zum Beispiel die Rechnung von oben zu

$$\left(\frac{8498}{5209}\right) = \left(\frac{3289}{5209}\right) = \left(\frac{5209}{3289}\right) = \left(\frac{1920}{3289}\right) = \left(\frac{2^7\cdot 15}{3289}\right) = \left(\frac{2}{3289}\right)^7\left(\frac{15}{3289}\right)$$

$$= 1^7\cdot\left(\frac{15}{3289}\right) = \left(\frac{3289}{15}\right) = \left(\frac{4}{15}\right) = \left(\frac{2}{15}\right)^2 = 1.$$

Literaturverzeichnis

[1] Michael Artin. *Algebra - Aus dem Englischen übersetzt von Annette A'Campo*. Basel: Birkhäuser Basel, 1998.

[2] Janko Böhm. *Grundlagen der Algebra und Zahlentheorie* -. Berlin Heidelberg New York: Springer-Verlag, 2016.

[3] Siegfried Bosch. *Algebra* -. Berlin, Heidelberg, New York: Springer Berlin, 2023.

[4] Falko Lorenz und Franz Lemmermeyer. *Algebra 1 - Körper und Galoistheorie*. Heidelberg: Spektrum Akademischer Verlag, 2007.

[5] Stefan Müller-Stach und Jens Piontkowski. *Elementare und algebraische Zahlentheorie - Ein moderner Zugang zu klassischen Themen*. Berlin Heidelberg New York: Springer-Verlag, 2011.