Ralf Gerkmann

Mathematisches Institut
Ludwig-Maximilians-Universität München

Vorlesung im Wintersemester 2022-23

Algebra

Zusammenfassung

In der Algebra-Vorlesung behandeln wir die Gruppen- und die Körpertheorie. während eine weitere wichtige algebraische Struktur, die Ringe, der Zahlentheorie-Vorlesung vorbehalten bleibt. Nach der Wiederholung der wichtigsten Grundbegriffe behandeln wir zunächst Gruppen mit einer besonders leicht verständlichen Struktur, die zyklischen Gruppen. Dagegen können wir die Klassifikation der endlich abelschen Gruppen erst in Angriff nehmen, nachdem wir mit dem Satz von Lagrange und dem Konzept der Faktorgruppe die Voraussetzungen dafür geschaffen haben. Ein wichtiges Konzept in der Gruppentheorie ist der Begriff der Operation, der einerseits dazu beiträgt, Gruppen mit einer anschaulich-geometrische Interpretation zu versehen, und andererseits auch für die Theorie wichtige Anwendungen nach sich zieht, wie beispielsweise die Auflösbarkeit der p-Gruppen und der Sylowsätze.

In der Körpertheorie steht der Begriff der algebraischen Körpererweiterung im Mittelpunkt. Ein wichtiges Hilfsmittel bei der Untersuchung solcher Erweiterungen ist der Erweiterungsgrad, von dem wir an vielen Stellen Gebrauch machen werden. Der Begriff des Zerfällungskörpers ist eine wichtige Voraussetzung sowohl für die Klassifikation der endlichen Körper, ein wichtiges Etappenziel der zweiten Vorlesungshälfte, als auch für die Galoistheorie, die am Ende der Vorlesungen die Gruppen- und Körpertheorie miteinander verbindet.

Inhaltsverzeichnis

§ 1. *Die Kategorie der Gruppen*

Zusammenfassung. Eine *Halbgruppe* ist eine Menge mit einer assoziativen Verknüpfung. Existiert in einer Halbgruppe ein Neutralelement, so spricht man von einem *Monoid*. Besitzt darüber hinaus jedes Element ein Inverses, dann liegt eine *Gruppe* vor. Neben diesen Strukturen Halbgruppe, Monoid und Gruppe definieren wir auch die zugehörigen strukturerhaltenden Abbildungen; diese bezeichnet man als *Homomorphismen*. Viele einfache Beispiele für Halbgruppen, Monoide und Gruppen erhält man durch Betrachtung von Addition und Multiplikation auf den Zahlbereichen $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$. Schränkt man die Verknüpfung eines Monoids auf die invertierbaren Elemente ein, so erhält man eine Gruppe. Aus zwei Gruppen G und H kann eine neue Gruppe konstruiert werden, das *direkte Produkt* $G \times H$.

Wichtige Grundbegriffe

- Halbgruppen, Monoide und Gruppen
- Homomorphismen von Halbgruppen, Monoiden und Gruppen; Mono-, Epi-, Iso-, Endo- und Automorphismen
- n-te Potenz eines Halbgruppen- (bzw. Monoid-, Gruppen-)elements
- Abgeschlossenheit einer Teilmenge einer Gruppe
- Permutationsgruppe, symmetrische Gruppe
- Automorphismengruppe $\mathrm{Aut}(G)$ einer Gruppe G
- (äußeres) direktes Produkt $G \times H$ zweier Gruppen G, H

In der Mathematik trifft man eine Vielzahl algebraischer Strukturen an, zum Beispiel Gruppen, Ringe, Körper, Vektorräume, Moduln, Algebren, Lie-Algebren, topologische Räume, Garben, Schemata, Motive und viele weitere. Um etwas Ordnung in diese Vielzahl von Strukturen zu bringen, wurde der Begriff der ***Kategorie*** eingeführt. Die sog. ***Objekte*** einer Kategorie sind algebraische Strukturen eines bestimmten Typs, beispielsweise die Klasse aller $\mathbb{R}$-Vektorräume. Neben den Objekten besitzt jede Kategorie sog. ***Morphismen***, durch die Beziehungen zwischen den Objekten hergestellt werden. Oft handelt es sich bei den Objekten um Mengen mit einer Zusatzstruktur; dies kann zum Beispiel eine Verknüpfung auf der Menge sein. Die Morphismen sind dann in der Regel Abbildungen, die diese Zusatzstruktur respektieren (indem sie zum Beispiel „verträglich“ mit der Verknüpufung sind). Man spricht in diesem Fall häufig auch von ***Homomorphismen***.

In der Kategorie der $\mathbb{R}$-Vektorräume ist jedes Objekt durch eine Menge V gegeben, für die zusätzlich eine Verknüpfung auf V (die Vektoraddition) und eine Abbildung $\mathbb{R} \times V \to V$ (die skalare Multiplikation) definiert sind. Sind nun V, W zwei Objekte, dann sind die Morphismen zwischen V und W genau diejenigen Abbildungen $V \to W$, die diese Zusatzstruktur respektieren, also verträglich mit der Vektoraddition und der skalaren Multiplikation sind. In der Vorlesung des zweiten Semesters haben wir solche Abbilungen unter der Bezeichnung „lineare Abbildung“ eingeführt.

In diesem Kapitel führen wir nun die Kategorien der Halbgruppen, der Monoide und der Gruppen ein. Bekanntlich ist eine ***Verknüpfung*** auf einer Menge X eine Abbildung $* : X \times X \to X$. Wir erinnern daran, dass eine solche Verknüpfung als ***assoziativ*** bezeichnet wird, wenn $(a * b) * c = a * (b * c)$ für alle $a, b, c \in X$ erfüllt ist, und als ***kommutativ*** oder ***abelsch***, wenn $a * b = b * a$ für alle $a, b \in X$ gilt. Die Kategorie der Halbgruppen ist nun wie folgt definiert.

Definition 1.1 Eine ***Halbgruppe*** ist ein Paar $(G, *)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $*$ auf G. Sei $(H, \circ)$ eine weitere Halbgruppe. Dann bezeichnet man eine Abbildung $\phi : G \to H$ mit der Eigenschaft $\phi(g * h) = \phi(g) \circ \phi(h)$ für alle $g, h \in G$ als ***Halbgruppen-Homomorphismus***.

Die einzige Zusatzstruktur, die Halbgruppen gegenüber den „nackten“ Mengen besitzen, ist also eine assoziative Verknüpfung. Monoide und Gruppen besitzen demgegenüber bereits eine komplexere Zusatzstruktur. Deren Einführung soll im Folgenden vorbereitet werden.

Definition 1.2 Sei $(G, *)$ eine Halbgruppe. Ein Element $e \in G$ mit der Eigenschaft, dass $a * e = e * a = a$ für alle $a \in G$ erfüllt ist, bezeichnet man als ***Neutralelement*** von $(G, *)$.

Wir notieren folgende einfache Beobachtung.

Proposition 1.3 Jede Halbgruppe besitzt höchstens ein Neutralelement.

Beweis: Sei $(G, *,)$ 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 $e' = e' * e = e$. □

Wir können nun die Kategorie der Monoide einführen.

Definition 1.4

(i) Eine Halbgruppe $(G, *)$ wird ***Monoid*** genannt, wenn sie mindestens ein Neutralelement besitzt. Nach Proposition 1.3 ist dieses Element dann eindeutig bestimmt; wir bezeichnen es mit e_G.

(ii) Sind $(G, *)$ und $(H, \circ)$ Monoide, so bezeichnet man eine Abbildung $\phi : G \to H$ als ***Monoid-Homomorphismus*** von $(G, *)$ nach $(H, \circ)$, wenn ϕ ein Halbgruppen-Homomorphismus ist und außerdem $\phi(e_G) = e_H$ gilt.

Wenden wir uns nun der Kategorie der Gruppen zu und definieren zur Vorbereitung.

Definition 1.5 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 1.6 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 von $(G, *)$ 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 $e_G * e_G = e_G$. □

Definition 1.7

(i) Ein Monoid $(G, *)$, in dem jedes Element ein Inverses besitzt, wird ***Gruppe*** genannt.

(ii) Eine Gruppe G, und ebenso eine Halbgruppe bzw. ein Monoid, wird als ***kommutativ*** oder ***abelsch*** bezeichnet, wenn die Verknüpfung $*$ kommutativ ist, also $g * h = h * g$ für alle $g, h \in G$ erfüllt ist.

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

Man beachte, dass man bei der Definition des Gruppen-Homomorphismus ϕ in nicht zu fordern braucht, dass Neutralelemente und Inverse unter ϕ erhalten bleiben, wie man es in Analogie zu Definition 1.4 (ii) vielleicht erwarten würde.

Lemma 1.8 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 $\phi(g^{-1}) = \phi(g)^{-1}$. □

Wir betrachten nun einige konkrete Beispiele für Halbgruppen, Monoide und Gruppen.

(i) Das Paar $(\mathbb{N}, +)$ ist eine Halbgruppe, $(\mathbb{N}, \cdot)$ sogar ein Monoid, mit 1 als Neutralelement.

(ii) Auch $(\mathbb{N}_0, +)$ ist ein Monoid (mit Neutralelement 0), ebenso wie $(\mathbb{N}_0, \cdot)$ (mit Neutralelement 1).

(iii) Das Paar $(\mathbb{Z}, +)$ ist eine Gruppe, $(\mathbb{Z}, \cdot)$ lediglich ein Monoid.

(iv) Auch bei $(\mathbb{Q}, +)$ handelt es sich um eine Gruppe, während $(\mathbb{Q}, \cdot)$ lediglich ein Monoid ist. Eine Gruppe erhält man, wenn man die 0 aus $\mathbb{Q}$ entfernt, d.h. das Paar $(\mathbb{Q}^\times, \cdot)$ mit $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ ist eine Gruppe.

(v) Bezeichnet K einen Körper und V einen K-Vektorraum, dann ist $(V, +)$ eine Gruppe. (Dies war Bestandteil der Vektorraum-Definition.)

Alle unter (i) bis (v) aufgezählten Halbgruppen, Monoide und Gruppen sind abelsch. Bei Punkt (iv) beachte man, dass durch die Addition keine Verknüpfung auf $\mathbb{Q}^\times$ definiert ist, denn das Bild von $+ : \mathbb{Q}^\times \times \mathbb{Q}^\times \to \mathbb{Q}$, $(a,b) \mapsto a+b$ ist nicht in $\mathbb{Q}^\times$ enthalten. Das Paar $(\mathbb{Q}^\times, +)$ ist also noch nicht einmal eine Halbgruppe. Um zumindest ein nicht-abelsches Beispiel zu haben, ergänzen wir unsere Liste noch um

(vi) Sei $n \in \mathbb{N}$ mit $n \geq 2$, K ein Körper und $\mathscr{M}_{n,K}$ die Menge der $n \times n$-Matrizen über K. Es bezeichne $\cdot$ die Multiplikation von Matrizen. Dann ist $(\mathscr{M}_{n,K}, \cdot)$ ein nicht-abelsches Monoid, mit der Einheitsmatrix E_n als Neutralelement. (Für $n = 1$ ist das Monoid offenbar abelsch.)

Anhand der aufgezählten Beispiele wird deutlich, dass Halbgruppen, Monoide und Gruppen in zwei unterschiedlichen Schreibweisen vorkommen, 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.

Häufig betrachten man Homomorphismen mit zusätzlichen Eigenschaften.

Definition 1.9 Seien $(G, *)$ und $(H, \circ)$ Halbgruppen und $\phi : G \to H$ ein Halbgruppen-Homomorphismus. Man bezeichnet ϕ als

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

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

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

Einen Halbgruppen-Homomorphismus $\phi : G \to G$ von $(G, \cdot)$ nach $(G, \cdot)$ bezeichnet man als Halbgruppen-***Endomorphismus***. Ist die Abbildung ϕ außerdem bijektiv, dann spricht man von einem Halbgruppen-***Automorphismus***. Alle fünf Bezeichnungen sind bereits aus der Linearen Algebra geläufig (in Verbindung mit den linearen Abbildungen), und man verwendet sie auch in vielen anderen Kategorien.

Man bezeichnet zwei Halbgruppen (bzw. Monoide, Gruppen) $(G, *)$ und $(H, \circ)$ als ***isomorph*** und schreibt $G \cong H$, wenn es einen Isomorphismus $\phi : G \to H$ von Halbgruppe (bzw. Monoiden, Gruppen) gibt. Wie wir im weiteren Verlauf noch sehen werden, besitzen zwei isomorphe Halbgruppen, Monoide oder Gruppen in jeder Hinsicht dieselben algebraischen Eigenschaften. Sind zwei Halbgruppen $(G, *)$ und $(H, \circ)$ beispielsweise isomorph, dann sind sie immer auch gleich mächtig, weil jeder Isomorphismus eine Bijektion ist. Ist $(G, *)$ darüber hinaus ein Monoid (bzw. eine Gruppe), dann gilt dasselbe für $(H, \circ)$ (Beweis als Übung).

Die in Proposition 1.6 (ii) formulierte Rechenregel lässt sich leicht auf mehrere Faktoren erweitern.

Lemma 1.10 Sei $(G, *)$ ein Monoid. Ist $r \in \mathbb{N}$ und sind $g_1, ..., g_r \in G$ invertierbare Elemente, dann gilt $(g_1 * ... * g_r)^{-1} = g_r^{-1} * ... * g_1^{-1}$.

Beweis: Wir führen den Beweis durch vollständige Induktion über die Anzahl r der Faktoren. Für $r = 1$ ist nichts zu zeigen. Sei nun $r \geq 1$ vorgegeben, und setzen wir die Aussage für dieses r voraus. Seien $g_1, ..., g_{r+1} \in G$ invertierbare Elemente. Nach Induktionsvoraussetzung gilt $(g_1 * ... * g_r)^{-1} = g_r^{-1} * ... * g_1^{-1}$. Damit erhalten wir

$$(g_1 * ... * g_r * g_{r+1})^{-1} \quad = \quad ((g_1 * ... * g_r) * g_{r+1})^{-1} \quad = \quad g_{r+1}^{-1} * (g_1 * ... * g_r)^{-1} \quad = \quad g_{r+1} * g_r^{-1} * ... * g_1^{-1} \quad ,$$

wobei im zweiten Schritt Prop. 1.6 angewendet wurde. □

Bereits in früheren Semestern 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 1.11 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 1.12 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.

Lemma 1.13 Sei $\phi : G \to H$ ein Homomorphismus zwischen den Halbgruppen $(G,*)$ und $(H,\circ)$, und sei $g \in G$. Dann gilt $\phi(g^n) = \phi(g)^n$ für alle $n \in \mathbb{N}$. Bei einem Monoid-Homomorphismus gilt die Regel für alle $n \in \mathbb{N}_0$. Ist g invertierbar, dann gilt dasselbe für $\phi(g)$, und die Gleichung $\phi(g^n) = \phi(g)^n$ ist für alle $n \in \mathbb{Z}$ gültig.

Beweis: Sei zunächst ϕ ein Halbgruppen-Homomorphismus. Wir beweisen die Aussage durch vollständige Induktion über n. Den Induktionsanfang erhält man durch die Gleichung $\phi(g^1) = \phi(g) = \phi(g)^1$, den Induktionsschritt von n auf $n+1$ durch

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

wobei bei der dritten Gleichung die Induktionsvoraussetzung verwendet wurde. Ist ϕ ein Monoid-Homomorphismus, dann gilt auch $\phi(g^0) = \phi(e_G) = e_H = \phi(g)^0$. Sei nun g ein invertierbares Element und $m \in \mathbb{N}$. Dann gilt $\phi(g^m) \circ \phi(g^{-m}) = \phi(g^m * g^{-m}) = \phi(g^{m-m}) = \phi(g^0) = \phi(e_G) = e_H$, und ebenso zeigt man $\phi(g^{-m}) \circ \phi(g^m) = e_G$. Dies zeigt, dass $\phi(g^m)$ für alle $m \in \mathbb{N}$ invertierbar ist, insbesondere das Element $\phi(g^1) = \phi(g)$. Außerdem gilt jeweils $\phi(g^{-m}) = \phi(g^m)^{-1} = (\phi(g^m))^{-1} = (\phi(g)^m)^{-1} = \phi(g)^{-m}$. Weil die Aussage $\phi(g^n) = \phi(g)^n$ für alle $n \in \mathbb{N}_0$ bereits gezeigt wurde, ist sie damit insgesamt für alle $n \in \mathbb{Z}$ bewiesen. □

Definition 1.14 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.
Darüber hinaus gilt

(i) Sind G und H abelsch, dann gilt dasselbe für $(G \times H, *)$.

(ii) Sind G' und H' zwei weitere Gruppen mit $G \cong G'$ und $H \cong H'$, dann folgt $G \times H \cong G' \times H'$.

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.

zu (i) Vorausgesetzt ist, dass G und H abelsch sind. Seien $(g_1,h_1),(g_2,h_2) \in G \times H$ vorgegeben. Dann gilt $(g_1,h_1)*(g_2,h_2) = (g_1g_2, h_1h_2) = (g_2g_1, h_2h_1) = (g_2,h_2)*(g_1,h_1)$.

zu (ii) Zur besseren Unterscheidung verwenden wir für die Gruppe $G' \times H'$ das Verknüpfungssymbol $\widehat{*}$. Auf Grund der Voraussetzungen $G \cong G'$ und $H \cong H'$ gibt es Isomorphismen $\phi : G \to G'$ und $\psi : H \to H'$. Wir zeigen, dass die Abbildung $\alpha : G \times H \to G' \times H'$ gegeben durch $\alpha(g,h) = (\phi(g), \psi(h))$ für alle $(g,h) \in G \times H$ einen Isomorphismus zwischen $G \times H$ und $G' \times H'$ definiert.

Zunächst beweisen wir die Bijektivität. Zum Nachweis der Injektivität seien $(g_1,h_1),(g_2,h_2)$ mit $\alpha(g_1,h_1) = \alpha(g_2,h_2)$ vorgegeben. Dann folgt $(\phi(g_1),\psi(h_1)) = (\phi(g_2),\psi(h_2))$ und somit $\phi(g_1) = \phi(g_2)$ und $\psi(h_1) = \psi(h_2)$. Weil ϕ und ψ injektiv sind, folgt $g_1 = g_2$ und $h_1 = h_2$ und damit auch $(g_1,g_2) = (h_1,h_2)$. Zum Nachweis der Surjektivität sei $(g',h') \in G' \times H'$ vorgegeben. Weil $\phi : G \to G'$ und $\psi : H \to H'$ surjektiv sind, gibt es Elemente $g \in G$ und $h \in H$ mit $\phi(g) = g'$ und $\psi(h) = h'$. Es folgt $\alpha(g,h) = (\phi(g),\psi(h)) = (g',h')$.

Zum Schluss überprüfen wir noch, dass $\alpha : G \times H \to G' \times H'$ ein Gruppenhomomorphismus ist. Wieder seien zwei Elemente (g_1,h_1) und (g_2,h_2) in $G \times H$ vorgegeben. Auf Grund der Definition von α und der Homomorphismus-Eigenschaft der beiden Abbildungen ϕ, ψ erhalten wir

$$\begin{aligned}\alpha((g_1,h_1)*(g_2,h_2)) \quad &= \quad \alpha(g_1g_2,h_1h_2) \quad = \quad (\phi(g_1g_2),\psi(h_1h_2)) \quad = \quad (\phi(g_1)\phi(g_2),\psi(h_1)\psi(h_2)) \\ &= \quad (\phi(g_1),\psi(h_1)) \,\widehat{*}\, (\phi(g_2),\psi(h_2)) \quad = \quad \alpha(g_1,h_1) \,\widehat{*}\, \alpha(g_2,h_2).\end{aligned}$$

□

Beispielsweise ist die Menge $\mathbb{Z}\times\mathbb{Z}$ mit der Verknüpfung $(a,b)\oplus(c,d) = (a+c, b+d)$ eine Gruppe. Das Neutralelement der Gruppe ist $(0,0)$, und das Inverse von (a,b) ist jeweils $(-a,-b)$.

Definition 1.15 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.

An dieser Stelle ist es angebracht, auf eine abweichende Einführung der Gruppenaxiome hinzuweisen, wie man sie häufig in der Physik-Literatur antrifft. Dort werden Gruppen durch die Formulierung definiert, dass sie „abgeschlossen sind, ein Neutralelement besitzen und jedes Element ein Inverses hat". Mit „abgeschlossen" ist dort gemeint, dass für Gruppenelemente $g, h \in G$ auch die Verknüpfung gh ein Element aus G ist. Dies ist natürlich nur dann eine sinnvolle Aussage, wenn von vornherein klar ist, welche Bedeutung der Ausdruck gh hat (unabhängig davon, ob gh in G liegt oder nicht).

Tatsächlich ist dies in physikalischen Anwendungen häufig der Fall. Ist G beispielsweise die Menge der Lorentz-Transformationen (aus der Speziellen Relativitätstheorie), dann sind die Elemente von G insbesondere bijektive Abbildungen $\mathbb{R}^4 \to \mathbb{R}^4$. Für beliebige $g, h \in G$ ist dann mit gh offenbar die ebenfalls bijektive Komposition der Abbildungen g und h gemeint (in ausführlicher Schreibeweise $g \circ h$). Unter „Abgeschlossenheit" versteht der Physiker dann die Feststellung, dass die bijektive Abbildung $g \circ h : \mathbb{R}^4 \to \mathbb{R}^4$ wiederum eine Lorentz-Transformation ist.

Auch in der Mathematik ist man häufig in der Situation, dass die Verknüpfung auf einer Menge U wie oben durch Einschränkung einer Verknüpfung zu Stande kommt, die ursprünglich auf einer größeren Menge $G \supseteq U$ definiert ist. Allerdings verwendet man für die Konstruktion von Gruppen, wie wir noch sehen werden, häufig auch recht „exotische" Mengen (deren Elemente zum Beispiel Äquivalenzklassen sind), auf denen eine Verknüpfung von Grund auf neu konstruiert werden muss, und nicht einfach von einer größeren Menge „geerbt" werden kann.

Aus diesem Grund ist der Zugang der Physiker zum Gruppenbegriff für unsere Zwecke nicht flexibel genug. Zunächst aber betrachten wir einen Fall, bei dem eine Gruppenverknüpfung tatsächlich durch Einschränkung einer Verknüpfung auf einer größeren Menge zu Stande kommt.

Satz 1.16 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 1.6 (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 1.6 (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 1.6 (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 $(G^\times, *_{G^\times})$ oft einfach wieder mit $*$ bezeichnet. Wir diskutieren eine Reihe von Anwendungsbeispielen von Satz 1.16.

(i) Die Zahlen ± 1 die einzigen invertierbaren Elemente des Monoids $(\mathbb{Z}, \cdot)$. Also bilden diese eine zweielementige Gruppe.

(ii) Für jeden Körper K und jedes $n \in \mathbb{N}$ bildet die Menge $\mathscr{M}_{n,K}$ der $(n \times n)$-Matrizen über K mit der Matrizenmultiplikation als Verknüpfung ein Monoid, mit der Einheitsmatrix als Neutralelement. Die Teilmenge $\mathrm{GL}_n(K) \subseteq \mathscr{M}_{n,K}$ der invertierbaren Matrizen bildet darin eine Gruppe, die als ***allgemeine lineare Gruppe*** bekannt ist.

(iii) Bezeichnet allgemeiner V einen K-Vektorraum, dann bildet die Menge $\mathrm{End}_K(V)$ der Vektorraum-Endomorphismen von V (also die Menge der linearen Abbildungen $V \to V$) zusammen mit der Komposition $\circ$ von Abbildungen ein Monoid, mit der identischen Abbildung id_V als Neutralelement. Die Teilmenge $\mathrm{Aut}_K(V) \subseteq \mathrm{End}_K(V)$ der Automorphismen von V, also der bijektiven Endomorphismen, bildet darin eine Gruppe. Man nennt $\mathrm{Aut}_K(V)$ auch die ***Automorphismengruppe*** oder allgemeine Gruppe des Vektorraums V; häufig wird auch die Bezeichnung $\mathrm{GL}(V)$ verwendet.

Das folgende Beispiel wird im weiteren Verlauf eine besonders wichtige Rolle spielen.

Proposition 1.17 Sei X eine Menge und $\mathrm{Map}(X)$ die Menge der Abbildungen $X \to X$. Für $f, g \in \mathrm{Map}(X)$ bezeichnet $f \circ g$ wie immer die Komposition von f und g gegeben durch

$$(f \circ g)(x) \quad = \quad f(g(x)) \qquad \text{für alle} \quad x \in X.$$

Dann ist das Paar $(\mathrm{Abb}, \circ)$ ein Monoid. Das Neutralelement ist die Abbildung id_X gegeben durch $\mathrm{id}_X(x) = x$ für alle $x \in X$.

Beweis: Um zu zeigen, dass $\circ$ eine assoziative Verknüpfung ist, müssen wir die Gleichung $(f \circ g) \circ h = f \circ (g \circ h)$ für alle $f, g, h \in \mathrm{Map}(X)$ überprüfen. Dazu rechnen wir nach, dass die Abbildung auf der linken Seite dieser Gleichung auf jedem Element $x \in X$ des Definitionsbereichs mit der Abbildung auf der rechten Seite übereinstimmt. Tatsächlich gilt

$$((f \circ g) \circ h)(x) \quad = \quad (f \circ g)(h(x)) \quad = \quad f(g(h(x))) \quad = \quad f((g \circ h)(x)) \quad = \quad (f \circ (g \circ h))(x).$$

Nun zeigen wir, dass id_X das Neutralelement von $(\mathrm{Map}(X), \circ)$ ist, indem wir die Gleichungen $f \circ \mathrm{id}_X = f$ und $\mathrm{id}_X \circ f = f$ überprüfen. Für beliebiges $x \in X$ gilt $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x)$ und $(\mathrm{id}_X \circ f)(x) = \mathrm{id}_X(f(x)) = f(x)$, also sind beide Gleichungen erfüllt. □

Proposition 1.18 Eine Abbildung $f \in \mathrm{Map}(X)$ ist genau dann im Monoid $(\mathrm{Map}(X), \circ)$ invertierbar, wenn sie bijektiv ist. In diesem Fall ist das Inverse von f durch die Umkehrabbildung f^{-1} gegeben.

Beweis: Aus der Erstsemester-Vorlesung ist bekannt, dass eine Abbildung $f : X \to X$ genau dann bijektiv ist, wenn eine Abbildung $g : X \to X$ mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_X$ existiert. Weil id_X in unserem Monoid das Neutralelement ist, sind diese beiden Gleichungen äquivalent zur Invertierbarkeit von f. □

Weil die bijektiven Abbildungen genau die invertierbaren Elemente im Monoid $(\mathrm{Map}(X), \circ)$ sind, liefern uns diese nach Satz 1.16 eine in $\mathrm{Map}(X)$ enthaltene Gruppe.

Definition 1.19 Sei X eine Menge. Dann bildet die Teilmenge $\mathrm{Per}(X) \subseteq \mathrm{Map}(X)$ bestehend aus den bijektiven Abbildungen $X \to X$ mit der Komposition $\circ$ von Abbildungen eine Gruppe. Man bezeichnet $(\mathrm{Per}(X), \circ)$ als die ***Permutationsgruppe*** und die Elemente von $\mathrm{Per}(X)$ als die ***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 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. 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

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

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***. Wir werden später sehen, 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*.

(iii) Die ***Signumsfunktion*** ist eine Abbildung $\mathrm{sgn} : S_n \to \{\pm 1\}$ mit folgenden Eigenschaften: Es gilt $\mathrm{sgn}(\mathrm{id}) = 1$ und $\mathrm{sgn}(\sigma \circ \tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ für alle $\sigma, \tau \in S_n$, mit andere Worten, die Abbildung ist ein Gruppenhomomorphismus. Außerdem gilt $\mathrm{sgn}(\sigma) = (-1)^{k-1}$, falls σ einen k-Zykel bezeichnet, für $2 \leq k \leq n$.

(iv) Man überprüft leicht, dass die Teilmenge $A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$ unter $\circ$ abgeschlossen ist und mit der auf A_n eingeschränkten Verknüpfung wiederum eine Gruppe bildet. Man nennt sie die ***alternierende Gruppe***.

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

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

Die Tabellenschreibweise ist deutlich übersichtlicher: Es gilt

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

Auch die Elemente der Gruppe S_4 lassen sich noch leicht in Zykelschreibweise angeben. Es ist

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

Die alternierende Gruppe A_4 ist gegeben durch

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

Innerhalb von A_4 existiert noch eine weitere wichtige Gruppe, die sogenannte ***Kleinsche Vierergruppe*** V_4 gegeben durch

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

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

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

also bezeichnen die Schreibweisen (1 2 3 4) und (2 3 4 1) dasselbe Element der Gruppe S_4. Der folgende Satz zeigt, dass wir eine zu $S_4 = \mathrm{Per}(M_4)$ isomorphe Gruppe erhalten, wenn wir $M_4 = \{1, 2, 3, 4\}$ durch eine beliebige andere vierelementige Menge ersetzen, zum Beispiel durch $\{2, 5, 7, 11\}$.

Satz 1.20 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 $\mathrm{Per}(X) \to \mathrm{Per}(X)$ definiert. Um zu zeigen, dass $\hat{\phi}$ ein Homomorphismus von Gruppen ist, seien $\sigma, \tau \in \mathrm{Per}(X)$ vorgegeben. Dann gilt

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

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 1.20 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.

Satz 1.21 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. □

Für eine letzte wichtige Klasse von Anwendungsbeispielen zu Satz 1.16 legen wir 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

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

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 1.22 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

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

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. □

Zusammen mit Satz 1.16 erhalten wir nun

Satz 1.23 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 1.22. Allerdings lassen sich zwei Isomorphismen $G \to H$ in der Regel nicht verknüpfen (jedenfalls nicht mit der Komposition von Abbildungen), also bilden die Isomorphismen zwischen G und H im Allgemeinen keine Gruppe.

§ 2. *Untergruppen und Erzeugendensysteme*

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. Bild- und Urbildmengen von Untergruppen unter Gruppenhomomorphismen sind ebenfalls Untergruppen. Hervorzuheben sind hierbei der *Kern* und das *Bild* von Gruppenhomomorphismen.

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. Untergruppen, die von einem einzigen Element erzeugt werden, nennt man *zyklisch*. Ist $\phi : G \to H$ ein Gruppenhomomorphismus und $S \subset G$ ein Erzeugendensystem von G, dann ist ϕ bereits durch die Bilder $\phi(s)$ mit $s \in S$ eindeutig festgelegt.

Wichtige Grundbegriffe

- Definition des Untergruppenbegriffs (Beispiele: A_n, $\mathrm{SL}_n(K)$)
- Kern und Bild eines Gruppenhomomorphismus
- von einer Teilmenge S erzeugte Untergruppe $\langle S \rangle$
- Erzeugendensysteme einer Gruppe (Beispiele: Erzeugendensysteme für S_n, A_n und für die Diedergruppen D_n)
- zyklische Untergruppe

Zentrale Sätze

- Gruppen-Eigenschaft der Untergruppen
- Bilder und Urbilder von Untergruppen unter Gruppenhomomorphismen sind Untergruppen
- Satz über die Eindeutigkeit von Gruppenhomomorphismen

Definition 2.1 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.

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 2.2 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. □

Im weiteren Verlauf der Vorlesung wird uns eine Vielzahl von Untergruppen begegnen. Zunächst beschränken wir uns auf die folgenden zwei Beispiele.

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

(ii) Sei K ein Körper, V ein K-Vektorraum und $\mathrm{Aut}_K(V)$ die bereits in § 1 definierte Menge der Vektorraum-Automorphismen von V. Dann ist $\mathrm{Aut}_K(V)$ eine Untergruppe der Permutationsgruppe $\mathrm{Per}(V)$. Denn aus der Linearen Algebra ist bekannt, dass id_V eine lineare Abbildung ist. Also ist das Neutralelement von $\mathrm{Per}(V)$ in $\mathrm{Aut}_K(V)$ enthalten. Seien nun $\varphi, \psi \in \mathrm{Aut}_K(V)$ vorgegeben. Nach Ergebnissen aus der Linearen Algebra sind auch die Kompositionen $\varphi \circ \psi$ und φ^{-1} linear, außerdem sind sie bijektiv, insgesamt also in $\mathrm{Aut}_K(V)$ enthalten. Damit haben wir die Untergruppen-Bedingungen verifiziert.

Darüber hinaus können auch Gruppenhomomorphismen zur Definition von Untergruppen definiert werden.

Proposition 2.3 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 $g'h' = \phi(g)\phi(h) = \phi(gh) \in U$, 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 2.3 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 $\mathscr{M}_{n,K}$ 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. Der Kern $\mathrm{SL}_n(K) = \{A \in \mathscr{M}_{n,K} \mid \det(A) = 1\}$ wird die ***spezielle lineare Gruppe*** vom Rang n über dem Körper K genannt. Es handelt sich um eine Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(K)$.

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

> **Proposition 2.4** 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 $g = h$. □

Häufig kann man aus einer gegebenen Familie von Unterstrukturen durch bestimmte Operationen neue Unterstrukturen definieren. In der Linearen Algebra haben wir dieses Phänomen am Beispiel der Summe und Durchschnitte von Untervektorräumen beobachtet. Entsprechend gilt in der Kategorie der Gruppen

> **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 § 6 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 2.1 formulierte Eigenschaft von Untergruppen als auch die in Proposition 1.6 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 $g_1 \cdot ... \cdot g_r$ 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 $r, s \in \mathbb{N}_0$, $g_1, \ldots, g_r, g_1', \ldots, g_s' \in S$ und $\varepsilon_1, \ldots, \varepsilon_r, \varepsilon_1', \ldots, \varepsilon_s' \in \{\pm 1\}$, so dass $g = g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r}$ und $g' = (g_1')^{\varepsilon_1'} \cdot \ldots \cdot (g_s')^{\varepsilon_s}$ erfüllt ist. Offenbar sind die Elemente

$$gg' = g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \cdot (g_1')^{\varepsilon_1'} \cdot \ldots \cdot (g_s')^{\varepsilon_s} \qquad \text{und} \qquad g^{-1} = g_r^{-\varepsilon_r} \cdot \ldots \cdot g_1^{-\varepsilon_1}$$

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 $r \in \mathbb{N}$, $g_1, \ldots, g_r \in S$ und $\varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$. Wegen $S \subseteq V$ gilt dann auch $g_1, \ldots, g_r \in V$. Weil V eine Untergruppe von G ist, folgt $g_k^{\varepsilon_k} \in V$ für $1 \leq k \leq r$ und schließlich $g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \in V$. 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 $e_1, \ldots, e_m, e_1', \ldots, e_m' \in \mathbb{Z}$ mit $g = g_1^{e_1} \cdot \ldots \cdot g_m^{e_m}$ und $g' = g_1^{e_1'} \cdot \ldots \cdot g_m^{e_m'}$. Es folgt

$$gg' \quad = \quad (g_1^{e_1} \cdot \ldots \cdot g_m^{e_m})(g_1^{e_1'} \cdot \ldots\ldots \cdot g_m^{e_m'}) \quad = \quad (g_1^{e_1} g_1^{e_1'}) \cdot \ldots (g_m^{e_m} g_1^{e_m'}) \quad = \quad g_1^{e_1+e_1'} \cdot \ldots \cdot g_m^{e_m+e_m'}$$

und

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

Damit ist der Nachweis der Untergruppen-Eigenschaft abgeschlossen. Nun zeigen wir, dass $U \supseteq S$ gilt. Sei dazu $k \in \{1, \ldots, m\}$ vorgegeben. Setzen wir $e_k = 1$ und $e_i = 0$ für $1 \leq i \leq m$ mit $i \neq k$, dann erhalten wir $g_k = g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \in U$. 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 $e_1, \ldots, e_m \in \mathbb{Z}$ beliebig vorgegeben, dann folgt auf Grund der Untergruppen-Eigenschaft $g_k^{e_k} \in V$ für $1 \leq k \leq m$ und schließlich $g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \in V$. 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 Beleg für die Nützlichkeit der Erzeugendensysteme zeigen wir, dass jeder Homomorphismus durch seine Werte auf einem Erzeugendensystem eindeutig bestimmt ist. Dies ermöglicht in vielen Fällen eine einfache Kennzeichnung von Homomorphismen. Insbesondere wird sich dieser Satz beim Studium der zyklischen Gruppen und ihrer Automorphismen als nützlich erweisen.

Satz 2.11 *(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.

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*** 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.

Satz 2.12 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 $|\mathrm{supp}(\sigma)|$, 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 $|\mathrm{supp}(\sigma)| = 0$ gilt $\mathrm{supp}(\sigma) = \varnothing$ und $\sigma = \mathrm{id}$, also ist hier nichts zu zeigen. Elemente $\sigma \in S_n$ mit $|\mathrm{supp}(\sigma)| = 1$ existieren nicht, und die Elemente mit $|\mathrm{supp}(\sigma)| = 2$ sind genau die Transpositionen.

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

Das folgende Resultat wird in der Galoistheorie benötigt. Man kann damit die Nicht-Auflösbarkeit bestimmter algebraischer Gleichungen durch Radikale beweisen.

> **Proposition 2.13** Für jedes $n \in \mathbb{N}$ ist die Menge $\{\sigma, \tau\}$ bestehend aus den beiden Elementen $\sigma = (1\ 2\ ...\ n)$ 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 $(i+1\ \ i+2) \circ (i\ \ i+1) \circ (i+1\ \ i+2) = (i\ \ i+2)$, $(i+2\ i+3) \circ (i\ \ i+2) \circ (i+2\ i+3) = (i\ \ i+3)$ 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 2.12 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. Sei $p = n$ eine ungerade Primzahl, $\sigma = (i_1\ i_2\ ...\ i_p)$ ein p-Zykel und τ eine beliebige Transposition. Definieren wir $\rho \in S_p$ durch

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

dann ist das Element $\tilde{\sigma} = \rho\sigma\rho^{-1}$ gegeben durch $\tilde{\sigma} = (\rho(i_1) \dots \rho(i_p)) = (1\ 2 \dots p)$. 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 $\sigma = (1\ 2 \dots p)$ 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 $r \equiv 1+k(i-1) \mod p$, 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 $r \equiv 1+k(i-1) \mod p$ und $s \equiv 1+(k+1)(i-1) \mod p$. 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 $r \in M_p$, $r = 1+1 = 1+k(i-1)+\ell p \equiv 1+k(i-1) \mod p$ und $(1\ r) = (1\ 2) \in \langle\sigma,\tau\rangle$. Wegen $\sigma = (1\ 2 \dots p) \in \langle\sigma,\tau\rangle$ enthält $\langle\sigma,\tau\rangle$ auf Grund der ersten Aussage der Proposition also ein vollständiges Erzeugendensystem von S_p. □

Sei $n \in \mathbb{N}$ mit $n \geq 3$. Wir definieren in der symmetrischen Gruppe S_n das Element $\rho_n = (1\ 2 \dots n)$. Außerdem setzen wir

$$\tau_n \quad = \quad \begin{cases} (1\ n)(2\ n-1) \circ \dots \circ (\frac{n}{2}\ \frac{n}{2}+1) & \text{falls } n \text{ gerade,} \\ (1\ n-1)(2\ n-2) \circ \dots \circ (\frac{n-1}{2}\ \frac{n+1}{2}) & \text{falls } n \text{ ungerade.} \end{cases}$$

Beispielsweise ist $\tau_6 = (1\ 6)(2\ 5)(3\ 4)$, $\tau_7 = (1\ 6)(2\ 5)(3\ 4)$ und $\tau_8 = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$. Man kann τ_n auch direkt als Abbildungsvorschrift angeben. Für $1 \leq k \leq n$ ist

$$\tau_n(k) \quad = \quad \begin{cases} n+1-k & \text{falls } n \text{ gerade} \\ n-k & \text{falls } n \text{ ungerade und } k \leq n-1 \\ n & \text{falls } n \text{ ungerade und } k = n \end{cases}$$

Diese Elemente besitzen folgende geometrische Interpretation: Wir betrachten in der Ebene ein regelmäßiges n-Eck, dessen Ecken entgegen dem Uhrzeigersinn mit $1,\dots,n$ durchnummeriert sind. Auf dieses n-Eck lassen sich nun eine Reihe von Symmetrieoperationen anwenden. Beispielsweise kann die Figur um ein ganzzahliges Vielfaches des Winkels $\frac{2\pi}{n}$ rotiert werden. Ist n gerade, dann können wir durch zwei gegenüberliegende Ecken oder Seiten der Figur eine Achse legen und bezüglich dieser Achse spiegeln. Ist n ungerade, so können wir bezüglich einer Achse spiegeln, die durch eine Ecke und die gegenüberliegende Seite verläuft.

Notieren wir uns bei jeder dieser Operationen, wie die Ecken vertauscht werden, dann erhält man ein Element der symmetrischen Gruppe S_n. Rotiert man zum Beispiel um den Winkel $\frac{2\pi}{n}$ gegen den Uhrzeigersinn, so erhält man das Element ρ_n. Rotiert man mit demselben Drehsinn um den Winkel $\frac{2\pi k}{n}$ mit $k \in \mathbb{N}$, so ist die Permutation der Ecken durch ρ_n^k gegeben. Auf dieselbe Weise repräsentiert τ_n für gerades n die Spiegelung bezüglich der Achse durch die beiden Seiten $1-n$ und $\frac{n}{2}-\frac{n}{2}+1$. Für ungerades n repräsentiert τ_n die Spiegelung bezüglich der Achse durch den Eckpunkt n und die Seite $\frac{n-1}{2}-\frac{n+1}{2}$.

Definition 2.14 Sei $n \in \mathbb{N}$ mit $n \geq 3$. Dann wird die Untergruppe $D_n = \langle \rho_n, \tau_n \rangle$ von S_n die ***n-te Diedergruppe*** genannt.

Im Kapitel über Normalteiler werden wir zeigen, dass die Gruppe D_n jeweils aus genau $2n$ Elementen besteht. Die $2n$ Elemente sind gegeben durch $\rho_n^a \circ \tau_n^b$ mit $0 \leq a < n$ und $b \in \{0, 1\}$.

§ 3. *Zyklische 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. Bei einer endlichen zyklischen Gruppe stimmt die Anzahl der Untergruppen mit der Anzahl der Teiler ihrer Ordnung überein. Ist G eine zyklische Gruppe, so lassen sich auch die Homomorphismen $G \to H$ in eine andere Gruppe H leicht beschreiben. Dies liefert uns auch eine einfache Beschreibung der Automorphismengruppe $\operatorname{Aut}(G)$ einer zyklischen Gruppe G.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Ordnung einer Gruppe	– äquivalente Charakterisierung der Elementordnung
– Ordnung eines Gruppenelements	– Rechenregeln für die Elementordnung
– prime Restklassengruppe	– Beschreibung der Untergruppen zyklischer Gruppen
	– Existenz von Homomorphismen von einer zyklischen Gruppe G in eine Gruppe H
	– Beschreibung der Automorphismengruppe zyklischer Gruppen

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.

In § 3 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 $g, g^2, g^3, ...$ 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 $\{e_G, g, ..., g^{m-1}\}$ 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

$$g^r \quad = \quad g^{m-qn} \quad = \quad g^m \cdot (g^n)^{-q} \quad = \quad e_G \circ e_G \quad = \quad e_G.$$

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 $\langle g \rangle = \{e_G, g, ..., g^{n-1}\}$. 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 zwei 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 der symmetrischen Gruppe S_n kann man leicht überprüfen, dass für $2 \leq k \leq n$ jeder k-Zykel, also jedes Element der Form $(a_1 \; ... \; a_k)$ mit voneinander verschiedenen Einträgen $a_i \in \{1, ..., n\}$, ein Element der Ordnung k ist. Ist σ ein Produkt disjunkter Zykel der Längen $k_1, ..., k_r$, dann gilt $\text{ord}(\sigma) = \text{kgV}(k_1, ..., k_r)$. Beispielsweise gilt $(1\,2\,3)^2 = (1\,2\,3)(1\,2\,3) = (1\,3\,2)$ und $(1\,2\,3)^3 = (1\,2\,3)^2(1\,2\,3) = (1\,3\,2)(1\,2\,3) = \text{id}$, also $\text{ord}((1\,2\,3)) = 3$.

Nun können wir die Elemente einer endlichen, zyklischen Gruppe genau angeben.

Folgerung 3.4 Sei G eine Gruppe. Besitzt $g \in G$ die endliche Ordnung n, dann sind durch $e_G, g, g^2, ..., g^{n-1}$ 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 $n \in \mathbb{N}$.
Im weiteren Verlauf beschäftigen wir uns nun mit der Untergruppenstruktur zyklischer Gruppen.

Satz 3.6 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 $\text{ord}(g) = n$ 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 „⊇“ gilt nach Definition der erzeugten Untergruppe. Nehmen wir nun an, dass „⊆“ 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. □

Wir erinnern an die Definition des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen zweier ganzer Zahlen. Seien $a, b \in \mathbb{Z}$ vorgegeben. Eine Zahl $d \in \mathbb{N}$ heißt ***gemeinsamer Teiler*** von a und b, wenn d ein Teiler von a und zugleich ein Teiler von b ist. Man nennt d den ***größten*** gemeinsamen Teiler von a und b und schreibt $d = \mathrm{ggT}(a, b)$, wenn $d'|d$ für jeden gemeinsamen Teiler von a und b gilt. Die Zahlen a und b werden als ***teilerfremd*** bezeichnet, wenn $\mathrm{ggT}(a, b) = 1$ ist.

Die Zahl d heißt ***gemeinsames Vielfaches*** von a und b, wenn sowohl $a|d$ als auch $b|d$ erfüllt ist. Vom ***kleinsten*** gemeinsamen Vielfachen $\mathrm{kgV}(a, b)$ spricht man, wenn jedes weitere gemeinsame Vielfache d' von a und b auch eine Vielfaches von d ist. Aus der Klassifikation der Untergruppen einer zyklischen Gruppe können wir das folgende zahlentheoretische Resultat herleiten.

Satz 3.7 *(Lemma von Bézout)*

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

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 3.6 ein $d \in \mathbb{N}$ mit $U = \langle d\rangle$. Wir zeigen, dass $d = \mathrm{ggT}(m, n)$ 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 $d = \mathrm{ggT}(m, n)$ abgeschlossen. Wegen $d \in U$ gibt es nun $a, b \in \mathbb{Z}$ mit $am + bn = d = \mathrm{ggT}(m, n)$. □

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

Satz 3.8 Sei G eine Gruppe und $g \in G$ ein Element der endlichen Ordnung n.

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

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

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

Beweis: zu (i) „⇒“ Wegen $g^m \in \langle g\rangle$ ist $\langle g^m\rangle$ eine Untergruppe von $\langle g\rangle$. Ist $\mathrm{ord}(g^m) = n = \mathrm{ord}(g)$, 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 $\mathrm{ggT}(m, n) = 1$ 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 $am + bn = \mathrm{ggT}(m, n) = 1$. Es folgt

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

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 $\mathrm{ord}(g^m) = |\langle g^m \rangle| = |\langle g \rangle| = \mathrm{ord}(g) = n$.

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

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

In der Ringtheorie 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 $0 \leq k < n$ nach Folgerung 3.4 (i) die n verschiedenen Elemente von G. Aus Satz 3.8 (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 3.9 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 3.10 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 3.6 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 3.6, 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 3.8 (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. □

Sei beispielsweise G eine zyklische Gruppe der Ordnung 12. 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 dieses Kapitels studieren wir die Endo- und Automorphismen zyklischer Gruppen. Dazu schauen wir uns zunächst an, wie sich die Ordnung eines Elements durch Anwendung eines Homomorphismus verändern kann.

Proposition 3.11 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 $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$. Mit dem Kriterium aus Satz 3.3 zur Ordnung von Gruppenelementen folgt sowohl die Endlichkeit von $\mathrm{ord}(\phi(g))$ als auch die Teiler-Eigenschaft. □

Proposition 3.12 *(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 2.11. 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 $n = \mathrm{ord}(g)$ endlich und ein Vielfaches von $\mathrm{ord}(h)$. 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 $\mathrm{ord}(h)$ 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 3.13 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 3.12 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 2.11 gibt es nur einen Homomorphismus $G \to G$ mit $g \mapsto g$, nämlich id_G. Somit ist $\psi \circ \phi = \mathrm{id}_G$. Ebenso schließt man aus der Gleichung $(\phi \circ \psi)(h) = h$, dass $\phi \circ \psi = \mathrm{id}_H$ 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. □

Der Vollständigkeit halber bestimmen wir noch die Automorphismengruppe zyklischer Gruppen. In der Linearen Algebra haben wir für jedes $n \in \mathbb{N}$ den Restklassenring $\mathbb{Z}/n\mathbb{Z}$ definiert. Wir erinnen daran, dass die Elemente von $\mathbb{Z}/n\mathbb{Z}$ die Teilmengen von $\mathbb{Z}$ der Form $a + n\mathbb{Z}$ mit $a \in \mathbb{Z}$ sind, und dass zwei Elemente $a + n\mathbb{Z}$ und $b + \mathbb{Z}$ stimmen genau dann übereinstimmen, wenn n ein Teiler von $b - a$ ist. Somit ist

$$\mathbb{Z}/n\mathbb{Z} \quad = \quad \{a + n\mathbb{Z} \mid 0 \leq a < n\}.$$

Mit Hilfe des Lemmas von Bézout kann man leicht zeigen, dass ein Element $a + n\mathbb{Z}$ aus $\mathbb{Z}/n\mathbb{Z}$ genau dann (bezüglich der Multiplikation) invertierbar ist, wenn $\mathrm{ggT}(a, n) = 1$ gilt. Nach Satz 1.16 bildet die Menge $(\mathbb{Z}/n\mathbb{Z})^\times$ mit der Multiplikation eine abelsche Gruppe der Ordnung $\varphi(n)$. Man bezeichnet diese Gruppen als ***prime Restklassengruppen***.

Sei nun G eine zyklische Gruppe der endlichen Ordnung n und $g \in G$ mit $G = \langle g \rangle$. Wegen Satz 3.8 ist $\mathrm{ord}(g^a)$ für jedes $a \in \mathbb{Z}$ ein Teiler von n. Wir können also Proposition 3.12 anwenden und erhalten für jedes $a \in \mathbb{Z}$ einen eindeutig bestimmten Endomorphismus

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

Zwei solche Endomorphismen τ_a, τ_b mit $a, b \in \mathbb{Z}$ stimmen genau dann überein, wenn n ein Teiler von $b - a$ ist, denn wegen $\mathrm{ord}(g) = n$ ist $n | (b - a)$ äquivalent zu $g^a = g^b$; siehe Satz 3.3. Jedem Element $a + n\mathbb{Z}$ wird damit ein $\tau_a \in \mathrm{End}(G)$ zugeordnet, und diese Zuordnung ist injektiv. Ist $\tau \in \mathrm{End}(G)$ beliebig vorgegeben, dann gilt $\tau(g) = g^a$ für ein $a \in \mathbb{Z}$ und somit $\tau = \tau_a$. Damit ist die Zuordnung auch surjektiv. Insgesamt haben wir damit gezeigt, dass durch die Zuordnung $a + n\mathbb{Z} \mapsto \tau_a$ eine wohldefinierte Bijektion $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$ gegeben ist.

Satz 3.14 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 die Abbildung $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$ ein Monoid-Isomorphismus ist, wobei $\mathbb{Z}/n\mathbb{Z}$ mit der Multiplikation als Verknüpfung ausgestattet ist. Es gilt $\tau_1(g) = g^1 = g$; weil auch $\mathrm{id}_G(g) = g$ gilt, folgt darauf $\tau_1 = \mathrm{id}_G$ auf Grund von Satz 2.11 und somit $\phi(1 + n\mathbb{Z}) = \mathrm{id}_G$. Seien nun $a + n\mathbb{Z}, b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ vorgegeben, mit $a, b \in \mathbb{Z}$. Es gilt

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

Nochmalige Anwendung von Satz 2.11 liefert also $\tau_a \circ \tau_b = \tau_{ab}$. Daraus folgt

$$\phi((a + n\mathbb{Z})(b + n\mathbb{Z})) \quad = \quad \phi(ab + n\mathbb{Z}) \quad = \quad \tau_{ab} \quad = \quad \tau_a \circ \tau_b \quad = \quad \phi(a + n\mathbb{Z})\phi(b + n\mathbb{Z}).$$

Also ist durch ϕ ein Monoid-Homomorphismus definiert. Weil ϕ eine Bijektion ist, handelt es sich um einen Isomorphismus.

Für jedes $a \in \mathbb{Z}$ ist $a + n\mathbb{Z}$ genau dann invertierbar, wenn ein $b \in \mathbb{Z}$ mit $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$ existiert. Wie soeben gezeigt, folgt daraus $\tau_a \circ \tau_b = \tau_1 = \mathrm{id}_G$ und somit die Invertierbarkeit von τ_a in $\mathrm{End}(G)$, also $\tau_a \in \mathrm{Aut}(G)$. Setzen wir umgekehrt $\tau_a \in \mathrm{Aut}(G)$ voraus, dann gibt es ein $b \in \mathbb{Z}$ mit $\tau_a^{-1} = \tau_b$. Wegen

$$\tau_{ab} \quad = \quad \tau_a \circ \tau_b \quad = \quad \mathrm{id}_G \quad = \quad \tau_1$$

muss $(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} = 1 + n\mathbb{Z}$ gelten, und es folgt $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Insgesamt haben wir damit gezeigt, dass man durch Einschränkung von ϕ auf $(\mathbb{Z}/n\mathbb{Z})^\times$ eine Bijektion zwischen $(\mathbb{Z}/n\mathbb{Z})^\times$ und $\mathrm{Aut}(G)$ erhält. Auf Grund der bereits nachgewiesenen Verträglichkeit von ϕ mit den Verknüpfungen auf den beiden Mengen handelt es sich um einen Isomorphismus von Gruppen. □

Auch im Fall, dass $G = \langle g \rangle$ unendlich ist, lässt sich die Automorphismengruppe leicht angeben. Nach Proposition 3.12 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 3.14 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 3.13 isomorph. Somit gilt auch $(\mathrm{Aut}(G), \circ) \cong (\mathbb{Z}/2\mathbb{Z}, +)$ für jede unendliche zyklische Gruppe G.

§ 4. *Nebenklassen und Satz von Lagrange*

Zusammenfassung. Unser Hauptziel in diesem Abschnitt ist der Beweis des *Satzes von Lagrange*, welcher besagt, dass bei einer endlichen Gruppe G die Ordnung jeder Untergruppe U ein Teiler von $|G|$ ist; für zyklische Gruppen ist uns dieses Resultat aus § 3 bereits bekannt. Der Beweis für beliebige (also auch nicht-kommutative) Gruppen beruht auf der Beobachtung, dass jede Untergruppe U eine *Zerlegung* der Gruppe in gleich große Teilmengen ermöglicht, die sog. Links- und Rechtsnebenklassen der Untergruppe. Die Zerlegung einer Menge kann über eine sog. *Äquivalenzrelationen* auf der Menge beschreiben, und für den praktischen Umgang mit einer Zerlegung sind *Repräsentantensysteme* hilfreich. Auch diese Konzepte werden wir im ersten Teil dieses Abschnitts kennenlernen.

Wichtige Grundbegriffe

- Links- und Rechtsnebenklassen einer Untergruppe
- Repräsentantensystem der Äquivalenzklassen einer Äquivalenzrelation
- Index $(G : U)$ einer Untergruppe
- induzierte Abbildungen auf Mengen von Äquivalenzklassen

Zentrale Sätze

- Zerlegung einer Gruppe in die Nebenklassen einer Untergruppe
- Satz von Lagrange
- Existenz und Eindeutigkeit der induzierten Abbildung
- Kleiner Satz von Fermat (Gruppentheorie)
- Kleiner Satz von Fermat (Zahlentheorie)

Definition 4.1 Sei $(G, \cdot)$ eine Gruppe und U eine Untergruppe. Eine Teilmenge von G, die mit einem geeigneten $g \in G$ in der Form

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

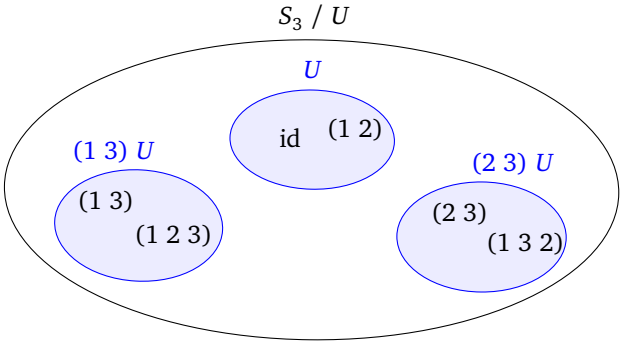
geschrieben werden kann, wird ***Linksnebenklasse*** von U genannt. Ebenso bezeichnet man die Teilmengen der Form $Ug = \{ug \mid u \in U\}$ mit $g \in G$ als ***Rechtsnebenklassen*** von U.

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 4.2 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 $\mathscr{Z} \subseteq \mathscr{P}(X)$ von Teilmengen von X mit den Eigenschaften $\emptyset \notin \mathscr{Z}$, $\bigcup_{A\in\mathscr{Z}} A = X$ und $\forall A, B \in \mathscr{Z} : A \neq B \Rightarrow A \cap B = \emptyset$; 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 $\mathscr{Z}$ eine Zerlegung von X, so erhält man durch

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

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

Lemma 4.3 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 4.4 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 4.3 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 4.3 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 4.5 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 4.6 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 4.7 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 4.8 *(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 4.4 ist G/U eine Zerlegung von G, und nach Lemma 4.2 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 4.9 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 bereits 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.

Die Bedeutung des folgenden Satzes wird im nächsten Kapitel bei der Konstruktion der Faktorgruppen deutlich werden. Wir beweisen ihn bereits hier, weil der Beweis auf dem Konzept der Repräsentantensysteme basiert.

Satz 4.10 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 alls $x, x' \in X$ 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 $5 + 4\mathbb{Z} = 1 + 4\mathbb{Z} \neq 2 + 4\mathbb{Z}$.

Wir notieren einige wichtige Folgerungen aus dem Satz von Lagrange.

Satz 4.11 *(Kleiner Satz von Fermat, gruppentheoretische Version)*

Sei G eine Gruppe der endlichen Ordnung n. Dann ist $\mathrm{ord}(g)$ für jedes $g \in G$ ein Teiler, insbesondere gilt $g^n = e_G$ für alle $g \in G$.

Beweis: Sei $g \in G$ beliebig. Aus der Endlichkeit von G folgt die Endlichkeit der zyklischen Untergruppe $\langle g \rangle$. Nach Definition gilt $\mathrm{ord}(g) = |\langle g \rangle|$, und auf Grund des Satzes von Lagrange ist $|\langle g \rangle|$ ein Teiler von n. Die Gleichung $g^n = e_G$ folgt dann aus Satz 3.3. □

Bei der folgenden zahlentheoretischen Formulierung setzen wir die Definition der Kongruenzrelation aus der Linearen Algebra als bekannt voraus.

Folgerung 4.12 *(Kleiner Satz von Fermat, zahlentheoretische Version)*

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

Beweis: Wir wenden die gruppentheoretische Version es Kleinen Satzes von Fermat auf die prime Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$. Aus der Linearen Algebra ist bekannt, dass $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ und somit $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ gilt. Für jedes $a \in \mathbb{Z}$ ist $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ äquivalent zu $p \nmid a$. Auf Grund des Kleinen Satzes von Fermat gilt $(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$ für diese a, was zu $a^{p-1} \equiv 1 \mod p$ äquivalent ist. Durch Multiplikation dieser Kongruenz mit a folgt $a^p \equiv a \mod p$. Diese Kongruenz ist auch im Fall $p \mid a$ erfüllt, denn dann gilt auch $p \mid a^p$ und somit $a^p \equiv 0 \equiv a \mod p$. □

Wir notieren noch zwei wichtige gruppentheoretische Konsequenzen.

Satz 4.13

(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 $|U|$ und $|V|$ teilerfremd sind, folgt $|U_1| = 1$ und $U_1 = \{e_G\}$. □

§ 5. *Normalteiler und Faktorgruppen*

Zusammenfassung. Bei einem speziellen Typ von Untergruppen N, den sog. *Normalteilern*, kann auf der Menge G/N der Linksnebenklassen von N wiederum eine Gruppenstruktur definiert werden. Die Gruppen, die auf diese Weise zu Stande kommen, bezeichnet man als *Faktorgruppen*. Einfachstes Beispiel sind die Restklassengruppen $\mathbb{Z}/n\mathbb{Z}$, die als Faktorgruppen der unendlichen zyklischen Gruppe $(\mathbb{Z}, +)$ auftreten. Die Faktorgruppen ermöglichen es, die Untersuchung bestimmter Merkmale der Gruppe G auf das Studium der kleineren Gruppe G/N zurückzuführen. Beispielsweise ermöglicht uns der *Korrespondenzsatz*, einen Teil der Untergruppenstruktur von G an der Gruppe G/N abzulesen. Mit Hilfe des Homomorphiesatzes kann eine Faktorgruppe G/N mit anderen Gruppen in Verbindung verglichen werden, die einfacher zu handhaben sind.

Wichtige Grundbegriffe

- Normalteiler einer Gruppe
- Komplexprodukt AB zweier Teilmengen A, B einer Gruppe
- inneres (semi-)direktes Produkt $G = NU$
- Faktorgruppe G/N (G Gruppe, $N \trianglelefteq G$)
- kanonischer Epimorphismus $\pi_N : G \to G/N$
- induzierter Homomorphismus

Zentrale Sätze

- Isomorphismus $NU \cong N \times U$ zwischen innerem und äußerem direkten Produkt
- Homomorphiesatz für Gruppen
- Isomorphiesätze für Gruppen $U/(N \cap U) \cong UN/N$, $(G/N)/(U/N) \cong G/U$
- Korrespondenzsatz für Gruppen

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 5.1 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 5.2 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) ⇒ (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) ⇒ (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) ⇒ (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 ***einfach***, wenn $G \neq \{e_G\}$ gilt und es neben diesen beiden keine weiteren Normalteiler gibt. Ist G abelsch, dann ist *jede* Untergruppe von G ein Normalteiler; vgl. die Bemerkung unmittelbar vor Lemma 4.2. Eine abelsche Gruppe ist also nur dann einfach, wenn sie außer $\{e_G\}$ und G keine weiteren Untergruppen besitzt. Wir werden in § 6 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 5.3

(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 5.3, 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 5.4 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 5.5 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.

Als Anwendung der Komplexprodukte bestimmen wir nun die Elemente der Diedergruppen.

Folgerung 5.6 Sei $n \in \mathbb{N}$, $n \geq 3$. Dann besteht die Diedergruppe $D_n = \langle \rho_n, \tau_n \rangle$ aus $2n$ Elementen, nämlich $\rho_n^a \circ \tau_n^b$ mit $0 \leq a < n$ und $b \in \{0, 1\}$.

Beweis: Wir definieren in S_n die beiden Untergruppen $N = \langle \rho_n \rangle$ und $U = \langle \tau_n \rangle$. Wir zeigen zunächst, dass das Komplexprodukt NU aus den angegebenen Elementen besteht, und dass es sich dabei um $2n$ verschiedene Elemente handelt. Aus § 3 ist bekannt, dass die Ordnung von Elementen der symmetrischen Gruppe S_n direkt angegebenen werden kann, wenn diese als Produkte disjunkter Zykel dargestellt werden. Weil ρ_n ein n-Zykel ist, gilt $\mathrm{ord}(\rho_n) = n$, und als Produkt disjunkter Transpositionen ist τ_n ein Element der Ordnung 2. Nach Folgerung 3.4 gilt damit $|N| = n$ und $|U| = 2$. Darüber hinaus sind die verschiedenen Elemente von N gegeben durch ρ_n^a mit $0 \leq n < a$, und die Elemente von U durch τ_n^b mit $b \in \{0, 1\}$.

Dies zeigt, dass NU tatsächlich aus den angegebenen Elementen besteht. Wenn wir zeigen können, dass darüber hinaus $N \cap U = \{\mathrm{id}\}$ gilt, dann folgt daraus mit Teil (i) von Lemma 5.5, dass es sich dabei um $2n$ verschiedene Elemente handelt. Dass $N \cap U$ mehr als ein Element besitzt, ist wegen $|U| = 2$ nur möglich, wenn U in N enthalten ist. In diesem Fall wären die Elemente von U mit den Elementen aus N vertauschbar, denn als zyklische Gruppe ist N abelsch, siehe Folgerung 2.10 (ii). An der Darstellung der Elemente ρ_n und τ_n lässt sich aber leicht ablesen, dass das Produkt $\tau_n \circ \rho_n \circ \tau_n^{-1} = \tau_n \circ \rho_n \circ \tau_n$ die Zahl 1 auf n und k auf $k-1$ abbildet, für $2 \leq k \leq n$ (wobei die Fälle, dass n gerade bzw. ungerade ist, unterschieden werden müssen). Es gilt also $\tau_n \circ \rho_n \circ \tau_n^{-1} = \rho_n^{-1}$, was zu $\tau_n \circ \rho_n = \rho_n^{-1} \circ \tau_n$

äquivalent ist. Die Gleichung $\tau_n \circ \rho_n = \rho_n \circ \tau_n$ wäre dann gleichbedeutend mit $\rho_n = \rho_n^{-1}$, was aber wegen $\mathrm{ord}(\rho_n) > 2$ nicht der Fall ist. Also gilt tatsächlich $|NU| = 2n$.

Nun zeigen wir noch, dass D_n mit NU übereinstimmt. Offenbar ist NU in D_n enthalten, denn mit ρ_n und τ_n enthält D_n auch alle Produkte, die mit ρ_n und τ_n gebildet werden können. Es genügt nun zu zeigen, dass NU eine Untergruppe von D_n (und somit auch von S_n) ist, denn NU enthält ρ_n und τ_n, und D_n ist nach Definition die *kleinste* Untergruppe mit dieser Eigenschaft. Das Neutralelement ist wegen $\rho_n^0 \tau_n^0 = \mathrm{id}$ jedenfalls in NU enthalten. Seien nun $\sigma_1, \sigma_2 \in NU$ vorgegeben. Dann gibt es $a, c \in \{0, \ldots, n-1\}$ und $b, d \in \{0, 1\}$ mit $\sigma_1 = \rho_n^a \tau_n^b$ und $\sigma_2 = \rho_n^c \tau_n^d$. Ist $b = 0$, dann sind $\sigma_1 \sigma_2 = \rho_n^{a+c} \tau_n^d$ und $\sigma^{-1} = \rho_n^{-a}$ offenbar wiederum in NU enthalten. Im Fall $b = 1$ bemerken wir, dass aus der Gleichung $\tau_n \circ \rho_n \circ \tau_n^{-1} = \rho_n^{-1}$ von oben durch vollständige Induktion unmittelbar $\tau_n \circ \rho_n^\nu = \rho_n^{-\nu} \circ \tau_n$ für alle $\nu \in \mathbb{N}$ folgt. Auf Grund der endlichen Ordnung von ρ_n ist die Gleichung sogar für alle $\nu \in \mathbb{Z}$ gültig. Es gilt nun

$$\sigma_1^{-1} \quad = \quad (\rho_n^a \circ \tau_n)^{-1} \quad = \quad \tau_n^{-1} \circ \rho_n^{-a} \quad = \quad \tau_n \circ \rho_n^{-a} \quad = \quad \rho_n^a \circ \tau_n \quad = \quad \sigma_1 \quad ,$$

also $\sigma_1^{-1} \in NU$. Auch das Element $\sigma_1 \circ \sigma_2$ ist wegen

$$\sigma_1 \circ \sigma_2 \quad = \quad \rho_n^a \circ \tau_n \circ \rho_n^b \circ \tau_n^d \quad = \quad \rho_n^a \circ \rho_n^{-b} \circ \tau_n \circ \tau_n^d \quad = \quad \rho_n^{a-b} \circ \tau_n^{d+1}$$

im Komplexprodukt NU enthalten. Also ist NU tatsächlich eine Untergruppe von D_n. □

Definition 5.7 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 5.8 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 $nun^{-1}n^{-1}$ 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 $u_1 n_2 = n_2 u_1$ erhalten wir

$$\phi(u_1, n_1)\phi(u_2, n_2) \quad = \quad (u_1 n_1)(u_2 n_2) \quad = \quad u_1(n_1 u_2)n_2 \quad = \quad u_1(u_2 n_1)n_2 \quad =$$

$$(u_1 u_2)(n_1 n_2) \quad = \quad \phi(u_1 u_2, n_1 n_2) \quad = \quad \phi((u_1, n_1)(u_2, n_2)).$$

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 5.5. □

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 5.5. 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.

Sei G eine Gruppe. Bereits in § 4 haben wir für eine beliebige Untergruppe U die Menge $G/U = \{gU \mid g \in G\}$ der Linksnebenklassen eingeführt. Da es für das Verständnis des restlichen Abschnitts eine wichtige Rolle spielt, weisen wir noch einmal darauf hin, dass für beliebige Elemente $g, h \in G$ die Identität $gU = hU$ äquivalent zu $g^{-1}h \in U$ oder (gleichbedeutend) zu $h^{-1}g \in U$ ist, aber keineswegs $g = h$ impliziert!

Proposition 5.9 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 4.10 (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 $n' = h^{-1}n_1 h$ in N enthalten. Stellen wir diese Gleichung zu $n_1 h = hn'$ 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 5.10 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

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

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 $a \in \mathbb{Z}$. Der Einfachheit halber schreibt man häufig $\bar{a}$ für das Element $a + n\mathbb{Z}$, dass die Zahl n aus dem Zusammenhang heraus klar ist. Für $a, b \in \mathbb{Z}$ gilt $a + n\mathbb{Z} = b + n\mathbb{Z}$ jeweils genau dann, wenn $b - a \in n\mathbb{Z}$ oder $a - b \in n\mathbb{Z}$ gilt. Daraus folgt

$$\mathbb{Z}/n\mathbb{Z} \quad = \quad \{r + n\mathbb{Z} \mid 0 \leq r < n\}.$$

Die Inklusion „$\subseteq$“ ist nach Definition von $\mathbb{Z}/n\mathbb{Z}$ offensichtlich. Ist umgekehrt $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ vorgegeben, mit $a \in \mathbb{Z}$, dann erhält man durch Division mit Rest ganze Zahlen q, r mit $0 \leq r < n$ und $a = qn + r$. Es ist dann $a - r = qn \in n\mathbb{Z}$ und folglich $a + n\mathbb{Z} = r + n\mathbb{Z}$. Wir bemerken noch, dass $(\mathbb{Z}/n\mathbb{Z}, +)$ eine zyklische Gruppe ist und vom Element $1 + n\mathbb{Z}$ erzeugt wird. Dies erkennt man an der Gleichung

$$a + n\mathbb{Z} \quad = \quad (a \cdot 1) + n\mathbb{Z} \quad = \quad a \cdot (1 + n\mathbb{Z}) \qquad \text{für beliebiges } a \in \mathbb{Z}.$$

Für $1 \leq a < n$ gilt nämlich $a \notin n\mathbb{Z}$ und somit $a \cdot (1 + n\mathbb{Z}) \neq 0 + n\mathbb{Z}$. Andererseits gilt $n \cdot (1 + n\mathbb{Z}) = 0 + \mathbb{Z}$. Somit ist $1 + n\mathbb{Z}$ ein Element der Ordnung n, dass die gesamte Gruppe $\mathbb{Z}/n\mathbb{Z}$ erzeugt. Wir bemerken noch, dass jede zyklische Grupper der Ordnung n isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$ ist. Dies ergibt sich unmittelbar aus Folgerung 3.13.

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 5.11 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

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

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 4.10 an, diesmal Teil (i). Demnach genügt es zu zeigen, dass für alle $g, g' \in G$ mit $g \equiv_\ell g'$ jeweils $\phi(g) = g'$ 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

$$\bar{\phi}(\bar{g}\bar{h}) \quad = \quad \bar{\phi}((gN)(hN)) \quad = \quad \bar{\phi}((gh)N) \quad = \quad \phi(gh) \quad = \quad \phi(g)\phi(h) \quad = \quad \bar{\phi}(gN)\bar{\phi}(hN) \quad = \quad \bar{\phi}(\bar{g})\bar{\phi}(\bar{h}).$$

□

Satz 5.12 *(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 5.3 (iii) ist $N = \ker(\phi)$ ein Normalteiler von G. Anwendung von Proposition 5.11 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 $\bar{g} \in \ker(\bar{\phi})$, 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 2.4 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 $a, 1, \ldots, 1$. Somit liefert der Homomorphiesatz einen Isomorphismus $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^\times$.

(iv) Die Signumsfunktion $\operatorname{sgn} : S_n \to \{\pm 1\}$ hat als Kern die Untergruppe $A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$, die bereits aus der Linearen Algebra bekannte alternierende Gruppe. Außerdem ist sie für $n \geq 2$ surjektiv, wegen $\operatorname{sgn}(\mathrm{id}) = 1$ und $\operatorname{sgn}((1\ 2)) = -1$. 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 5.13 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 5.14 *(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 $\bar{\mathscr{G}}$ die Menge der Untergruppen von $\bar{G}$ und $\mathscr{G}_N$ die Menge der Untergruppen U von G mit $U \supseteq N$. Dann sind die beiden Abbildungen

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

bijektiv und zueinander invers. Außerdem gilt:

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

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

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

Beweis: Sei $U \in \mathscr{G}_N$, 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 5.13 (i), im zweiten Lemma 5.5 (ii) und im dritten Lemma 5.5 (i) verwendet haben. Umgekehrt liefert Teil (ii) von Proposition 5.13 die Gleichung $\pi_N(\pi_N^{-1}(\bar{U})) = \bar{U}$ für alle Untergruppen $\bar{U}$ von $\bar{G}$.

zu (i) Seien $U, V \in \mathscr{G}_N$ 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 5.3 (iv) bzw. (iii).

zu (iii) Wir zeigen, dass durch $\bar{g}\bar{U} \mapsto \pi_N^{-1}(\bar{g}U)$ 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 $(\mathbb{Z}/44\mathbb{Z}, +)$ isteine zyklische Gruppe der Ordnung 44. Durch Satz 3.10 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 5.15 *(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 5.5 eine Untergruppe von G ist, und aus $N \trianglelefteq G$ folgt $N \trianglelefteq UN$. Wir wenden nun den Homomorphiesatz, Satz 5.12, 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 5.3 (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 5.15 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 $\bar{m} = m + n\mathbb{Z}$.

§ 6. *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

- Torsionsuntergruppe $\mathrm{Tor}(G)$ (G abelsche Gruppe)
- m-Torsionsuntergruppe $G[m]$, für $m \in \mathbb{N}$
- torsionsfreie und freie endlich erzeugte abelsche Gruppen

Zentrale Sätze

- Zerlegung $\mathbb{Z}^r \times \mathrm{Tor}(G)$ endlich erzeugter abelscher Gruppen in einen freien Anteil und einen Torsionsanteil
- Endlichkeit von $\mathrm{Tor}(G)$ für solche Gruppen
- Jede endlich erzeugte abelsche Gruppe G ist isomorph zu einem direkten Produkt zyklischer Gruppen.
- Chinesischer Restsatz: $\mathbb{Z}/(mn)\mathbb{Z}\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, falls $\mathrm{ggT}(m,n) = 1$

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 6.1 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 2.3 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. Eine wichtige Rolle wird in diesem Kapitel das innere direkte Produkt aus § 5 spielen, weshalb wir auch hierfür eine Notation einführen: 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 6.2 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 6.3 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 6.4

(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) Zunächst beweisen wir durch vollständige Induktion über $n \in \mathbb{N}_0$, dass für jedes solche n jede Untergruppe von $\mathbb{Z}^n$ eine freie endlich erzeugte abelsche Gruppe ist. Für $n = 0$ ist $\mathbb{Z}^n = \{0\}$ trivial und die Aussage somit offensichtlich. Für $n = 1$ können wir Satz 3.6 anwenden, weil $(\mathbb{Z}, +)$ zyklisch ist. Jede Untergruppe von $(\mathbb{Z}, +)$ ist demnach stimmt demnach mit $m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$ überein, ist also selbst entweder unendlich zyklisch oder trivial, also isomorph zu $\mathbb{Z}^0$ oder $\mathbb{Z}^1$.

Sei nun $n \geq 1$ und U eine Untergruppe von $(\mathbb{Z}^{n+1}, +)$. Es sei $\pi : \mathbb{Z}^{n+1} \to \mathbb{Z}$ die Projektionsabbildung $\pi(a_1, ..., a_{n+1}) = a_{n+1}$ auf die letzte Komponente. Dann ist $\pi(U)$ eine Untergruppe von $\mathbb{Z}$ und somit, wie soeben gezeigt, gleich $m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$ und isomorph zu $\mathbb{Z}^t$ mit $t \in \{0, 1\}$. 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 $r \in \mathbb{N}_0$. Wenn wir zeigen können, dass $U \cong \ker(\pi|_U) \times \pi(U)$ gilt, dann folgt $U \cong \mathbb{Z}^r \times \mathbb{Z}^t = \mathbb{Z}^{r+t}$. Somit wäre U dann auch eine freie endlich erzeugte abelsche Gruppe.

Sei $v \in U$ ein Element mit $\pi(v) = m$, wobei wir $v = 0_{\mathbb{Z}^{n+1}}$ im Fall $m = 0$ setzen. Dann bildet π offenbar die Gruppe $\langle v \rangle$ isomorph auf $\pi(U) = m\mathbb{Z}$ ab. Wie wir gleich sehen werden, gilt $U = \ker(\pi|_U) \oplus \langle v \rangle$. Nach Proposition 5.8 folgt daraus $U \cong \ker(\pi|_U) \times \langle v \rangle \cong \ker(\pi|_U) \times \pi(U)$, so dass der Induktionsssschritt damit abgeschlossen 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 $m = 0_{\mathbb{Z}^{n+1}}$ oder $k = 0$. In beiden Fällen ist $w = kv = 0_{\mathbb{Z}^{n+1}}$ erfüllt. 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.

Sei nun G eine beliebige endlich erzeugte freie abelsche Gruppe und U eine Untergruppe von G. Dann existiert ein $n \in \mathbb{N}_0$ und ein Isomorphismus $\phi : G \to \mathbb{Z}^n$. Weil $\pi(U)$ eine Untergruppe von $\mathbb{Z}^n$ ist, gilt (wie soeben gezeigt) $\pi(U) \cong \mathbb{Z}^r$ für ein $r \in \mathbb{N}_0$. Es folgt $U \cong \pi(U) \cong \mathbb{Z}^r$, also ist auch U eine endlich erzeugte freie abelsche Gruppe.

zu (ii) Sei G eine torsionsfreie endlich erzeugte abelsche Gruppe. Weiter sei S ein endliches Erzeugendensystem und $T = \{g_1, ..., g_n\} \subseteq S$ eine *maximale* Teilmenge von S mit der Eigenschaft, dass die Abbildung $\phi : \mathbb{Z}^n \to G$, $(a_1, ..., a_n) \mapsto a_1 g_1 + ... + a_n g_n$ 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 $(a, a_1, ..., a_n)$ ganzer Zahlen mit $ag + a_1 g_1 + ... + a_n g_n = 0_G$ und $a \neq 0$, $a_i \neq 0$ für ein $i \in \{1, ..., n\}$. Wegen $ag = -a_1 g_1 - ... - a_n g_n$ ist dann ag in U enthalten. Auf diese Weise erhalten wir für jedes $g \in S$ ein $a_g \in \mathbb{Z}$ mit $a_g g \in U$, 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 6.5 Ist G eine endlich erzeugte abelsche Gruppe, dann gibt es ein $r \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$. 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 6.4 (ii). Sei ϕ die Komposition des kanonischen Epimorphismus $G \to G/\mathrm{Tor}(G)$ mit diesem Isomorphismus, seien $v_1, ..., v_r$ Urbilder der Einheitsvektoren $e_1, ..., e_r \in \mathbb{Z}^r$ unter ϕ, und sei $U = \langle v_1, ..., v_r \rangle$. 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 $k_1, ..., k_r \in \mathbb{Z}$ mit $g = k_1 v_1 + ... + k_r v_r$. Es folgt $mg = mk_1 v_1 + ... + mk_r v_r$ und $0_{\mathbb{Z}^r} = \phi(mg) = mk_1 e_1 + ... + mk_r e_r = (mk_1, ..., mk_r)$. 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 $(k_1, ..., k_r) = \phi(g)$, $h = k_1 v_1 + ... + k_r v_r$ und $g' = g - h$. Dann ist $g = g' + h$, $h \in U$ und $\phi(g') = \phi(g) - \phi(h) = (k_1, ..., k_r) - (k_1, ..., k_r) = 0_{\mathbb{Z}^r}$, 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 5.8 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 6.1 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

$$\mathrm{Tor}(G) \quad = \quad \{k_1 h_1 + ... + k_s h_s \mid k_1, ..., k_s \in \mathbb{Z}\} \quad = \quad \{k_1 h_1 + ... + k_s h_s \mid 0 \le k_i < m_i\}.$$

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 6.6

(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

$$\phi(\bar{a}_1, ..., \bar{a}_s) \quad = \quad a_1 g_1 + ... + a_s g_s \qquad \text{für alle} \quad a_1, ..., a_s \in \mathbb{Z}.$$

(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 $\phi(\bar{a}_1, ..., \bar{a}_s) = a_1 g_1 + ... + a_r g_r$ 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 $a_i = q_i m_i + r_i$ mit $0 \le r_i < m_i$, dann gilt auf Grund der Elementordnungen jeweils $m_i g_i = 0_G$ und somit $a_i g_i = (q_i m_i + r_i) g_i = q_i (m_i g_i) + r_i a_i = q_i \cdot 0_G + r_i a_i = r_i a_i$. 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 6.7 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 5.8 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 3.7 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 6.8 *(Chinesischer Restsatz)*
Sind $m,n \in \mathbb{N}$ teilerfremd, dann gilt $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

In der Zahlentheorie-Vorlesung wird gezeigt, dass $\mathbb{Z}/(mn)\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ als Ringe isomorph sind. Damit sind insbesondere die additiven Gruppen zueinander isomorph. Man kann den Isomorphismus mit den hier zur Verfügung

stehenden Mitteln auch leicht direkt zeigen. Die Gruppe $G = \mathbb{Z}/(mn)\mathbb{Z}$ ist eine zyklische Gruppe der Ordnung mn, mit $\bar{1}$ als Erzeuger, und wegen $|G| = mn$ gilt $(mn)g = 0_G$ für alle $g \in G$, also $G[mn] = G$. Nach Satz 6.7 (i) ist G also isomorph zu $G[m] \times G[n]$. Ist $a \in \mathbb{Z}$ und $\bar{a}$ das Bild in G, dann ist $m\bar{a} = \bar{0}$ äquivalent zu $mn \mid ma \Leftrightarrow n \mid a \Leftrightarrow \bar{a} \in \langle \bar{n} \rangle$. Es gilt also $G[m] = \langle \bar{n} \rangle$. Weil $\bar{n} = n \cdot \bar{1}$ wegen $\mathrm{ord}(\bar{1}) = mn$ nach Satz 3.8 ein Element der Ordnung m ist, gilt $G[m] \cong \mathbb{Z}/m\mathbb{Z}$. Genauso erhält man $G[n] \cong \mathbb{Z}/n\mathbb{Z}$. Insgesamt ist damit $G \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ nachgewiesen.

Man beachten, 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 6.9 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 6.6 (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 6.6 (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 5.8. 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 6.10 *(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 $1\le i<s$ erfüllt ist. Im Fall (ii) gezeichnet man die Zahlen d_i als ***Elementarteiler*** der abelschen Gruppe.

Beweis: Nach Satz 6.5 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 6.7 (ii), und wegen Satz 6.9 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).

In der Zahlentheorie-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 $\prod_{j=1}^v p_j^{f_j}$ 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 6.8, 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 $1\le i\le s$. 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 6.10 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.

§ 7. Semidirekte Produkte und Auflösbarkeit

Zusammenfassung. In § 5 hatten wir die inneren direkten Produkte definiert. Lässt man die Forderung der Normalteiler-Eigenschaft für einen der Faktoren fallen, so spricht man von inneren *semidirekten* Produkten. Der Isomorphismus $G \cong N \times U$ aus § 5 ist dann nicht mehr gültig; an die Stelle des äußeren direkten Produkts tritt eine neue Gruppe $N \rtimes_\phi U$, die als Menge mit $N \times U$ übereinstimmt, deren Gruppenverknüpfung aber nicht komponentenweise definiert wird, 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 § 5 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 § 6 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. In vielen Fällen lässt sich dies aber zumindest in endlich vielen Schritten bewerkstelligen, also indem man in N und G/N wiederum nach Normalteilern sucht und diese Prozedur hinreichend oft wiederholt. Gruppen, die auf diese Weise in lauter abelsche „Komponenten“ zerlegt werden können, bezeichnet man als *auflösbar*. In der Galoistheorie werden wir sehen, dass ein Zusammenhang zwischen auflösbaren Gruppen und der expliziten Lösbarkeit von Polynomgleichungen existiert, ein Umstand, der ebenfalls zur Namensgebung beigetragen hat.

Wichtige Grundbegriffe

- inneres semidirektes Produkt (von $U \leq G$ und $N \trianglelefteq G$)
- äußeres semidirektes Produkt $U \rtimes_\phi N$ (wobei U, N Gruppe und $\phi : U \to \mathrm{Aut}(N)$ Homomorphismus)
- Normalisator einer Untergruppe
- höhere Kommutatorgruppen $G^{(n)}$ einer Gruppe G
- Auflösbarkeit einer Gruppe

Zentrale Sätze

- Jedes innere semidirekte Produkt von $U \leq G$ und $N \trianglelefteq G$ definiert einen Homomorphismus $\phi : U \to \mathrm{Aut}(N)$.
- Isomorphie zwischen innerem und äußerem semidirekten Produkt
- Charakterisierung auflösbarer Gruppen durch Normalreihen
- 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 N 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 7.1 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

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

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 7.2 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 7.1 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 7.3 Seien U und N Gruppen und $\phi : U \to \mathrm{Aut}(N)$ ein Homomorphismus. Wir definieren auf $N \times U$ eine Verknüpfung $*$ durch

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

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

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

Nun überprüfen wir, dass (e_N, e_U) ein bezüglich $*$ neutrales Element ist. Für jedes $(n,u) \in N \times U$ gilt $(e_N, e_U) * (n,u) = (e_N \phi(e_U)(n), e_U u) = (e_N n, e_U u) = (n,u)$ 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 7.3 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 Definition 1.14 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 den Zusammenhang zwischen inneren und äußeren direkten Produkten her.

Satz 7.4 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 7.1, 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 7.1 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 $\psi((n_1,u_1)*(n_2,u_2)) = \psi(n_1\phi(u_1)(n_2),u_1u_2) = n_1\phi(u_1)(n_2)u_1u_2$. □

In § 2 hatten wir die Diedergruppen D_n eingeführt. Die semidirekten Produkte liefern einen neuen Ansatz zum Verständnis dieser Gruppen. Zunächst benötigen wir einen neuen Begriff.

Definition 7.5 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 7.6 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: Zunächst überprüfen wir, dass $N_G(U)$ eine Untergruppe von G ist. Wegen $eUe^{-1} = U$ ist e in $N_G(U)$ enthalten. Seien nun $g,h \in N_G(U)$ vorgegeben. Dann gilt $(gh)U(gh)^{-1} = g(hUh^{-1})g^{-1} = gUg^{-1} = U$, also ist auch gh in $N_G(U)$ enthalten. Die Rechnung $g^{-1}Ug = g^{-1}(gUg^{-1})g = (g^{-1}g)U(g^{-1}g) = eUe = U$ zeigt, dass auch $g^{-1} \in U$ gilt.

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. □

Wie im Beispiel oben sei wieder $\iota : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ der Automorphismus der Gruppe $(\mathbb{Z}/n\mathbb{Z},+)$ gegeben durch $\iota(\bar{a}) = -\bar{a}$, und es sei $\phi_n : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ Homomorphismus gegeben durch $\phi_n(\bar{0}) = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$ und $\phi_n(\bar{1}) = \iota$.

Proposition 7.7 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 zum äußeren semidirekten Produkt $\mathbb{Z}/n\mathbb{Z} \rtimes_{\phi_n} \mathbb{Z}/2\mathbb{Z}$.

Beweis: Zunächst zeigen wir, dass $\langle g \rangle$ ein Normalteiler von G ist. Dazu zeigen wir, dass für den Normalisator dieser Gruppe $N_G(\langle g \rangle) = G$ gilt. Wegen $g \in \langle g \rangle$ ist g auf jeden Fall im Normalisator enthalten. Weil die Konjugationsabbildung $\tau_h : G \to G$, $g_1 \mapsto hg_1h^{-1}$ ein Automorphismus von G ist, und auf Grund der Gleichung $hgh^{-1} = g^{-1}$, gilt für jedes $a \in \mathbb{Z}$ auch $hg^ah^{-1} = \tau_h(g^a) = \tau_h(g)^a = (hgh^{-1})^a = (g^{-1})^a = g^{-a} \in \langle g \rangle$ und somit $h\langle g \rangle h^{-1} \subseteq \langle g \rangle$.

Wegen $h = h^{-1}$ folgt daraus unmittelbar auch $h^{-1}\langle g\rangle h \subseteq \langle g\rangle \Leftrightarrow \langle g\rangle \subseteq h\langle g\rangle h^{-1}$ und insgesamt $h\langle g\rangle h^{-1} = \langle g\rangle$, also $h \in N_G(\langle g\rangle)$. Aus $\{g,h\} \subseteq N_G(\langle g\rangle)$ folgt nun $G = \langle g,h\rangle \subseteq N_G(\langle g\rangle)$ und somit $N_G(\langle g\rangle) = G$. Damit ist der Nachweis von $\langle g\rangle \trianglelefteq G$ abgeschlossen.

Da $\langle g\rangle$ eine Normalteiler und $\langle h\rangle$ eine Untergruppe von G ist, handelt es sich auch bei $U = \langle g\rangle\langle h\rangle$ um eine Untergruppe von G. Wegen $g,h \in U$ gilt $G = \langle g,h\rangle \subseteq U$ und somit $G = U = \langle g\rangle\langle h\rangle = \{g^a h^b \mid a,b \in \mathbb{Z}\}$. Wegen $\mathrm{ord}(g) = n$ und $\mathrm{ord}(h) = 2$ sind die Elemente von G bereits durch $g^a h^b$ mit $0 \leq a < n$ und $b \in \{0,1\}$ gegeben. Wir zeigen, dass diese Elemente voneinander verschieden sind. Gilt $g^a h^b = g^c h^d$ mit $0 \leq a,c < n$ und $b,d \in \{0,1\}$, dann folgt $g^{a-c} = h^{d-b} \in \langle g\rangle \cap \langle h\rangle$. Außerdem ist $\langle g\rangle \cap \langle h\rangle = \{e\}$. Denn ansonsten wäre $h \in \langle g\rangle$, und weil zyklische Gruppen abelsch sind, würde daraus $g = (hh^{-1})g = hgh^{-1} = g^{-1}$ und somit $g^2 = e$ folgen, im Widerspruch zu $\mathrm{ord}(g) \geq 3$. Also ist G eine Gruppe der Ordnung $2n$, und jedes Element aus G hat eine eindeutige Darstellung der Form $g^a h^b$ mit $0 \leq a < n$ und $b \in \{0,1\}$.

Die Eindeutigkeit der Darstellung zeigt, dass die Abbildung $\psi : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G, (\bar{a},\bar{b}) \mapsto g^a h^b$ wohldefiniert und bijektiv ist. Wir weisen jetzt nach, dass sie darüber hinaus ein Gruppenhomomorphismus zwischen $\mathbb{Z}/n\mathbb{Z} \rtimes_{\phi_n} \mathbb{Z}/2\mathbb{Z}$ und G ist, wodurch der Beweis dann insgesamt abgeschlossen wird. Seien $a,b,c,d \in \mathbb{Z}$ vorgegeben und $\bar{a},\bar{c} \in \mathbb{Z}/n\mathbb{Z}$ sowie $\bar{b},\bar{d} \in \mathbb{Z}/2\mathbb{Z}$ die entsprechenden Bildelemente. Wegen $\tau_h(g) = g^{-1}$ gilt $\tau_h^b(g) = g^{(-1)^b}$ und $h^b g^c h^{-b} = \tau_h^b(g^c) = \tau_h^b(g)^c = (g^{(-1)^b})^c = g^{(-1)^b c}$, woraus $(g^a h^b)(g^c h^d) = g^a(h^b g^c h^{-b})h^{b+d} = g^a g^{(-1)^b c} h^{b+d} = g^{a+(-1)^b c} h^{b+d}$ folgt. Andererseits gilt nach Definition der Verknüpfung im äußeren semidirekten Produkt

$$(\bar{a},\bar{b}) * (\bar{c},\bar{d}) \quad = \quad (\bar{a} + \phi_n(\bar{b})(\bar{c}), \bar{b}+\bar{d}) \quad = \quad (\bar{a} + \iota^b(\bar{c}), \bar{b}+\bar{d}) \quad = \quad (\bar{a} + (-1)^b\bar{c}, \bar{b}+\bar{d}).$$

Insgesamt erhalten wir $\psi((\bar{a},\bar{b}) * (\bar{c},\bar{d})) = \psi(\bar{a} + (-1)^b\bar{c}, \bar{b}+\bar{d}) = g^{a+(-1)^b c} h^{b+d} = (g^a h^b)(g^c h^d) = \psi(\bar{a},\bar{b})\psi(\bar{c},\bar{d})$, wie gewünscht. □

Folgerung 7.8 Für alle $n \in \mathbb{N}$ mit $n \geq 3$ gilt $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\phi_n} \mathbb{Z}/2\mathbb{Z}$.

Beweis: Nach Definition gilt $D_n = \langle \sigma_n, \tau_n\rangle$, außerdem ist $\mathrm{ord}(\sigma_n) = n$ und $\mathrm{ord}(\tau_n) = 2$. Wie wir schon in § 5 beim Beweis von Proposition 5.6 festgestellt haben, gilt $\tau_n \circ \sigma_n \circ \tau_n^{-1} = \rho_n^{-1}$, was zu $\sigma_n\tau_n\sigma_n\tau_n = \mathrm{id}$ umgeformt werden kann. Damit sind alle Bedingungen von Proposition 7.7 verifiziert, und es folgt $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\phi_n} \mathbb{Z}/2\mathbb{Z}$. □

Kommen wir nun zum zweiten Thema dieses Kapitels, den auflösbaren Gruppen.

Definition 7.9 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 7.10 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 7.10 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 7.11 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 7.9 gesehen haben.

Definition 7.12 Eine ***Normalreihe*** 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 Normalreihe. Sind alle Faktoren abelsch, dann spricht man von einer ***abelschen Normalreihe***.

Proposition 7.13 Jede endliche abelsche Gruppe besitzt eine Normalreihe 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 6.10 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 Normalreihe mit zyklischen Faktoren, so dass wir insgesamt eine solche Reihe für G erhalten. □

Satz 7.14 Für eine endliche Gruppe G sind die folgenden Eigenschaften äquivalent.

(i) Die Gruppe G ist auflösbar.

(ii) Sie besitzt eine abelsche Normalreihe.

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

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

Beweis: Sei G zunächst ein beliebige, möglicherweise unendliche Gruppe. „(i) ⇒ (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 7.10 festgestellt, 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 Normalreihe mit abelschen Faktoren.

„(ii) ⇒ (i)“ Sei $G_0, ..., G_r$ eine Normalreihe 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 7.10 (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) ⇒ (ii)“ ist offenbar gültig, da zyklische Gruppen stets abelsch sind (siehe § 2). Beweisen wir nun „(ii) ⇒ (iii)“ und setzen dazu voraus, dass $G_0, ..., G_r$ eine Normalreihe 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 7.13 besitzt diese eine Normalreihe $\bar{U}_0, ..., \bar{U}_s$ 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 5.14 (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 5.15 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 Normalreihe 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 7.15

(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 7.15 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.

§ 8. Gruppenoperationen

Zusammenfassung. Eine Hauptmotivation für die Gruppentheorie als Teilgebiet der Algebra ist die Tatsache, dass viele Gruppen als Symmetrieoperationen auf geometrischen oder algebraischen Strukturen in Erscheinung treten. Beispielsweise wirkt die orthogonale Gruppe $\mathrm{O}(3) = \{A \in \mathrm{GL}_3(\mathbb{R}) \mid {}^tAA = E_3\}$ und Drehungen und Spiegelungen auf dem dreidimensionalen Raum. Ist X allgemein eine Struktur und G eine Gruppe, und kann jedem Element $g \in G$ eine auf natürliche Weise eine strukturerhaltende Abbildung $X \to X$ zugeordnet werden, dann spricht man von einer *Operation* der Gruppe G auf der Struktur X.

In den einfachsten Situationen handelt sich bei X lediglich um eine Menge, und die strukturerhaltenden Abbildungen $X \to X$ sind nichts weiter als Bijektionen. Wir werden im vorliegenden Abschnitt diesen Typ von Gruppenoperationen präzise definieren und eine fundamentale Gesetzmäßigkeiten herleiten. Beispielsweise werden wir sehen, dass die Gruppenoperation eine Zerlegung der Menge X in sog. *Bahnen* bewirkt, deren Länge im Fall einer endlichen Gruppe stets ein Teiler der Gruppenordnung ist. Dies führt uns auf die sog. *Bahngleichung* für Gruppenoperationen. Lässt man eine Gruppe auf geeignete Weise auf sich selbst operieren, so folgen aus der Bahngleichung, die in dieser Situation *Klassengleichung* genannt wird, eine Reihe interessanter gruppentheoretischer Sätze. Dazu zählt die Kommutativität aller Gruppen von Primzahlquadratordnung, und die Auflösbarkeit aller Gruppen von Primzahlpotenzordnung.

Ein andere Typ von Gruppenoperationen ermöglicht es uns, den *Satz von Cayley* zu beweisen, welcher besagt, dass jede endliche Gruppe bis auf Isomorphie als Untergruppe einer symmetrischen Gruppe vorkommt. Hätte man also die Struktur der symmetrischen Gruppen S_n vollständig aufgeklärt, dann wüsste man also auch über alle anderen endlichen Gruppen vollständig Bescheid! Leider ist die Struktur der S_n für großes n so kompliziert, dass dieses Resultat in konkreten Situationen keine nennenswerte Vereinfachung mit sich bringt.

Wichtige Grundbegriffe

- Operation einer Gruppe G auf einer Menge X
- Bahnen und Fixpunkte einer Operation
- Repräsentantensysteme der Bahnen

Zentrale Sätze

- Untergruppeneigenschaft des Stabilisators G_x
- Zerlegung von X durch die Bahnen einer Operation
- Zusammenhang $(G : G_x) = |G(x)|$ zwischen Bahnlänge und Stabilisator
- Zusammenhang zwischen Operationen von G auf X und Homomorphismen $G \to \mathrm{Per}(X)$
- Satz von Cayley
- Bahngleichung für Gruppenoperationen auf endlichen Mengen
  Klassengleichung als Spezialfall
- Anwendungen: Auflösbarkeit von p-Gruppen, Gruppen der Ordnung p^2 sind abelsch

Definition 8.1 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. Man sagt auch, dass G mittels α auf X ***operiert***.

An Stelle von $\alpha(g, x)$ schreibt man häufig auch einfach $g \cdot x$. 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 $v \in V$.

Nun schauen wir uns an, durch welche Merkmale eine Gruppenoperation genauer beschrieben werden kann.

Definition 8.2 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.

Allgemein bezeichnet man eine Teilmenge $Y \subseteq X$ als ***G-invariant***, wenn für alle $g \in G$ und $y \in Y$ jeweils $g \cdot y \in Y$ gilt. Dies ist gleichbedeutend mit $G(y) \subseteq Y$ für alle $y \in Y$. In diesem Fall kann die Gruppenoperation $\cdot$ zu einer Abbildung

$$\cdot : G \times Y \longrightarrow Y \quad , \quad (g, y) \mapsto g \cdot y$$

eingeschränkt werden, und man erhält eine Gruppenoperation von G auf Y. Offenbar ist jede Bahn einer Gruppenoperation G-invariant, ebenso jede Vereinigung von Bahnen.

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

Beweis: Wir überprüfen die in § 4, direkt im Anschluss an Lemma 4.2 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 $z \in G(x)$. □

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 8.4 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 (i) 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 8.5 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 8.6 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 4.10 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 $\bar{g} = gG_x = g(g^{-1}h)G_x = hG_x = \bar{h}$. □

Ist inbesondere G eine endliche Gruppe, dann ist also die Länge $|G(x)|$ jeder Bahn stets ein ***Teiler der Gruppenordnung*** $|G|$. Denn nach dem Satz von Lagrange ist $(G : G_x)$ ein Teiler von $|G|$, und nach Satz 8.6 gilt $|G(x)| = (G : G_x)$.

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 8.7 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.

Proposition 8.8 Sei G eine Gruppe. Dann ist durch $G \times G \to G$, $g \cdot h = gh$ eine Gruppenoperation von G auf sich definiert. Man bezeichnet diese als Operation durch ***Linkstranslation***.

Beweis: Wir überprüfen, dass die definierenden Gleichungen einer Gruppenoperation erfüllt sind: Für alle $h \in G$ gilt $e_G \cdot h = e_G = h$. Sind $g_1, g_2 \in G$ vorgegeben, dann ist $g_1 \cdot (g_2 \cdot h) = g_1 \cdot (g_2 h) = g_1(g_2 h) = (g_1 g_2)h = (g_1 g_2) \cdot h$. □

Satz 8.9 *(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: Nach Proposition 8.8 operiert G durch Linkstranslation auf sich selbst, und nach Satz 8.7 ist durch $g \mapsto \tau_g$, $\tau_g(h) = g \cdot h$ ein Homomorphismus $\Psi : G \to \mathrm{Per}(G)$ definiert. Dieser Homomorphismus ist injektiv. Sei nämlich $g \in G$ mit $\Psi(g) = \tau_g = \mathrm{id}_G$ vorgegeben. Dann gilt insbesondere $g = g e_G = \tau_g(e_G) = \mathrm{id}_G(e_G) = e_G$. Damit ist die Injektivität von Ψ bewiesen.

Darüber hinaus gibt es wegen $|G| = n$ eine Bijektion $\phi : M_n \to G$, wobei $M_n = \{1, \ldots, n\}$ ist. Wie man leicht überprüft, gilt $\phi \circ \sigma \circ \phi^{-1} \in \mathrm{Per}(G)$ für alle $\sigma \in S_n$, und $\Phi : S_n \to \mathrm{Per}(G)$, $\sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$ ist ein Isomorphismus von Gruppen. Ingesamt ist $\Phi^{-1} \circ \Psi : G \to S_n$ also ein Monomorphismus, der einen Isomorphismus zwischen G und der Untergruppe $(\Phi^{-1} \circ \Psi)(G)$ von S_n definiert. □

Wenden wir uns nun als nächstem Thema der Formulierung der Bahngleichung zu.

Definition 8.10 Sei G eine Gruppe, die auf einer Menge X operiert, $\mathscr{B}$ die Menge der Bahnen dieser Operation und $\mathscr{S} \subseteq \mathscr{B}$ eine Teilmenge. Eine Teilmenge $R \subseteq X$ wird ***Repräsentantensystem*** von $\mathscr{S}$ genannt, wenn $G(x) \in \mathscr{S}$ für alle $x \in R$ gilt und die Abbildung $R \to \mathscr{S}$, $x \mapsto G(x)$ bijektiv ist.

Damit erhalten wir im Fall einer endlichen Menge X

Satz 8.11 *(Bahngleichung)*

Sei G eine Gruppe, die auf einer endlichen Menge X operiert. Sei $F \subseteq X$ die Fixmpunktmenge 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 $\mathscr{B}$ die Menge aller Bahnen, $\mathscr{S} \subseteq \mathscr{B}$ die Teilmenge aller Bahnen der Länge > 1 und $R \subseteq X$ ein Repräsentantensystem von $\mathscr{S}$. Weil die einelementigen Bahnen genau die Mengen $\{x\}$ mit $x \in F$ sind, ist $F \cup R$ ein

Repräsentantensystem von $\mathscr{B}$, und die Mengen R und F sind disjunkt. Weil X die disjunkte Vereinigung der Mengen aus $\mathscr{B}$ ist und nach Definition des Repräsentantensystems für jedes $B \in \mathscr{B}$ genau ein $x \in F \cup R$ mit $B = G(x)$ existiert, gilt

$$\begin{aligned} |X| &= \sum_{B\in\mathscr{B}} |B| = \sum_{x\in F\cup R} |G(x)| = \sum_{x\in F} |G(x)| + \sum_{x\in R} |G(x)| \\ &= \sum_{x\in F} |\{x\}| + \sum_{x\in R} |G(x)| = |F| + \sum_{x\in R} |G(x)|. \end{aligned}$$

Durch Anwendung von Satz 8.6 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 $x \in R$. □

Wir betrachten nun ein weiteres Beispiel für die Operation einer Gruppe auf sich selbst.

Proposition 8.12 Sei G eine Gruppe. Dann ist durch $G \times G \to G, (g,h) \mapsto ghg^{-1}$ eine Operation von G auf sich selbst definiert. Man bezeichnet diese als ***Operation durch Konjugation***.

Beweis: Seien $g_1, g_2, h \in G$ vorgegeben. Dann gilt $e_G \cdot h = e_G h e_G^{-1} = h$ und

$$g_1 \cdot (g_2 \cdot h) = g_1 \cdot (g_2 h g_2^{-1}) = g_1 g_2 h g_2^{-1} g_1^{-1} = (g_1 g_2) h (g_1 g_2)^{-1} = (g_1 g_2) \cdot h. \qquad \square$$

Die Bahnen der soeben definierten Operation bezeichnet man als ***Konjugationsklassen***, und zwei Elemente, die in derselben Bahn liegen, nennt man zueinander ***konjugiert***.

Proposition 8.13 Der Stabilisator eines Elements $h \in G$ unter der Operation durch Konjugation ist gegeben durch $C_G(h) = \{g \in G \mid gh = hg\}$. Man bezeichnet diese Untergruppe von G als ***Zentralisator*** von h. Die Fixpunkte der Operation sind die Elemente der Menge

$$Z(G) = \{g \in G \mid gh = hg \ \forall\ h \in G\} \quad ,$$

dem sogenannten ***Zentrum***. Auch $Z(G)$ ist eine Untergruppe, darüber hinaus sogar ein Normalteiler von G.

Beweis: Sei G_h der Stabilisator von h. Für alle $g \in G$ gilt dann

$$g \in G_h \iff g \cdot h = h \iff ghg^{-1} = h \iff gh = hg \iff g \in C_G(h) \quad ,$$

somit haben wir $G_h = C_G(h)$ gezeigt. Aus der Gleichung folgt auch, dass $C_G(h)$ eine Untergruppe von G ist. 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 8.14 *(Klassengleichung)*
Sei G eine endliche Gruppe, die durch Konjugation auf sich selbst operiert. Sei R ein Repräsentantensystem der Bahnen mit Länge > 1. 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 8.13 berücksichtigt. □

Ist ein Element $\sigma \in S_n \setminus \{\mathrm{id}\}$ ein Produkt von r Zyklen der Längen $k_1, ..., k_r$ mit $r \geq 1$ und $k_1 \geq ... \geq k_r \geq 2$, dann nennt man $(k_1, ..., k_r)$ den ***Zerlegungstyp*** von σ. Zum Beispiel hat das Element $(1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9\ 10) \in S_{10}$ den Zerlegungstyp $(4, 3, 3)$. Es ist nicht schwer zu zeigen, dass die Zerlegungstypen genau den Konjugationsklassen in S_n entsprechen, d.h. zwei Elemente $\sigma, \tau \in S_n$ ungleich id sind genau dann konjugiert zueinander, wenn sie denselben Zerlegungstyp besitzen.

Die Anzahl der Elemente eines festen Zerlegungstyps kann durch einfache kombinatorische Überlegungen bestimmt werden. Auf diese Weise kann für jedes S_n die Klassengleichung aufgestellt werden. Für S_4 lautet sie beispielsweise

$$|S_4| \quad = \quad 24 \quad = \quad 1 + 6 + 8 + 6 + 3 \quad ,$$

weil S_4 neben $Z(S_4) = \{\mathrm{id}\}$ aus sechs Transpositionen, acht 3-Zyklen, sechs 4-Zyklen und drei Doppeltranspositionen, also Elementen vom Zerlegungstyp $(2, 2)$, besteht.

Sei p eine Primzahl. Bereits im Kapitel § 6 haben wir den Begriff der p***-Gruppe*** eingeführt; dabei handelte es sich um Gruppen von p-Potenzordnung. Während wir dort in erster Linie an kommutativen Gruppen interessiert waren, werden wir hier beliebige p-Gruppen betrachten.

Satz 8.15 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 8.14 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 8.16 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 8.17 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 8.15 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 8.16 abelsch. $\square$

Satz 8.18 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 8.7 abelsch und somit auflösbar. Sei nun $n \geq 3$, und setzen wir die Aussage für Werte kleiner als n voraus. Nach Satz 8.15 ist $Z(G)$ eine nichttrivale Untergruppe von G, wegen Proposition 8.13 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 7.15 (ii) folgt daraus auch die Auflösbarkeit von G. $\square$

§ 9. *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 9.1 *(„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 6.10 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 3.8 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 6.10 abgeleitet werden, wenn man noch berücksichtigt, dass nach Satz 3.10 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 kann man zeigen, dass die alternierende Gruppe A_4 keine Untergruppe der Ordnung 6 besitzt, obwohl 6 ein Teiler von $|A_4| = 12$ ist.

Folgerung 9.2 *(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 9.1 gibt es in G eine Untergruppe U der Ordnung p. Als Gruppe von Primzahlordnung ist U nach Folgerung 4.13 (ii) zyklisch, es gibt also ein $g \in U$ mit $U = \langle g \rangle$. Nach Definition der Elementordnung gilt $\text{ord}(g) = |\langle g \rangle| = |U| = p$. □

Wenden wir uns nun dem eigentlichen Thema dieses Abschnitts zu.

Definition 9.3 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, müssen wir einen neuen Typ von Gruppenoperationen betrachten, bei dem eine Gruppe G auf der Menge ihrer p-Sylowgruppen operiert.

Lemma 9.4 Sei G eine Gruppe. Für jedes $g \in G$ ist durch $\tau_g : G \to G$, $h \mapsto ghg^{-1}$ ein Automorphismus von G definiert.

Beweis: Zunächt überprüfen wir, dass τ_g ein Endomorphismus ist. Für $h_1, h_2 \in G$ gilt

$$\tau_g(h_1h_2) \quad = \quad gh_1h_2g^{-1} \quad = \quad (gh_1g^{-1})(gh_2g^{-1}) \quad = \quad \tau_g(h_1)\tau_g(h_2).$$

Damit ist die Endomorphismus-Eigenschaft nachgewiesen. Außerdem ist $\tau_{g^{-1}}$ offenbar die Umkehrabbildung von τ_g. Also τ_g bijektiv und somit ein Automorphismus von G. □

Wir erinnern an die in § 7 eingeführte Definition des *Normalisators* $N_G(U)$ einer Untergruppe U einer Gruppe G. Dies war die Definition aller Elemente $g \in G$ mit $gUg^{-1} = U$. Es handelte sich bei $N_G(U)$ um die größte Untergruppe von G mit U als Normalteiler.

Proposition 9.5 Sei G eine Gruppe und $\mathscr{U}$ die Menge der Untergruppen von G.

(i) Durch $G \times \mathscr{U} \to \mathscr{U}$, $(g, U) \mapsto g \cdot U$ mit $g \cdot U = gUg^{-1}$ ist eine Gruppenoperation von G auf $\mathscr{U}$ definiert.

(ii) Liegen zwei Elemente $U, V \in \mathscr{U}$ in derselben Bahn, dann sind sie isomorph.

(iii) Für jedes $U \in \mathscr{U}$ ist der Normalisator $N_G(U)$ genau der Stabilisator von U bezüglich der Gruppenoperation.

Beweis: zu (i) Nach Definition gilt $g \cdot U = \tau_g(U)$ für alle $g \in G$ und $U \in \mathscr{U}$, mit dem τ_g aus Lemma 9.4. Wegen der Automorphismus-Eigenschaft von τ_g ist $\tau_g(U)$ auch wieder eine Untergruppe von G, es gilt also $g \cdot U \in \mathscr{U}$. Die beiden Bedingungen für eine Gruppenoperation rechnet man unmittelbar nach: Sind $g, h \in G$ und $U \in \mathscr{U}$, dann gilt $e_G \cdot U = e_G U e_G^{-1} = U$ und

$$g \cdot (h \cdot U) \quad = \quad g \cdot (hUh^{-1}) \quad = \quad ghUhg^{-1} \quad = \quad (gh)U(gh)^{-1} \quad = \quad (gh) \cdot U.$$

zu (ii) Liegen $U, V \in \mathscr{U}$ in derselben Bahn, dann gibt es ein $g \in G$ mit $V = g \cdot U = \tau_g(U)$. Weil τ_g ein Automorphismus von G ist, sind U und $\tau_g(U)$ isomorph.

zu (iii) Für jedes $U \in \mathscr{U}$ und jedes $g \in G$ ist $g \in G_U$ nach Definition äquivalent zu $g \cdot U = U$ und zu $g \in N_G(U)$, also ist $N_G(U)$ der Stabilisator von U. □

Lemma 9.6 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 5.5 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 7.6, folgt $S \trianglelefteq HS$. □

Wir können nun unser Hauptresultat formulieren und beweisen.

Satz 9.7 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 $\nu_p \equiv 1 \mod p$ 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 der Untergruppen von G. Nach Satz 9.1 gibt es mindestens eine p-Sylowgruppe $P \in \mathcal{V}$. Die Bahn $\mathcal{U} = G(P)$ eine G-invariante Teilmenge. Weil nach Proposition 9.5 je zwei Elemente in derselben Bahn isomorph sind, besteht $\mathcal{U}$ ausschließlich aus p-Sylowgruppen. Ebenfalls auf Grund von Proposition 9.5 ist $N_G(P)$ der Stabilisator von P bezüglich der Operation.

Wir zeigen nun, dass p teilerfremd zu $|\mathcal{U}|$ ist. Auf Grund des allgemeinen Zusammenhangs aus Satz 8.6 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 4.8 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 8.11 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 9.6 ist das Komplexprodukt HS jedenfalls eine Untergruppe von G und S ein Normalteiler von HS. Nach dem Isomorphiesatz, Satz 5.15, 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 $P'' \in \mathscr{U}$ 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 $\mathscr{U} = G(P)$ bereits die Menge *aller* p-Sylowgruppen von G ist und somit $\nu_p = |\mathscr{U}| = (G : N_G(P))$ 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 $\mathscr{U}$. 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 $\mathscr{U}$ zerfällt in Bahnen von p-Potenzlänge > 1. Bezeichnen wir mit R ein Repräsentantensystem dieser Bahnen, dann gilt auf Grund der Bahngleichung

$$\nu_p \quad = \quad |\mathscr{U}| \quad = \quad |\{P\}| + \sum_{U \in R} (P : P_U).$$

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 9.8 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 $g \in G$. Dann ist nach Proposition 9.5 (iii) 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 9.9 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 $\nu_3 \equiv 1 \mod 3$. Da $5 \not\equiv 1 \mod 3$ ist, bleibt als einzige Möglichkeit $\nu_3 = 1$. Die einzige 3-Sylowgruppe ist nach Folgerung 9.8 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 $\mu_5 \equiv 1 \mod 5$. Wegen $3 \not\equiv 1 \mod 5$ muss $\nu_5 = 1$ sein, und die einzige 5-Sylowgruppe ist wiederum ein Normalteiler von G. □

Folgerung 9.10 Jede Gruppe der Ordnung 15 ist zyklisch.

Beweis: Sei G eine Gruppe mit $|G| = 15$. Nach Lemma 9.9 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 5.8 folgt daraus $G \cong N \times U$. Als Gruppen von Primzahlordnung sind N und U nach Folgerung 4.13 zyklisch, es gilt also $N \cong \mathbb{Z}/3\mathbb{Z}$ und $U \cong \mathbb{Z}/5\mathbb{Z}$. Mit dem Chinesischen Restsatz, Satz 6.8, 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. □

Satz 9.11 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 7.7 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 $\nu_p \equiv 1 \mod p$. 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 $g^{b^2} = (g^b)^b = (hgh)^b = hg^bh = h^2gh^2 = e_G g e_G = g$ und $\mathrm{ord}(g) = p$ folgt $b^2 \equiv 1 \mod p$. 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 $b \equiv \pm 1 \mod p$.

Betrachten wir zunächst den Fall $b \equiv 1 \mod p$. 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 7.6 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 5.8 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 $b \equiv 1 \mod p$ ausgeschlossen ist.

Somit bleibt $b \equiv -1 \mod p$ 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. □

§ 10. Körpererweiterungen und Erweiterungsgrad

Zusammenfassung. Um die Theorie der algebraischen Erweiterungen vorzubereiten, beschäftigen wir uns in diesem Kapitel zunächst noch einmal allgemein mit der Kategorie der Körper allgemein und wiederholen bei dieser Gelegenheit, was bereits aus der Zahlentheorie-Vorlesung bekannt ist. Im Mittelpunkt unserer Interesses stehen dabei die *Körpererweiterungen* (für die $\mathbb{C}|\mathbb{R}$ eines der einfachsten Beispiele ist), für die wir auch einen passenden Typ von Homomorphismen, die sog. *K-Homomorphismen*, definieren.

Wir zeigen, wie die Elemente eines Erweiterungskörpers $K(a)$, der von einem einzigen Element a erzeugt wird, im Allgemeinen aussehen: Es handelt sich um die Elemente, die man dadurch erhält, dass man a in rationale Funktionen einsetzt, also in Quotienten von Polynomen f/g mit $f, g \in K[x]$. Schließlich definieren wir noch mit dem *Grad* einer Erweiterung eine wichtige Größe, mit der sich die Struktur von Körpererweiterungen untersuchen lässt. Diese wird im gesamten weiteren Verlauf der Vorlesung, bis hin zur Galoistheorie, eine zentrale Rolle spielen.

Wichtige Grundbegriffe

- Teilkörper und Primkörper eines Körpers
- Körpererweiterungen
- Körperhomomorphismen und K-Homomorphismen
- Erzeugendensysteme von Körpererweiterungen
- Grad $[L : K]$ einer Körpererweiterung

Zentrale Sätze

- Klassifikation der Primkörper
- Beschreibung der Elemente von einfachen Erweiterungen der Form $K(a)|K$
- Gradformel

Die Definition der ***Körper*** wurde bereits in der Erstsemester- und später noch einmal, in leicht veränderter aber äquivalenter Form, in der Zahlentheorie-Vorlesung angegeben. Demnach ist ein Körper ein Ring K, dessen Einheitengruppe durch $K^\times = K \setminus \{0_K\}$ gegeben ist. Beispiele für Körper sind $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$. In der Zahlentheorie wurde auch schon für jede Primzahl p ein Körper definiert, der aus genau p Elementen besteht, nämlich $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Ein ***Teilkörper*** eines Körpers K ist ein Teilring $L \subseteq K$ mit der zusätzlichen Eigenschaft, dass für jedes $a \in L$ ungleich 0_K auch das Inverse a^{-1} in L enthalten ist. Um zu zeigen, dass eine Teilmenge L eines Körpers K ein Teilkörper von K ist, muss also insgesamt geprüft werden, dass 1_K in L liegt, und dass für alle $a, b \in L$ auch $a - b$ und ab in L liegen, im Fall $a \neq 0_K$ auch das Element a^{-1}. Aus der Zahlentheorie ist bekannt, dass Null- und Einselement zweier Ringe übereinstimmen, wenn R ein Teilring von S ist. Dasselbe gilt natürlich erst recht für Teilkörper.

Wie bei den Ringen ist leicht zu sehen, dass für jede Familie $(L_i)_{i\in I}$ von Teilkörpern eines Körpers K auch der Durchschnitt $\bigcap_{i\in I} L_i$ ein Teilkörper von K ist. Bildet man den Durchschnitt über *alle* Teilkörper eines Körpers K, dann erhält man den kleinsten Teilkörper von K.

Definition 10.1 Sei K ein Körper. Dann wird der kleinste Teilkörper von K der ***Primkörper*** von K genannt.

Enthält K den Körper $\mathbb{Q}$ der rationalen Zahlen als Teilkörper, dann muss $\mathbb{Q}$ der Primkörper von K sein. Ist nämlich F ein beliebiger Teilkörper von K, dann muss dieser das Einselement von K enthalten, das mit $1 \in \mathbb{Q}$ übereinstimmt. Durch vollständige Induktion zeigt man, dass $n \in F$ für alle $n \in \mathbb{N}$ gilt. Mit der Teilkörper-Eigenschaft von F folgt daraus unmittelbar auch $0 \in F$ und $-n \in F$ für alle $n \in \mathbb{N}$, insgesamt also $\mathbb{Z} \subseteq F$, und schließlich $\mathbb{Q} \subseteq F$, da F unter Kehrwertbildung und Multiplikation abgeschlossen ist. Weil $\mathbb{Q}$ also in jedem Teilkörper von F enthalten ist, muss es sich bei $\mathbb{Q}$ um den kleinsten Teilkörper von K handeln.

Noch einfacher sieht man, dass für jeden Körper K, der $\mathbb{F}_p$ als Teilkörper enthält, $\mathbb{F}_p$ der Primkörper von K sein muss. Denn jeder Teilkörper F von K muss das Einselement 1_K von K enthalten, das mit $\bar{1} \in \mathbb{F}_p$ übereinstimmt. Daraus folgt auch $\bar{a} \in F$ für $1 \leq a \leq p$, wobei $\bar{p} = \bar{0} = 0_K$ ist. Jeder Teilkörper von F muss also $\mathbb{F}_p$ enthalten.

Auch bei den Körpern, die $\mathbb{Q}$ und $\mathbb{F}_p$ nicht als Teilkörper enthalten, ist die Struktur des Primkörpers dieselbe. Um hier eine entsprechende Aussage zu formulieren, erinnern wir an den Begriff der ***Charakteristik*** eines Rings R, die wir in der Zahlentheorie mit $\mathrm{char}(R)$ bezeichnet hatten. Im Fall, dass $n \cdot 1_R \neq 0_R$ für alle $n \in \mathbb{N}$ gilt, hatten wir $\mathrm{char}(R) = 0$ gesetzt, ansonsten auf die kleinste Zahl $n \in \mathbb{N}$, für die $n \cdot 1_R = 0_R$ erfüllt ist. Dort hatten wir bereits festgestellt, dass für Integritätsbereiche, also erst recht für Körper, die Charakteristik entweder 0 oder eine Primzahl ist.

Satz 10.2 Sei K ein Körper und P sein Primkörper.

(i) Ist $\mathrm{char}(K) = 0$, dann gilt $P \cong \mathbb{Q}$.

(ii) Ist $\mathrm{char}(K) = p$ für eine Primzahl p, dann gilt $P \cong \mathbb{F}_p$.

Beweis: Aus der Zahlentheorie-Vorlesung ist bekannt, dass für jeden Ring R ein eindeutig bestimmter Ringhomomorphismus $\mathbb{Z} \to R$ existiert, gegeben durch $n \mapsto n \cdot 1_R$ für alle $n \in \mathbb{Z}$. Sei $\phi : \mathbb{Z} \to K$ dieser Homomorphismus für $R = K$. Mit Hilfe von ϕ beweisen wir nun die beiden Aussagen des Satzes.

zu (i) Im Fall $\mathrm{char}(K) = 0$ 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 eine natürliche Zahl $m \in \mathbb{N}$ mit $m \cdot 1_K = \phi(m) = 0_K$, was aber der Voraussetzung $\mathrm{char}(K) = 0$ widerspricht. Wir definieren nun eine Abbildung $\tilde{\phi} : \mathbb{Q} \to K$, indem wir jeder rationalen Zahl $\frac{a}{b}$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ das Bild $\phi(a)\phi(b)^{-1}$ zuordnen. Das Bild ist unabhängig von der Darstellung der rationalen Zahl als Bruch. Gilt nämlich $\frac{a}{b} = \frac{c}{d}$ mit $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{N}$, dann folgt $ad = bc$, somit

$$\phi(a)\phi(d) \quad = \quad \phi(b)\phi(c) \qquad \text{und} \qquad \phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1}.$$

Wir überprüfen nun, dass $\tilde{\phi}$ ein Ringhomomorphismus ist. Zunächst gilt

$$\tilde{\phi}(1) \quad = \quad \tilde{\phi}(\tfrac{1}{1}) \quad = \quad \phi(1)\phi(1)^{-1} \quad = \quad 1_K \cdot 1_K^{-1} \quad = \quad 1_K.$$

Seien $\alpha, \beta \in \mathbb{Q}$ mit $\alpha = \frac{a}{b}$, $\beta = \frac{c}{d}$, $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$. Dann gilt

$$\alpha + \beta = \frac{ad + bc}{bd} \qquad \text{und} \qquad \alpha\beta = \frac{ac}{bd} \quad ,$$

und es folgt $\tilde{\phi}(\alpha + \beta) = \phi(ad + bc)\phi(bd)^{-1} = \phi(ad)\phi(bd)^{-1} + \phi(bc)\phi(bd)^{-1} = \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} = \tilde{\phi}(\alpha) + \tilde{\phi}(\beta)$ sowie $\tilde{\phi}(\alpha\beta) = \phi(ac)\phi(bd)^{-1} = \phi(a)\phi(b)^{-1}\phi(c)\phi(d)^{-1} = \tilde{\phi}(\alpha)\tilde{\phi}(\beta)$. Damit ist die Homomorphismus-Eigenschaft nachgewiesen.

Der Ringhomomorphismus $\tilde{\phi} : \mathbb{Q} \to K$ definiert einen Isomorphismus von $\mathbb{Q}$ auf sein Bild $\tilde{\phi}(\mathbb{Q})$. Als isomorphes Bild eines Körpers ist $\tilde{\phi}(\mathbb{Q})$ ein Teilkörper von K. Wir zeigen nun, dass $\tilde{\phi}(\mathbb{Q})$ der Primkörper von K ist. Dafür genügt es zu überprüfen, dass $\tilde{\phi}(\mathbb{Q})$ in einem beliebig vorgegebenen Teilkörper F von K enthalten ist. Zunächst gilt $\tilde{\phi}(1) = 1_K \in F$. Setzen wir für ein $n \in \mathbb{N}$ voraus, dass $\tilde{\phi}(n)$ in F liegt, dann folgt

$$\tilde{\phi}(n+1) \quad = \quad \tilde{\phi}(n) + \tilde{\phi}(1) \quad = \quad \tilde{\phi}(n) + 1_K \quad \in \quad F.$$

Durch vollständige Induktion erhält man also $\tilde{\phi}(n) \in F$ für alle $n \in \mathbb{N}$. Wegen $\tilde{\phi}(-n) = -\tilde{\phi}(n) \in F$ für alle $n \in \mathbb{N}$ gilt auch $\tilde{\phi}(n) \in F$ für alle $n \in \mathbb{Z}$. Sei nun $\alpha \in \mathbb{Q}$ beliebig vorgegeben, $\alpha = \frac{a}{b}$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Wie bereits gezeigt, gilt $\tilde{\phi}(a), \tilde{\phi}(b) \in F$, und auf Grund der Injektivität von ϕ gilt $\tilde{\phi}(b) = \phi(b)\phi(1)^{-1} \neq 0_K$. Weil F ein Teilkörper von K ist, folgt $\tilde{\phi}(\alpha) = \tilde{\phi}(a)\tilde{\phi}(b)^{-1} \in F$. Damit ist $\tilde{\phi}(\mathbb{Q}) \subseteq F$ 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 $p\mathbb{Z}$ enthält. Wie in § 3 der Gruppentheorie gezeigt, muss $\ker(\phi) = n\mathbb{Z}$ gelten, mit einem Teiler $n \in \mathbb{N}$ von p. Damit sind $\ker(\phi) = \mathbb{Z}$ und $\ker(\phi) = p\mathbb{Z}$ die einzigen beiden Möglichkeiten. Wäre $\ker(\phi) = \mathbb{Z}$, dann wäre ϕ die Nullabbildung, was aber im Widerspruch zu $\phi(1) = 1_K \neq 0_K$ steht. Also muss $\ker(\phi) = p\mathbb{Z}$ gelten. Der Homomorphiesatz für Ringe liefert einen Ringisomorphismus $\bar{\phi} : \mathbb{Z}/p\mathbb{Z} \to \phi(\mathbb{Z})$, es gilt also $\mathbb{F}_p \cong \phi(\mathbb{Z})$.

Wir überprüfen nun, dass $\phi(\mathbb{Z})$ der Primkörper von K ist. Als Bild von $\mathbb{F}_p$ unter dem Isomorphismus $\bar{\phi}$ ist $\phi(\mathbb{Z})$ jedenfalls ein Teilkörper von K. Sei nun F ein beliebiger Teilkörper von K. Zunächst gilt $\phi(1) = 1_K \in F$. Mit vollständiger Induktion und durch Verwendung der Abgeschlossenheit von F unter Addition zeigt man, dass $\phi(a) \in F$ für alle $a \in \mathbb{N}$ gilt. Es folgt $\bar{\phi}(\bar{a}) = \phi(a) \in F$ für $1 \leq a \leq p$ und damit $\bar{\phi}(\mathbb{F}_p) = \phi(\mathbb{Z}) \subseteq F$. □

Definition 10.3 Eine ***Körpererweiterung*** $L|K$ ist ein Paar (K, L) von Körpern mit der Eigenschaft, dass K ein Teilkörper von L ist. Einen Teilkörper M von L mit $M \supseteq K$ bezeichnet man als ***Zwischenkörper*** der Erweiterung $L|K$.

Beispielsweise ist $\mathbb{C}|\mathbb{Q}$ eine Körpererweiterung, und $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Zwischenkörper dieser Erweiterung.

Bereits in der Zahlentheorie wurden die zu den Körpern gehörigen strukturerhaltenden Abbildungen definiert, die ***Körperhomomorphismen***. Dort wurde festgelegt, dass ein Körperhomomorphismus zwischen Körpern L und M nichts weiter als ein Ringhomomorphismus zwischen L und M ist, also eine Abbildung $\phi : L \to M$ mit der Eigenschaft, dass $\phi(1_L) = 1_M$ und $\phi(a + b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$ für alle $a, b \in L$ gilt. Daraus folgt dann auch $\phi(a^{-1}) = \phi(a)^{-1}$ für alle $a \in L$ ungleich Null, wegen $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_L) = 1_M$. Auch wurde dort gezeigt, dass Körperhomomorphismen stets injektiv sind.

Die Menge aller Körperhomomorphismen bezeichnen wir mit $\mathrm{Hom}(L, M)$. Weiter sei $\mathrm{Isom}(L, M)$ die Menge der bijektiven Körperhomomorphismen $L \to M$, die wir als ***Körperisomorphismen*** bezeichnen. Ist diese Menge nichtleer, dann bezeichnen wir L und M als ***isomorph***. Schließlich setzen wir noch $\mathrm{Aut}(L) = \mathrm{Isom}(L, L)$ und nennen die Elemente dieser Menge die ***Automorphismen*** von L.

Lemma 10.4 Seien L, M isomorphe Körper und $\sigma \in \mathrm{Isom}(L, M)$. Dann liegt die Umkehrabbildung σ^{-1} von σ in $\mathrm{Isom}(M, L)$. Die Menge $\mathrm{Aut}(L)$ bildet mit der Komposition von Abbildungen als Verknüpfung eine Gruppe.

Beweis: Aus $\sigma(1_L) = 1_M$ und der Bijektivität von σ folgt $1_L = \sigma^{-1}(1_M)$. Seien nun $\alpha, \beta \in M$ vorgegeben. Aus $\sigma(\sigma^{-1}(\alpha) + \sigma^{-1}(\beta)) = \sigma(\sigma^{-1}(\alpha)) + \sigma(\sigma^{-1}(\beta)) = \alpha + \beta$ erhalten wir durch Anwendung von σ^{-1} die Gleichung $\sigma^{-1}(\alpha) + \sigma^{-1}(\beta) = \sigma^{-1}(\alpha + \beta)$. Genauso beweist man auch die Verträglichkeit mit der Multiplikation. Somit ist σ^{-1} ein Körperhomomorphismus. Als Umkehrabbildung einer bijektiven Abbildung ist σ^{-1} auch bijektiv. Insgesamt ist damit gezeigt, dass mit σ auch σ^{-1} ein Element von $\mathrm{Isom}(M, L)$ ist.

Nun beweisen wir die Gruppeneigenschaft von $\mathrm{Aut}(L)$. Wie man leicht überprüft, ist mit $\sigma, \tau \in \mathrm{Aut}(L)$ auch $\sigma \circ \tau$ in $\mathrm{Aut}(L)$ enthalten. Dies zeigt, dass die Komposition $\circ$ tatsächlich eine Verknüpfung auf $\mathrm{Aut}(L)$ ist. Die identische Abbildung id_L ist offenbar ein Element von $\mathrm{Aut}(L)$, und es gilt $\sigma \circ \mathrm{id}_L = \mathrm{id}_L \circ \sigma = \sigma$ für alle $\sigma \in \mathrm{Aut}(L)$. Wie wir gerade gezeigt haben, liegt mit σ auch σ^{-1} in $\mathrm{Aut}(L) = \mathrm{Hom}(L, L)$, und nach Definition der Umkehrabbildung gilt $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}_L$. Insgesamt ist $(\mathrm{Aut}(L), \circ)$ also tatsächlich eine Gruppe. □

Im Hinblick auf spätere Anwendungen definieren wir auch für Körpererweiterungen einen passenden Typ von Homomorphismen. Sind $L|K$ und $M|K$ Körpererweiterungen, dann ist ein ***K-Homomorphismus*** ein Körperhomomorphismus $\phi : L \to M$ mit der Eigenschaft, dass $\phi(a) = a$ für alle $a \in K$ erfüllt ist. Die Menge dieser Abbildungen bezeichnen wir mit $\mathrm{Hom}_K(L, M)$. Die bijektiven$K$-Homomorphismen $L \to M$ nennen wir entsprechend ***K-Isomorphismen*** und bezeichen deren Menge mit $\mathrm{Isom}_K(L, M)$. Schließlich definieren wir $\mathrm{Aut}_K(L) = \mathrm{Isom}_K(L, L)$ und nennen die Elemente dieser Menge die ***K-Automorphismen*** von L. Beispielsweise ist die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ ein Element von $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, und zugleich von $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$.

Proposition 10.5 Für jede Körpererweiterung $L|K$ ist $\mathrm{Aut}_K(L)$ eine Untergruppe von $\mathrm{Aut}(L)$.

Beweis: Wegen $\mathrm{id}_L(a) = a$ für alle $a \in K$ ist das Neutrallement id_L von $\mathrm{Aut}(L)$ in $\mathrm{Aut}_K(L)$ enthalten. Seien nun $\sigma, \tau \in \mathrm{Aut}_K(L)$ vorgegeben. Wegen $\sigma(a) = \tau(a) = a$ gilt $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$ für jedes $a \in K$. Also ist $\sigma \circ \tau$ in $\mathrm{Aut}_K(L)$ enthalten. Aus $\sigma(a) = a$ folgt durch Anwendung von σ^{-1} jeweis $a = \sigma^{-1}(a)$, für jedes $a \in K$. Dies zeigt, dass auch σ^{-1} in $\mathrm{Aut}_K(L)$ liegt. □

Körperhomomorphismen können zur Definition von Teilkörpern genutzt werden.

Proposition 10.6 Sei $\phi : L \to M$ ein Körperhomomorphismus, wobei wir voraussetzen, dass L und M einen gemeinsamen Teilkörper besitzen. Dann ist auch die Teilmengen K gegeben durch $K = \{a \in L \mid \phi(a) = a\}$ ein gemeinsamer Teilkörper von L und M, und es gilt $\phi \in \mathrm{Hom}_K(L, M)$.

Beweis: Bezeichnen wir den gemeinsamen Teilkörper von L und M aus der Voraussetzung mit F, so folgt aus der Homomorphismus-Eigenschaft von ϕ, dass $\phi(1_L) = 1_M = 1_F = 1_L$ und somit $1_L \in K$ gilt. Seien nun $a, b \in K$ vorgegeben. Aus $\phi(a) = a$ und $\phi(b) = b$ folgt $\phi(a - b) = \phi(a) - \phi(b) = a - b$, ebenso $\phi(ab) = \phi(a)\phi(b) = ab$ und im Fall $a \neq 0_L$ auch $\phi(a^{-1}) = \phi(a)^{-1} = a^{-1}$. Dies zeigt, dass auch $a - b$ und ab, und im Fall $a \neq 0_L$ auch a^{-1} in K liegen. Insgesamt ist damit nachgewiesen, dass K ein Teilkörper von L ist. Jedes $a \in K$ liegt wegen $\phi(a) = a$ auch in M, somit ist K eine Teilmenge von M, und auf Grund der soeben bewiesenen Abgeschlossenheits-Eigenschaften ist K damit auch ein Teilkörper von M. Die Aussage $\phi \in \mathrm{Hom}_K(L, M)$ folgt nun direkt aus der Definition des Begriffs der K-Homomorphismen, denn K besteht ja gerade aus den Elementen, die von ϕ auf sich selbst abgebildet werden. □

Der Teilkörper K aus der Proposition enthält natürlich den gemeinsamen Primkörper der Körper L und M. Daraus folgt, dass jeder Körperhomomorphismus zwischen Erweiterungen von $\mathbb{Q}$ automatisch ein $\mathbb{Q}$-Homomorphismus ist, denn in diesem Fall ist, wie wir oben bemerkt haben, $\mathbb{Q}$ der gemeinsame Primkörper dieser Erweiterungen. Ebenso ist jeder Körperhomomorphismus zwischen Erweiterungen von $\mathbb{F}_p$ ein $\mathbb{F}_p$-Homomorphismus.

Ähnlich wie bei Ringerweiterungen lassen sich auch Körpererweiterungen am einfachsten mit Hilfe von Erzeugendensystemen beschreiben.

Satz 10.7 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 in der Zahlentheorie 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 10.7 eindeutig bestimmten Körper mit $K(S)$ und nennen ihn den von 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 10.8 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 10.7 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 Körpererweiterungen an, die von einem einzelnen Element erzeugt werden.

Proposition 10.9 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. □

Definition 10.10 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 10.11 *(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

$$\{\alpha_i \beta_j \mid 1 \le i \le m \ , \ 1 \le j \le n\}$$

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 $1 \le j \le n$. 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 $1 \le j \le n$. Da die Elemente $\alpha_1, ..., \alpha_n$ im K-Vektorraum L linear unabhängig sind, folgt daraus wiederum $a_{ij} = 0$ für $1 \le i \le m$ und $1 \le j \le n$. $\square$

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 $K = \mathbb{R}$.

§ 11. *Algebraische Körpererweiterungen*

Zusammenfassung. Nachdem wir im letzten Kapitel allgemeine Körpererweiterungen studiert haben, konzentrieren wir uns nun auf solche, die von *algebraischen Elementen* erzeugt werden. Dabei wird ein Element α in einer Erweiterung eines Körpers K als algebraisch über K bezeichnet, wenn es Nullstelle eines Polynoms $f \neq 0$ in $K[x]$ ist. Die Elemente des erzeugten Körpers $K(\alpha)$ lassen sich dann als Polynomausdrücke $g(\alpha)$ mit $g \in K[x]$ darstellen, wobei für die Darstellung sämtlicher Elemente nur Polynome beschränkten Grades benötigt werden. Gegenüber der allgemeinen Situation, die wir in Proposition 10.9 betrachtet haben, stellt dies eine enorme Vereinfachung dar.

Der maximal benötigte Polynomgrad wird hierbei durch ein irreduzibles Polynom $f \in K[x]$ bestimmt, das sog. *Minimalpolynom* von α über K. Bemerkenswerterweise kann man umgekehrt, wie wir sehen werden, zu jedem irreduziblen Polynom $f \in K[x]$ eine Erweiterung $L|K$ konstruieren, in der das Polynom f eine Nullstelle besitzt. Dies haben wir in der Zahlentheorie bereits auf das Polynom $f = x^2 + 1$ angewendet und auf diesem Wege die komplexen Zahlen konstruiert. Hier behandeln wir diese Konstruktion für allgemeines irreduzibles Polynom. Zum Abschluss des Kapitels wird noch untersucht, in welcher Beziehung die endlichen und die algebraischen Körpererweiterungen zueinander stehen.

Wichtige Grundbegriffe

- algebraische und transzendente Körperelemente
- algebraische Körpererweiterung
- Minimalpolynom $\mu_{\alpha,K}$ eines Elements α über einem Grundkörper K
- Aufbau des von einem algebraischen Element α erzeugten Körpers $K(\alpha)$
- Existenz algebraischer Erweiterungen
- endliche und algebraische Erweiterungen

Zentrale Sätze

- Eigenschaften des Minimalpolynoms
- Struktur einer einfache algebraischen Erweiterung $K(\alpha)|K$ als K-Vektorraum
- Durchführbarkeit von Rechnenoperationen in algebraischen Erweiterungen
- Existenz algebraischer Erweiterungen
- Beziehung zwischen endlichen und algebraischen Erweiterungen

In diesem Abschnitt wird der Ring $K[x]$ der Polynome über einem Körper K eine wichtige Rolle spielen. Wir sammeln hier zunächst eine Reihe von Eigenschaften dieses Rings, die wir im weiteren Verlauf als bekannt voraussetzen. Die meisten davon wurden in der Linearen Algebra oder der Zahlentheorie behandelt, lediglich der Beweis der letzten beiden Punkte in der Zahlentheorie-Vorlesung steht noch aus.

(i) Ist $f \in K[x]$, $f \neq 0$ ein Element der Form $\sum_{i=0}^{n} a_i x^i$ mit $n \in \mathbb{N}_0$, $a_0, ..., a_n \in K$ und $a_n \neq 0$, dann nennt man n den ***Grad*** (Bezeichnung $\operatorname{grad}(f)$) und a_n den ***Leitkoeffizienten*** von f. Ist $a_n = 1$, dann bezeichnet man das Polynom als ***normiert***, und die Multiplikation eines Polynoms mit dem Kehrwert a_n^{-1} seines Leitkoeffizienten bezeichnet man als ***Normierung***. Ist der Grad $n = 0$ spricht man von ***konstanten*** Polynomen. Auch das Nullpolynom wird als konstantes Polynom bezeichnet, wir ordnen ihm aber keinen Grad zu.

(ii) ***Division mit Rest:*** Seien $f, g \in K[x]$ mit $g \neq 0$. Dann gibt es Polynome $q, r \in K[x]$, so dass $f = qg + r$ und außerdem $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$ gilt. Für je zwei Polynome $f, g \in K[x]$ mit $(f, g) \neq (0, 0)$ gibt es Polynome $a, b \in K[x]$, so dass $af + bg = \text{ggT}(f, g)$ erfüllt ist.

(iii) Sei L ein Erweiterungskörper von K. Ein Element $\alpha \in L$ mit $f(\alpha) = 0$ wird ***Nullstelle*** von f genannt. Ein Polynom $f \neq 0$ vom Grad n besitzt in einem beliebigen Erweiterungskörper L höchstens n Nullstellen.

(iv) ***universelle Eigenschaft*** des Polynomrings: Für jeden Homomorphismus $\phi : K \to R$ von K in einen Ring R und jedes $a \in R$ gibt es eine eindeutig bestimmten Homomorphismus $\phi_a : K[x] \to R$ mit $\phi_a(x) = a$ und $\phi_a|_K = \phi$.

(v) Ein Polynom f heißt ***irreduzibel*** (oder unzerlegbar), wenn es nicht konstant ist und es auch keine nicht-konstanten Polynome $g, h \in K[x]$ mit $f = gh$ gibt. Ein ***reduzibles*** Polynom ist ein nicht-konstantes, nicht irreduzibles Polynom.

(vi) Sei f ein irreduzibles Polynom, und seien $g, h \in K[x]$, so dass f ein Teiler von gh ist. Dann gilt $f|g$ oder $f|h$.

(vii) Für jedes nicht-konstante Polynom $f \in K[x]$ gibt es ein $a \in K^\times$ und normierte, irreduzible Polynome $g_1, ..., g_r \in K[x]$ mit $f = ag_1 \cdot ... \cdot g_r$. Dabei sind die Polynome g_i durch f bis auf Reihenfolge eindeutig bestimmt.

Definition 11.1 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 Körpererelemente.

(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 11.2 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 $\text{grad}(h) < \text{grad}(f)$. 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 11.3 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 $g \in K[x]$ ein weiteres normiertes, irreduzibles Polynom mit α als Nullstelle, 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 11.4 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

$$U \quad = \quad = \left\{ \sum_{k=0}^{n-1} a_k \alpha^k \;\middle|\; a_0, ..., a_{n-1} \in K \right\} \quad = \quad \left\{ g(\alpha) \;\middle|\; g \in K[x]\,,\ \text{grad}(g) < n \text{ oder } g = 0 \right\}.$$

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 $\operatorname{grad}(g-h) < n$; 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 $\operatorname{grad}(r) < n$. Es folgt

$$\beta\gamma \quad = \quad g(\alpha)h(\alpha) \quad = \quad (qf+r)(\alpha) \quad = \quad q(\alpha)f(\alpha) + r(\alpha) \quad = \quad q(\alpha)\cdot 0 + r(\alpha) \quad = \quad r(\alpha).$$

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 $\operatorname{grad}(r) < n$. 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 $\operatorname{grad}(g) < n$. 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 11.4 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 $n = \operatorname{grad}(f)$. 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 $\operatorname{grad}(g+h)<n$.

(ii) ***Negative:***
Es gilt $-\beta=(-g)(\alpha)$ und $-g=0$ oder $\operatorname{grad}(-g)<n$.

(iii) ***Multiplikation:***
Durch Division mit Rest bestimmen wir Polynome $q,r\in K[x]$ mit $gh=qf+r$ und $r=0$ oder $\operatorname{grad}(r)<n$. Wie im Beweis von Satz 11.4 gezeigt wurde, gilt $\beta\gamma=r(\alpha)$.

(iv) ***Kehrwerte:***
Hier sei $\beta\neq 0$ vorausgesetzt. Wie im Beweis des Satzes gezeigt wurde, gilt $\operatorname{ggT}(f,g)=1$. 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 $\operatorname{grad}(r)<n$. 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 $\dim_{\mathbb{F}_3}\mathbb{F}_3(\alpha)=\operatorname{grad}(f)=2$ 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 11.5 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 11.4 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 11.3 ist g ein Vielfaches des Minimalpolynoms f, also $g \in (f)$. Der Homomorphiesatz für Ringe aus der Zahlentheorie-Vorlesung liefert nun den angegebenen Isomorphismus. □

Satz 11.6 *(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) laut Zahlentheorie-Vorlesung 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

$$\phi(ab) \quad = \quad ab+(f) \quad = \quad (a+(f))(b+(f)) \quad = \quad \phi(a)\phi(b).$$

In der Zahlentheorie wurde gezeigt (Satz 2.12 im Zahlentheorie-Skript): 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

$$\begin{aligned} \hat{\phi}(f(\alpha)) &= \hat{\phi}\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} \phi(a_i)\hat{\phi}(\alpha)^i = \sum_{i=0}^{n} (a_i + (f))(x + (f))^i = \\ \sum_{i=0}^{n} (a_i x^i + (f)) &= \left(\sum_{i=0}^{n} a_i x^i\right) + (f) = f + (f) = 0 + (f) = 0_{\tilde{L}} \quad , \end{aligned}$$

und somit $f(\alpha) = \hat{\phi}^{-1}(0_{\tilde{L}}) = 0_L$. □

Definition 11.7 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 11.8 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 10.8 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 11.4 gilt $[L : L_0] = \text{grad}(f)$. Weil $L_0|K$ und $L|L_0$ endliche Erweiterungen sind, ist nach Satz 10.11 auch $L|K$ endlich. □

Satz 11.9

(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 11.8 (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 11.8 (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 10.11 können wir schließen, dass $L_0(\alpha)|K$ endlich ist. Aber dies bedeutet nach Proposition 11.8 (i) wiederum, dass $L_0(\alpha)|K$ algebraisch und insbesondere α algebraisch über K ist. □

Folgerung 11.10 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 11.9 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 11.11 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 $\mathrm{grad}(f)=[K(\alpha):K]=2$ gibt es $p,q\in K$ mit $f=x^2+px+q$. Wegen $\mathrm{char}(K)\neq 2$ 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. Im Folgenden setzen wir die Eindeutigkeit und Existenz der Primfaktorzerlegung natürlicher Zahlen als bekannt voraus. Diese Aussage, die in der Schulmathematik auch als *Fundamentalsatz der Arithmetik* bekannt ist, ergibt sich aus der Tatsache, dass $\mathbb{Z}$ ein faktorieller Ring ist. Dies wiederum wird in der Zahlentheorie-Vorlesung bewiesen.

Folgerung 11.12 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 11.11 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 $n^2r=(n\alpha)^2\in\mathbb{Z}$. 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 $t\in\mathbb{N}_0$, $e_1,\ldots,e_t\in\mathbb{N}$ und den verschiedenen Primteilern $p_1,\ldots,p_t$ 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 $r=n^2m$. Aus $(\frac{1}{n}\alpha)^2=(\frac{1}{n})^2r=m$ 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 11.13 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 11.4 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 $\text{ggT}(a, b) = 1$, 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 $\text{ggT}(a, b) = 1$ 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. □

§ 12. *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, werden wir diese Fragen vollständig beantworten. In den Übungen wird sich zeigen, dass mit den Ergebnissen dieses Abschnitts auch mehrelementige Erzeugendensysteme behandelt werden können.

Wie wir im weiteren Verlauf sehen werden, spielen Körperhomomorphismen und ihre Fortsetzung beim Studium algebraischer Erweiterungen eine wichtige Rolle. Im folgenden Abschnitt § 13 werden wir mit ihrer Hilfe zeigen, dass der algebraische Abschluss eines Körpers und (allgemeiner) Zerfällungskörper beliebiger Polynommengen bis auf Isomorphie eindeutig bestimmt sind. In einem späteren Kapitel werden wir zwei Eigenschaften algebraischer Körpererweiterungen einführen, die sog. *normalen* bzw. *separablen* Erweiterungen, die sich durch Körperhomomorphismen charakterisieren lassen. In der Galoistheorie, die wir am Ende der Vorlesung behandeln werden, spielen Körperhomomorphismen als Elemente der *Galoisgruppen* sogar eine ganz zentrale Rolle.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Fortsetzung eines Körperhomomorphismus	– eindeutige Festlegung einer Fortsetzung durch die Bilder der Erzeuger – Existenz von Fortsetzungen auf endliche und algebraische Erweiterungen – Festlegung der Anzahl der Fortsetzungen durch die Nullstellen des Bildpolynoms in der Erweiterung

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 12.1 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 12.2 *(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 12.1 klar. Zum Nachweis der Existenz verwenden wir Satz 11.5. 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 12.3 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 12.4 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 12.3 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 12.5 Für jede algbraische Erweiterung $L|K$ gilt $\text{Hom}_K(L, L) = \text{Aut}_K(L)$.

Beweis: Die Inklusion $\text{Aut}_K(L) \subseteq \text{Hom}_K(L, L)$ ist auf Grund der Definitionen trivial. Zum Beweis der umgekehrten Inklusion sei $\phi \in \text{Hom}_K(L, L)$ 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. Aus der Zahlentheorie-Vorlesung ist bekannt, dass es sich bei N um eine endliche Menge handelt, genauer sogar, dass $|N| \leq \text{grad}(f)$ gilt. Wir betrachten nun die

eingeschränkte Abbildung $\phi|_N$. Als Einschränkung einer injektiven Abbildung ist auch $\phi|_N$ injektiv. Nach Satz 12.3 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 sog. ***Eisenstein-Kriterium***, das wir in der Zahlentheorie-Vorlesung behandeln werden, ist das Polynom $f = x^3 - 2$ in $\mathbb{Q}[x]$ irreduzibel. Außerdem gilt $f(\sqrt[3]{2}) = 0$, also ist f nach Proposition 11.3 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 in der Zahlentheorie-Vorlesung 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 12.4 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 12.4, 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 12.6 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. □

§ 13. Zerfällungskörper

Zusammenfassung. Bereits in § 11 haben wir gezeigt: Ist K ein Körper und $f \in K[x]$ ein irreduzibles Polynom, dann gibt es eine Körpererweiterung $L|K$, die eine Nullstelle von f enthält. Betrachten wir zum Beispiele $K = \mathbb{Q}$ und $f = x^3 - 2 \in \mathbb{Q}[x]$, dann ist $L = \mathbb{Q}(\sqrt[3]{2})$ ein solcher Erweiterungskörper, mit der Nullstelle $\sqrt[3]{2} \in L$ des Polynoms f. Im Allgemeinen bedeutet der Übergang zu einer solchen Erweiterung $L|K$ aber nicht, dass f über L vollständig in Linearfaktoren zerfällt. Im angegebenen Beispiel etwa besitzt das Polynom f über $\mathbb{Q}(\sqrt[3]{2})$ die Faktorisierung

$$f \quad = \quad (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

wobei der quadratische Faktor allerdings nicht weiter zerlegt werden kann (Details siehe Haupttext). Ist ein nicht-konstantes Polynom f über einem Körper K vorgegeben, so bezeichnet man einen minimalen Erweiterungskörper $L \supseteq K$, über dem f in Linearfaktoren zerfällt, als *Zerfällungskörper* von f über K. In unserem Beispiel ist dies eine echte Erweiterung des Körpers $\mathbb{Q}(\sqrt[3]{2})$, nämlich $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ mit der nicht-reellen Zahl $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \in \mathbb{C}$.

Wie wir sehen werden, kann nicht nur einem einzelnen nicht-konstantem Polynom, sondern jeder beliebigen Menge $S \subseteq K[x]$ solcher Polynome ein Zerfällungskörper zugeordnet werden. Wir zeigen, dass ein solcher Körper stets existiert und bis auf Isomorphie eindeutig bestimmt ist. Bereits im ersten Semester wurde erwähnt (und später im Rahmen der Funktionentheorie-Vorlesung bewiesen), dass der Körper $\mathbb{C}$ der komplexen Zahlen *algebraisch abgeschlossen* ist, was bedeutet, dass jedes nicht-konstante Polynom über $\mathbb{C}$ in Linearfaktoren zerfällt. Als Anwendung der Zerfällungskörper zeigen wir, dass jeder beliebige Körper K einen minimalen algebraisch abgeschlossenen Erweiterungskörper besitzt. Man bezeichnet einen solchen Körper als *algebraischen Abschluss* von K. Auch dieser ist bis auf Isomorphie eindeutig.

Wichtige Grundbegriffe

- Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[x]$
- Zerfällungskörper einer Teilmenge S der Menge S_K aller nicht-konstanten Polynome
- algebraisch abgeschlossener Körper
- algebraischer Abschluss eines Körpers

Zentrale Sätze

- Existenz und Eindeutigkeit des Zerfällungskörpers bis auf K-Isomorphie
- Existenz und Eindeutigkeit des algebraischen Abschlusses bis auf K-Isomorphie
- Fortsetzbarkeit von Körperhomomorphismen auf beliebige algebraische Erweiterungen (unter der Voraussetzung, dass der Wertebereich algebraisch abgeschlossen ist)

Satz 13.1 Sei K ein Körper und $f \in K[x]$ ein nicht-konstantes Polynom. Dann gibt es einen Erweiterungskörper L von K mit den beiden Eigenschaften

(i) Das Polynom f zerfällt über L in Linearfaktoren.

(ii) Sind $\alpha_1, ..., \alpha_r$ die Nullstellen von f in L, dann gilt $L = K(\alpha_1, ..., \alpha_r)$.

Ein Erweiterungskörper von L mit diesen Eigenschaften wird ***Zerfällungskörper*** von f über K genannt.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über $n = \text{grad}(f)$. 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 11.6 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, $g = (x - \alpha_1) \cdot ... \cdot (x - \alpha_r)$, und $L = M(\alpha_2, ..., \alpha_r)$ gilt. Es folgt

$$f = (x - \alpha_1)(x - \alpha_2) \cdot ... \cdot (x - \alpha_r) \qquad \text{und} \qquad L = M(\alpha_2, ..., \alpha_r) = K(\alpha_1, \alpha_2, ..., \alpha_r). \qquad \square$$

Nach Satz 11.8 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 $p^2 - 4q = (\sqrt[3]{2})^2 - 4\sqrt[3]{3} = \sqrt[3]{4} - 4\sqrt[3]{3} = (-3)\sqrt[3]{3}$, 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 die Gleichung $\zeta = \frac{\zeta\sqrt[3]{2}}{\sqrt[3]{2}}$.

Man beachte, dass das Polynom f in Satz 13.1 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.

Satz 13.2 Ist K ein Körper und $S \subseteq K[x]$ eine beliebige (möglicherweise unendliche) Menge von nicht-konstanten Polynomen, dann gibt es einen Erweiterungskörper L von K mit der Eigenschaft, dass *jedes* Polynom $f \in S$ über L in Linearfaktoren zerfällt, und dass $L = K(N)$ gilt, wobei

$$N \quad = \quad \{\alpha \in L \mid f(\alpha) = 0 \text{ für ein } f \in S\}$$

die Menge der Nullstellen sämtlicher Polynome aus S bezeichnet. Man nennt L dann einen Zerfällungskörper von S über dem Grundkörper K.

Ist die Teilmenge $S \subseteq K[x]$ endlich, dann folgt die Aussage direkt aus Satz 13.1. 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 13.3 Sei K ein Körper und $S \subseteq K[x]$ eine beliebige Menge nicht-konstanter Polynome. Dann ist jeder Zerfällungskörper von S eine algebraische Erweiterung von K.

Beweis: Dies ergibt sich direkt aus Folgerung 11.10, weil jeder Zerfällungskörper durch Adjunkten von Nullstellen von Polynomen über K entsteht, also durch Adjunktion von Elementen, die über K algbraisch sind. □

Der Zerfällungskörper einer Menge $S \subseteq K[x]$ nicht-konstanter Polynome ist im Allgemeinen nicht eindeutig bestimmt, sondern nur, wie wir weiter unten zeigen werden, eindeutig bis auf K-Isomorphie. Beschränkt man sich bei der Suche nach Zerfällungskörpern aber auf Teilkörper eines vorgegebenen Erweiterungskörpers $\tilde{L} \supseteq K$, dann erhält man echte Eindeutigkeit.

Proposition 13.4 Sei K ein Körper, $S \subseteq K[x]$ eine Menge nicht-konstanter Polynome und $\tilde{L}$ ein Erweiterungskörper von K mit der Eigenschaft, dass jedes Polynom aus S über $\tilde{L}$ in Linearfaktoren zerfällt. Dann enthält $\tilde{L}$ genau einen Zerfällungskörper L_S von S über K. Es handelt sich um den kleinsten Zwischenkörper von $\tilde{L}|K$ mit der angegebenen Eigenschaft; ist L_1 ein beliebiger Zwischenkörper mit dieser Eigenschaft, dann folgt $L_1 \supseteq L_S$.

Beweis: Sei $N = \{\alpha \in \tilde{L} \mid f(\alpha) = 0 \text{ für ein } f \in S\}$ und $L_S = K(N)$. Jedes Polynom $f \in S$ zerfällt über $\tilde{L}$ in Linearfaktoren, und alle Nullstellen $\alpha \in \tilde{L}$ von f sind in L_S enthalten. Also zerfällt jedes $f \in S$ bereits über L_S in Linearfaktoren. Zusammen mit $L_S = K(N)$ folgt daraus, dass L_S ein Zerfällungskörper von S über K ist. Ist L_1 ein beliebiger Zwischenkörper von $\tilde{L}|K$ mit der Eigenschaft, dass jedes Polynom aus S über L_1 in Linearfaktoren zerfällt, dann enthält L_1 die Nullstellen aller Polynome aus S in $\tilde{L}$. Es gilt also $N \subseteq L_1$ und damit auch $L_S = K(N) \subseteq L_1$. Nehmen wir nun an, dass L' ein weiterer Zwischenkörper von $\tilde{L}|K$ ist, der zugleich Zerfällungskörper von S über K ist. Dann wird L' insbesondere von N über K erzeugt. Es gilt also $L' = K(N) = L_S$. □

Unter den Voraussetzungen von Proposition 13.4 ist es also zulässig, von *dem* Zerfällungskörper der Menge S in $\tilde{L}$ zu sprechen. Besonders häufig verwendet man diese Eindeutigkeit in der Situtation, dass $\tilde{L} = \mathbb{C}$ und K ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$ ist. Weil nach dem in der Funktionentheorie-Vorlesung bewiesenen *Fundamentalsatz der Algebra* jedes Polynom $f \in \mathbb{C}[x]$ über $\mathbb{C}$ in Linearfaktoren zerfällt, besitzt jede Menge $S \subseteq K[x]$ nicht-konstanter Polynome über einem solchen Zwischenkörper K, erst recht jedes einzelne nicht-konstante Polynom, einen eindeutig bestimmten Zerfällungskörper in $\mathbb{C}$.

Wir wenden uns nun einem besonders wichtigen Typ von Zerfällungskörpern zu, dem *algebraischen Abschluss* eines Körpers K. Zunächst definieren wir

Definition 13.5 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 $\text{grad}(f)$ 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 13.6 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 13.7 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 $f \in K[x]$ 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 $f = \mu_{K,\alpha}$ 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. Sei $S_K \subseteq K[x]$ die Menge aller nicht-konstanten Polynome und $N = \{\alpha \in L \mid f(\alpha) = 0 \text{ für ein } f \in S_K\}$. Jedes Polynom $f \in S_K$ zerfällt nicht nur über L, sondern auch über $K(N)$ in Linearfaktoren. Auf Grund der Minimalitätseigenschaft gilt also $L = K(N)$. Die über K algebraischen Elemente in L bilden nach Satz 11.9 einen Teilkörper T von L, der offenbar K und N enthält. Es gilt also $K(N) \subseteq T \subseteq L$. Daraus folgt $T = L$, die Erweiterung $L|K$ ist also algebraisch.

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 11.9 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 13.8 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 13.7 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, denn jedes $\alpha \in L$ ist jeweils Nullstelle von $\mu_{K,\alpha} \in S_K$. Also ist L ein Zerfällungskörper von S_K über K. □

Wegen Satz 13.2 ergibt sich aus Folgerung 13.8, 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, und dieser ist nach Satz 13.4 eindeutig bestimmt. Die Behauptung folgt ist somit eine Konsequenz von Folgerung 13.8. 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 13.9 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 wir 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 12.2, 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 13.10 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 13.9 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 12.3 eine Nullstelle von $\tilde{f} = \phi(f)$. Es folgt $\psi(\alpha) \in \tilde{N}$ und insgesamt $\psi(N) \subseteq \tilde{N}$. Mit Lemma 12.6 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 13.11 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 13.8 sind L und $\tilde{L}$ beide Zerfällungskörper der Menge S_K aller nicht-konstanten Polynome über K. Somit existiert nach Satz 13.10 ein Isomorphismus $\psi : L \to \tilde{L}$ mit $\psi|_K = \mathrm{id}_K$, also ein K-Isomorphismus. □

Anhang: Unendliche algebraische Erweiterungen und Zornsches Lemma

In diesem Anhang werden die vollständigen Beweise von Satz 13.2 und Proposition 13.9 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 13.12 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 13.13 *(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 $\mathscr{X}$, deren Elemente selbst Mengen sind, eine Menge C existiert, die aus jedem $X \in \mathscr{X}$ genau ein Element

enthält, und keine weiteren Elemente. Wir können also eine Menge bilden, indem wir aus jeder Menge $X \in \mathscr{X}$ 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 Mengen 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 13.14 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 $\mathscr{M}$ 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 $\mathscr{M}$ enthalten. Auf $\mathscr{M}$ 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 $(A_1, f_1), (A_2, f_2) \in \mathscr{M}$. Zunächst weisen wir nach, dass $\preceq$ eine Halbordnung auf $\mathscr{M}$ ist. Die Reflexivität ist offensichtlich, denn für jedes Paar $(A, f) \in \mathscr{M}$ 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 $(A_1, f_1), (A_2, f_2), (A_3, f_3) \in \mathscr{M}$ 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 $(\mathscr{M}, \preceq)$ die Voraussetzungen des Zornschen Lemmas erfüllt. Dass $\mathscr{M}$ nichtleer ist, haben wir bereits festgestellt. Sei nun $\mathscr{T}$ eine nichtleere Kette in $\mathscr{M}$. Zu zeigen ist, dass $\mathscr{T}$ in $\mathscr{M}$ eine obere Schranke besitzt. Dafür sei $A_{\mathscr{T}} \subseteq X$ die Vereinigung aller Mengen A, für die eine Abbildung $f : A \to Y$ mit $(A, f) \in \mathscr{T}$ existiert. Wir definieren eine Abbildung $f : A_{\mathscr{T}} \to Y$, indem wir für jedes $a \in A_{\mathscr{T}}$ ein Paar $(A, f_a) \in \mathscr{T}$ mit $a \in A$ wählen und $f_{\mathscr{T}}(a) = f_a(a)$ setzen. Das Bild $f_{\mathscr{T}}(a)$ ist von der Wahl des Paares (A, f_a) unabhängig. Ist nämlich $(A', f') \in \mathscr{T}$ ein weiteres Element mit $a \in A'$, dann gilt $(A, f_a) \preceq (A', f')$ oder $(A', f') \preceq (A, f_a)$, weil $\mathscr{T}$ 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 $(A_{\mathscr{T}}, f_{\mathscr{T}})$ in $\mathscr{M}$ liegt und eine obere Schranke von $\mathscr{T}$ ist. Für Ersteres müssen wir noch zeigen, dass $f_{\mathscr{T}}$ injektiv ist. Seien also $a_1, a_2 \in A_{\mathscr{T}}$ mit $f_{\mathscr{T}}(a_1) = f_{\mathscr{T}}(a_2)$ vorgegeben. Auf Grund der Definition von $A_{\mathscr{T}}$ gibt es Paare $(A_1, f_1), (A_2, f_2) \in \mathscr{T}$ mit $a_1 \in A_1$, $a_2 \in A_2$, und unsere Feststellung aus dem vorherigen Absatz zeigt, dass $f_1(a_1) = f_{\mathscr{T}}(a_1) = f_{\mathscr{T}}(a_2) = f_2(a_2)$ gilt. Weil $\mathscr{T}$ 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 $(A_{\mathscr{T}}, f_{\mathscr{T}})$ nachgewiesen. Ist nun $(A, f) \in \mathscr{T}$ beliebig vorgegeben, dann gilt $A_{\mathscr{T}} \supseteq A$ nach Definition von $A_{\mathscr{T}}$, und für jedes $a \in A$ ist $f_{\mathscr{T}}(a) = f(a)$, also $f_{\mathscr{T}}|_A = f$. Also gilt $(A, f) \preceq (A_{\mathscr{T}}, f_{\mathscr{T}})$, und somit ist $(A_{\mathscr{T}}, f_{\mathscr{T}})$ in der Tat eine obere Schranke von $\mathscr{T}$.

Nach dem Zornschen Lemma 13.13 existiert in $\mathscr{M}$ 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 $\mathscr{M}$ 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 13.9 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 $\mathscr{F}$ 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 $\mathscr{F}$, 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 $(M_1, \psi_{M_1}), (M_2, \psi_{M_2}) \in \mathscr{F}$ gilt. Wegen $(K, \phi) \in \mathscr{F}$ ist die Menge $\mathscr{F}$ nicht leer. Ähnlich wie im Beweis von Satz 13.14 überprüft man, dass durch $\preceq$ eine Halbordnung auf $\mathscr{F}$ definiert ist; der einzige Unterschied besteht darin, dass an Stelle von Abbildungen nun Körperhomomorphismen betrachtet werden.

Nun zeigen wir, dass die halbgeordnete Menge $(\mathscr{F}, \preceq)$ die Voraussetzungen des Zornschen Lemmas erfüllt. Sei $\mathscr{T} \subseteq \mathscr{F}$ eine nichtleere Kette in $\mathscr{F}$. Weiter sei $M_{\mathscr{T}}$ die Vereinigung aller Zwischenkörper M von $L|K$, für die ein Körperhomomorphismen $\psi_M : M \to \tilde{K}$ mit $(M, \psi_M) \in \mathscr{T}$ existiert. Dann ist auch $M_{\mathscr{T}}$ ein Zwischenkörper von $L|K$. Zunächst ist das Einselement $1_K = 1_L$ in $M_{\mathscr{T}}$ enthalten, denn weil M für jedes Element (M, ψ_M) aus $\mathscr{T}$ ein Teilkörper von L ist, gilt jeweils $1_K \in M$. Seien nun $\alpha, \beta \in M_{\mathscr{T}}$ vorgegeben. Dann gibt es Elemente $(M_\alpha, \psi_{M_\alpha}), (M_\beta, \psi_{M_\beta}) \in \mathscr{T}$ mit $\alpha \in M_\alpha$ und $\beta \in M_\beta$. Weil $\mathscr{T}$ 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 $M_{\mathscr{T}}$ all diese Elemente. Damit ist die Teilkörpereigenschaft nachgewiesen.

Außerdem definieren wir eine Abbildung $\psi_{\mathscr{T}} : M_{\mathscr{T}} \to \tilde{K}$, indem wir für jedes $\alpha \in M_{\mathscr{T}}$ ein Element $(M_\alpha, \psi_{M_\alpha})$ mit $\alpha \in M_\alpha$ auswählen und $\psi_{\mathscr{T}}(\alpha) = \psi_{M_\alpha}(\alpha)$ setzen. Ist $\alpha \in K$, dann gilt $\psi_{\mathscr{T}}(\alpha) = \psi_{M_\alpha}(\alpha) = \phi(\alpha)$, weil ψ_{M_α} eine Fortsetzung von ϕ ist. Außerdem ist $\psi_{\mathscr{T}}$ ein Körperhomomorphismus. Dazu bemerken wir zunächst: Ist $\alpha \in M_{\mathscr{T}}$ und $(M, \psi_M) \in \mathscr{T}$ ein beliebiges Element mit $\alpha \in M$, dann gilt $\psi_{\mathscr{T}}(\alpha) = \psi_M(\alpha)$. Denn weil $\mathscr{T}$ 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 $\psi_M(\alpha) = (\psi_{M_\alpha}|_M)(\alpha) = \psi_{M_\alpha}(\alpha) = \psi_{\mathscr{T}}(\alpha)$, und durch eine ähnliche Rechnung erhält man dasselbe Resultat auch im zweiten Fall. Seien nun $\alpha, \beta \in M_{\mathscr{T}}$ vorgegeben, und es seien $(M_\alpha, \psi_{M_\alpha}), (M_\beta, \psi_{M_\beta})$ Elemente aus $\mathscr{T}$ 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

$$\psi_{\mathscr{T}}(\alpha+\beta) \quad = \quad \psi_{M_\beta}(\alpha+\beta) \quad = \quad \psi_{M_\beta}(\alpha) + \psi_{M_\beta}(\beta) \quad = \quad \psi_{\mathscr{T}}(\alpha) + \psi_{\mathscr{T}}(\beta)$$

und ebenso $\psi_{\mathscr{T}}(\alpha\beta) = \psi_{\mathscr{T}}(\alpha)\psi_{\mathscr{T}}(\beta)$. Ebenso gilt $\psi_{\mathscr{T}}(1_K) = \psi_{M_\beta}(1_K) = \phi(1_K) = 1_{\tilde{K}}$, weil ψ_{M_β} eine Fortsetzung von ϕ ist. Nach Konstruktion gilt $M \subseteq M_{\mathscr{T}}$ und $\psi_{\mathscr{T}}|_M = \psi_M$ für jedes $(M, \psi_M) \in \mathscr{T}$. Also ist $(M_{\mathscr{T}}, \psi_{\mathscr{T}})$ tatsächlich eine obere Schranke von $\mathscr{T}$.

Auf Grund des Zornschen Lemmas, Satz 13.13, existiert nun in $\mathscr{F}$ 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 11.8 um eine endliche Erweiterung. Da Satz 13.9 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 $\mathscr{F}$ 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 13.2 über die Existenz von Zerfällungskörpern für beliebige Mengen nicht-konstanter Polynome vorzubereiten, zeigen wir

Lemma 13.15 Sei X eine Menge und $\mathscr{P}(X)$ ihre Potenzmenge. Dann existiert keine surjektive Abbildung $\phi : X \to \mathscr{P}(X)$.

Beweis: Die Argumentation ähnelt dem Cantorschen Diagonalverfahren, mit dem gezeigt wird, dass die reellen Zahlen surjektiv sind. Nehmen wir an, $\phi : X \to \mathscr{P}(X)$ 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 13.16 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 $\Omega = \mathscr{P}(\Omega_0)$, die Potenzmenge von Ω. 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 13.15 existiert keine surjektive Abbildung von Ω_0 auf Ω. □

Nun kann der Beweis von Satz 13.2 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 13.16 (ii). Nach Ersetzung von Ω durch $\Omega \cup K$ dürfen wir $\Omega \supseteq K$ annehmen. Es sei nun $\mathscr{F}$ 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 $\emptyset \subseteq S$. Wir definieren eine Relation $\preceq$ auf $\mathscr{F}$, 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 $L_1, L_2 \in \mathscr{F}$ 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 $\mathscr{F}$ gegeben ist. Die Relation ist reflexiv, denn jedes $L \in \mathscr{F}$ ist ein Teilkörper von sich selbst. Sind $L_1, L_2 \in \mathscr{F}$ 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 $L_1, L_2, L_3 \in \mathscr{F}$ 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 $\mathscr{T}$ in $\mathscr{F}$ eine obere Schranke besitzt. Auf der Teilmenge $L_{\mathscr{T}} = \bigcup_{L \in \mathscr{T}} L$ von Ω definieren wir auf folgende Weise Verknüpfungen $+_{\mathscr{T}}$ und $\cdot_{\mathscr{T}}$: Sind $\alpha, \beta \in L_{\mathscr{T}}$ vorgegeben, dann gibt es einen Körper $L_1 \in \mathscr{T}$ mit $\alpha \in L_1$ und ein $L_2 \in \mathscr{T}$ mit $\beta \in L_2$. Weil $\mathscr{T}$ 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 $L_{\mathscr{T}}$ können wir also einen Körper $L_{(\alpha,\beta)} \in \mathscr{T}$ 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

$$\alpha +_{\mathscr{T}} \beta = \alpha +_{(\alpha,\beta)} \beta \quad , \quad \alpha \cdot_{\mathscr{T}} \beta = \alpha \cdot_{(\alpha,\beta)} \beta .$$

Zu überprüfen ist nun, dass es sich bei $(L_{\mathscr{T}}, +_{\mathscr{T}}, \cdot_{\mathscr{T}})$ 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 $\alpha, \beta, \gamma \in L_{\mathscr{T}}$ vorgegeben, außerdem $\alpha' = \alpha +_{(\alpha,\beta)} \beta$ und $\gamma' = \beta +_{(\beta,\gamma)} \gamma$. Weil $\mathscr{T}$ 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

$$\begin{aligned}(\alpha +_{\mathscr{T}} \beta) +_{\mathscr{T}} \gamma &= (\alpha +_{(\alpha,\beta)} \beta) +_{\mathscr{T}} \gamma = \alpha' +_{\mathscr{T}} \gamma = \alpha' +_{(\alpha',\gamma)} +\gamma \\ = \alpha' +_L \gamma &= (\alpha +_L \beta) +_L \gamma = \alpha +_L (\beta +_L \gamma) = \alpha +_L \gamma' = \alpha +_{(\alpha,\gamma')} +\gamma' = \\ &\alpha +_{\mathscr{T}} \gamma' = \alpha +_{\mathscr{T}} (\beta +_{\beta,\gamma} \gamma) = \alpha +_{\mathscr{T}} (\beta +_{\mathscr{T}} \gamma).\end{aligned}$$

Der Nachweis der übrigen Körperaxiome funktioniert nach dem gleichen Schema; dabei stellt man insbesondere fest, dass Null- bzw. Einselement von $L_{\mathscr{T}}$ mit Null- und Einselement des Grundkörpers K übereinstimmen. Darüber hinaus ist jedes $L \in \mathscr{T}$ ein Teilkörper von $L_{\mathscr{T}}$. 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 $\alpha +_{\mathscr{T}} \beta = \alpha +_{(\alpha,\beta)} \beta$ und $\alpha + \beta$ übereinstimmen. Ebenso stimmt die Multiplikation von $L_{\mathscr{T}}$ mit der Multiplikation von L überein. Weil K ein Teilkörper von L ist, gilt $1_L = 1_K = 1_{L_{\mathscr{T}}}$. Weil L ein Körper ist und die Verknüpfungen von L und $L_{\mathscr{T}}$ übereinstimmen, ist L abgeschlossen unter der Subtraktion und der Multiplikation in $L_{\mathscr{T}}$, für Elemente ungleich 0_K auch unter Inversenbildung.

Zeigen wir nun noch, dass $L_{\mathscr{T}}$ Zerfällungskörper einer Teilmenge $T \subseteq S$ ist, dann ist $L_{\mathscr{T}}$ insgesamt eine obere Schranke von $\mathscr{T}$ in $\mathscr{F}$. Nach Definition von $\mathscr{F}$ existiert für jedes $L \in \mathscr{F}$, erst recht für jedes $L \in \mathscr{T}$ eine Teilmenge $T_L \subseteq S$, so dass L Zerfällungskörper von T_L ist. Wir beweisen jetzt, dass $L_{\mathscr{T}}$ Zerfällungskörper von $T = \bigcup_{L \in \mathscr{T}} T_L$ ist. Jedes $f \in T$ ist in einer Teilmenge T_L enthalten. Also zerfällt f über L, und damit auch über dem Erweiterungskörper $L_{\mathscr{T}}$ von L, in Linearfaktoren. Für jedes $L \in \mathscr{T}$ sei $N_L \subseteq L$ jeweils die Menge aller Nullstellen von Polynomen aus T_L. Dann gilt $L = K(N_L)$, und $N = \bigcup_{L \in \mathscr{T}} N_L$ ist die Menge aller Nullstellen von Polynomen aus T. Wir müssen nun $L_{\mathscr{T}} \subseteq K(N)$ nachweisen. Tatsächlich liegt jedes $\alpha \in L_{\mathscr{T}}$ in L für ein $L \in \mathscr{T}$, und somit in $K(N_L) \subseteq K(N)$.

Ingesamt haben wir damit die Voraussetzungen des Zornschen Lemmas verifiziert, und demnach existiert in $\mathscr{F}$ 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 13.1 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 2.12 aus der Zahlentheorie-Vorlesung 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 $\mathscr{F}$ 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 13.14 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. □

§ 14. *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 § 13 verwendet, um die endlichen Körper insgesamt zu klassifizieren. Außerdem diskutieren wir die Teilkörperstruktur und die Automorphismen endlicher Körper.

Wichtige Grundbegriffe

- formale Ableitung eines Polynoms
- Frobenius-Endomorphismus eines Rings der Charakteristik p

Zentrale Sätze

- 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")

Satz 14.1 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 10.2 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 § 13 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 14.2 Sei K ein Körper und $f = \sum_{k=0}^{n} a_k x^k \in K[x]$, mit $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in K$. 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 14.3 Sei K ein Körper, $f \in K[x]$ ein Polynom vom Grad $n \geq 1$ und 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 L nur *einfache* Nullstellen, d.h. es ein $a \in K^\times$ und n verschiedene Elemente $\alpha_1, \ldots, \alpha_n \in L$, so dass $f = a\prod_{i=1}^{n}(x-\alpha_i)$.

Beweis: Sei $\alpha \in L$ 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 $g \in L[x]$ 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 L in Linearfaktoren. Jede Nullstelle von p in L ist eine gemeinsame Nullstelle von f und f' und somit eine mehrfache Nullstelle von f.

Eine mehrfache Nullstelle α von f in 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 14.4 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 14.1 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 14.5 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 $1 \leq k \leq p-1$ 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 $1 \leq k \leq p-1$ also gleich Null, und wir erhalten $(a+b)^p = a^p + b^p$. □

Definition 14.6 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 14.7 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 14.5 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 14.5 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

$$(a^{-1})^{p^n} \quad = \quad a^{-p^n} \quad = \quad (a^{p^n})^{-1} \quad = \quad a^{-1}$$

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 14.3 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 14.8 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 14.7. Sei nun $\tilde{K}$ ein beliebiger Körper mit p^n Elementen und $\tilde{P}$ sein Primkörper. Nach Proposition 14.4 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 13.10 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 14.9 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.

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 14.7. 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 14.4 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 $dm = n$. □

§ 15. *Normale und separable Erweiterungen*

Zusammenfassung. In diesem Abschnitt behandeln wir zwei Eigenschaften algebraischer Körpererweiterungen, die sich im nächsten Kapitel als Voraussetzungen für die Anwendbarkeit der Galoistheorie herausstellen werden. Eine algebraische Erweiterung $L|K$ ist ***normal*** genau dann, wenn L als Zerfällungskörper einer Menge von Polynomen aus $K[x]$ aufgefasst werden kann. Sie ist ***separabel***, wenn das Minimalpolynom jedes Element von L über K nur einfache Nullstellen hat. Wie wir sehen werden, ist diese zweite Bedingung immer erfüllt, wenn K ein Körper der Charakteristik 0 oder ein endlicher Körper ist.

Für beide Eigenschaften gehen wir der Frage nach, inwieweit sie bei Übergang zu Teilerweiterungen erhalten bleibt, und wie sie mit der Existenz von Körperhomomorphismen zusammenhängt. Eine wichtige Eigenschaft endlicher separabler Erweiterungen kommt im Satz vom ***primitiven Element*** zum Ausdruck, welcher besagt, dass solche Erweiterungen stets durch ein einzelnes Element erzeugt werden können. In Anbetracht der Tatsache, dass solche Erweiterungen bei einem Körper wie $\mathbb{Q}$ bereits eine sehr komplizierte Struktur haben können, ist dies eine bemerkenswerte Aussage.

Wichtige Grundbegriffe

- normale Körpererweiterungen
- Konjugierte eines Elements in einer normalen Erweiterung
- separables Polynom
- separables Element in einer Körpererweiterung
- separable Körpererweiterung

Zentrale Sätze

- Charakterisierung normaler Erweiterungen als Zerfällungskörper
- Charakterisierung normaler Erweiterungen durch die Automorphismengruppe
- Charakterisierung durch den Separabilitätsgrad
- Satz vom primitiven Element

Definition 15.1 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 15.2 Sei K ein Körper und $L|K$ eine Erweiterung 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 $\operatorname{grad}(f) = [K(\alpha) : K] \in \{1, 2\}$. Im Fall $\operatorname{grad}(f) = 1$ ist f bereits ein lineares Polynom. Im Fall $\operatorname{grad}(f) = 2$ ist $x - \alpha$ ein Teiler von $f \in L[x]$. Es gibt somit ein Polynom $\operatorname{grad}(g)$ 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 15.3 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) $\Rightarrow$ (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) $\Rightarrow$ (iii)“ Die Inklusion „$\supseteq$“ ist auf Grund der Definition von $\mathrm{Hom}_K(L, \tilde{K})$ und $\mathrm{Aut}_K(L)$ klar. Zum Nachweis von „$\subseteq$“ sei nun $\phi \in \mathrm{Hom}_K(L, \tilde{K})$ vorgegeben. Außerdem setzen wir voraus, dass L der Zerfällungskörper des nicht-konstanten 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 12.3 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 12.6 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) $\Rightarrow$ (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 13.9 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 15.3 (iii) ist jeder $\mathbb{Q}$-Homomorphismus $\phi : L \to \mathbb{C}$ ein $\mathbb{Q}$-Automorphismus von L.

Definition 15.4 Sei $L|K$ eine normale Erweiterung und $\alpha \in L$. Dann werden die Nullstellen des Minimalpolynoms $\mu_{K,\alpha}$ 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 15.3 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 15.3 (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 12.3 auch β eine Nullstelle von f. Zum Schluss untersuchen wir noch, wie sich die Eigenschaft „normal“ bei Türmen von Körpererweiterungen verhält.

Proposition 15.5 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 15.5 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.

Wenden wir uns nun den separablen Erweiterungen zu.

Definition 15.6 Sei K ein Körper. Ein irreduzibles Polynom $f \in K[x]$ wird ***separabel*** genannt, wenn $\mathrm{ggT}(f, f') = 1$ gilt.

Nach Proposition 14.3 ist die Separabilität von f gleichbedeutend damit, dass f irreduzibel ist und in jedem Erweiterungskörper L von K nur einfache Nullstellen besitzt.

Definition 15.7 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 15.8 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 15.9 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 15.10 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 14.3. □

In Anbetracht der Sätze 15.9 und 15.10 drängt sich die Frage auf, ob es überhaupt Körper mit nicht-separablen algebraischen Erweiterungen gibt. Sei p eine Primzahl, $L = \mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$ und $K = \mathbb{F}_p(t^p)$. Dann ist das Element $\alpha = t \in L$ nicht separabel über K. Um dies zu sehen, bemerken wir zunächst, dass das Polynom $f = x^p - t^p \in K[x]$ das Element $\alpha = t$ als Nullstelle besitzt und über L in Linearfaktoren zerfällt, denn wegen $\text{char}(L) = p$ gilt $f = (x-t)^p$. Wäre f über K reduzibel, dann hätte ein Teiler $g \in K[x]$ von f die Form $(x-t)^m$ mit $1 \leq m < p$. Aber der konstante Term $(-1)^m t^m$ von g ist nicht in K enthalten, denn für jedes Element $u/v \in K$ mit $u, v \in \mathbb{F}_p[t]$ ist die Zahl $\text{grad}(u) - \text{grad}(v)$ durch p teilbar. Also ist f über K irreduzibel und somit das Minimalpolynom von α. Da f aber in L eine p-fache Nullstelle hat, ist es nicht separabel.

Proposition 15.11 Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann gilt

$$|\mathrm{Hom}_K(L,\tilde{K})| \quad \leq \quad [L:K]$$

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 12.4 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 α separabel über K ist. Denn genau dann sind f und damit auch $\tilde{f}$ über K separabel (denn die Bedingung $\mathrm{ggT}(f,f') = 1$ bleibt unter dem Körperhomomorphismus ϕ erhalten), und genau dann besitzt $\tilde{f}$ in $\tilde{K}$ genau m verschiedene Nullstellen. Wir bezeichnen die verschiedenen Fortsetzungen von ϕ mit $\psi_1, ..., \psi_{m_1}$.

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 15.8 auch separabel über $K(\alpha)$, die Erweiterung $L|K(\alpha)$ also separabel. Nach Induktionsvoraussetzung besitzt jedes ψ_i genau r Fortsetzungen. Insgesamt existieren damit 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 $mr = [L:K]$. □

Man bezeichnet $|\mathrm{Hom}_K(L,\tilde{K})|$ als den ***Separabilitätsgrad*** $[L:K]_s$ der Erweiterung $L|K$; er ist von der Wahl des Körpers $\tilde{K}$ unabhängig. Denn zunächst einmal ist jedes $\sigma \in \mathrm{Hom}_K(L,\tilde{K})$ ein K-Isomorphismus von L auf sein Bild $\sigma(L)$ und damit eine endliche Erweiterung und insbesondere algebraische Erweiterung von K. Das Bild ist also im algebraischen Abschluss von K innerhalb des Körper $\tilde{K}$ enthalten, so dass sich $\mathrm{Hom}_K(L,\tilde{K})$ nicht ändert, wenn wir $\tilde{K}$ durch diesen algebraischen Abschluss ersetzen. Außerdem existiert nach Folgerung 13.11 zwischen je zwei algebraischen Abschlüssen $\tilde{K}_1$ und $\tilde{K}_2$ ein K-Isomorphismus ϕ, so dass zwischen $\mathrm{Hom}_K(L,\tilde{K}_1)$ und $\mathrm{Hom}_K(L,\tilde{K}_2)$ durch $\sigma \mapsto \phi \circ \sigma$ eine Bijektion gegeben ist.

Wir kommen nun zu einer wichtigen Eigenschaft separabler Erweiterungen.

Definition 15.12 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.

Es gilt nun der wichtige

Satz 15.13 *(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

$$\gamma_c \quad = \quad \alpha + c\beta \qquad \text{und} \qquad M_c \quad = \quad K(\gamma_c).$$

Wir werden zeigen, dass c so gewählt werden kann, dass $M_c = K(\alpha, \beta)$ erfüllt ist. Dazu betrachten wir das Polynom $h_c \in M_c[x]$ gegeben durch

$$h_c \quad = \quad f(\gamma_c - cx) \quad = \quad \prod_{i=1}^{m}((\gamma_c - cx) - \alpha_i) \quad = \quad \prod_{i=1}^{m}(\gamma_c - (\alpha_i + cx)).$$

Wir bezeichnen die einzelnen Linearfaktoren $\gamma_c - (\alpha_i + cx)$ von h_c mit $h_{c,i}$. Das Polynom h_c ist so konstruiert, dass es $\beta = \beta_1$ auf jeden Fall als Nullstelle besitzt, denn nach Definition gilt

$$h_{c,1}(\beta) \quad = \quad \gamma_c - (\alpha_1 + c\beta) \quad = \quad \gamma_c - (\alpha + c\beta) \quad = \quad \gamma_c - \gamma_c \quad = \quad 0$$

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 $2 \le j \le n$ gilt nämlich

$$h_{c,i}(\beta_j) \quad = \quad \gamma_c - (\alpha_i + c\beta_j) \quad = \quad (\alpha + c\beta) - (\alpha_i + c\beta_j) \quad = \quad (\alpha - \alpha_i) + c(\beta - \beta_j).$$

Weil K unendlich ist, können wir c so wählen, dass

$$c \neq -\frac{\alpha - \alpha_i}{\beta - \beta_j} \quad \text{für} \quad 1 \le i \le m, 2 \le j \le n \qquad \Leftrightarrow \qquad h_{c,i}(\beta_j) \neq 0 \quad \text{für} \quad 1 \le i \le m, 2 \le j \le n$$
$$\Leftrightarrow \qquad h_c(\beta_j) \neq 0 \quad \text{für} \quad 2 \le j \le n$$

erfüllt ist. In diesm Fall ist dann $x - \beta_1$ der einzige Linearfaktor von g, der auch das Polynom h_c teilt.Es gilt also

$$x - \beta \quad = \quad \text{ggT}(g, h_c).$$

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 $K(\alpha, \beta) = K(\gamma_c)$. □

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 15.14 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 $M = K(a_0, ..., a_{n-1})$.

Beweis: Sei $M_0 = K(a_0, ..., a_{n-1})$. 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 15.15 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 15.14 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 15.16 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 15.15 besitzt $L|K$ deshalb nur endlich viele Zwischenkörper. □

§ 16. *Der Hauptsatz der Galoistheorie*

Zusammenfassung. Der Hauptsatz der Galoistheorie verbindet zwei Teilgebiete der Algebra miteinander, die Gruppen- und die Körpertheorie. Genauer gesagt wird jeder endlichen, normalen und separablen Erweiterung $L|K$ eine endliche Gruppe $\mathrm{Gal}(L|K)$ zugeordnet, die sog. ***Galois-Gruppe***. Anhand der Gruppenstruktur lässt sich feststellen, wieviele Zwischenkörper die Erweiterung $L|K$ besitzt, wie diese innerhalb der Erweiterung $L|K$ angeordnet sind, welche Erweiterungsgrade diese über dem Grundkörper K haben, und welche davon normale Erweiterungen über K sind.

Auch nicht-konstanten Polynomen $f \in K[x]$ kann eine Galoisgruppe zugeordnet werden: Man wählt einen Zerfällungskörper L von f über K und definiert $\mathrm{Gal}(f|K) = \mathrm{Gal}(L|K)$. Nummeriert man die n Nullstellen von f in L in beliebiger Weise, dann kann $\mathrm{Gal}(f|K)$ mit einer Untergruppe der symmetrischen Gruppe S_n identifiziert werden, und einzelne Elemente mit Permutationen. All dies werden wir durch konkrete Beispiele illustrieren.

Wichtige Grundbegriffe

- Galois-Erweiterung
- Galois-Gruppe $\mathrm{Gal}(L|K)$ einer Galois-Erweiterung $L|K$
- Galois-Gruppe $\mathrm{Gal}(f|K)$ eines Polynoms $f \in K[x]$

Zentrale Sätze

- Hauptsatz der Galoistheorie und Ergänzungen
- Identifikation von Galois-Gruppen von Polynomen mit Untergruppen von symmetrischen Gruppen
- Verschiebungssatz der Galoistheorie

Definition 16.1 Eine Körpererweiterung $L|K$ wird ***Galois-Erweiterung*** genannt, wenn sie normal und separabel ist. Die Gruppe $\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$ heißt dann die ***Galoisgruppe*** der Erweiterung $L|K$.

Ist $L|K$ eine Galois-Erweiterung und M ein Zwischenkörper von $L|K$, dann ist auch $L|M$ eine Galois-Erweiterung. Dies folgt aus den Propositionen 15.5 und 15.8. Somit können wir auch die Galoisgruppe $\mathrm{Gal}(L|M)$ bilden. Es handelt sich dabei um eine Untergruppe von $\mathrm{Gal}(L|K)$, denn wegen $M \supseteq K$ ist jeder M-Automorphismus auch ein K-Automorphismus des Körpers L.

Damit haben wir also einen Weg gefunden, jedem Zwischenkörper von $L|K$ eine Untergruppe von $\mathrm{Gal}(L|K)$ zuzuordnen. Wir überlegen uns nun, wie man umgekehrt von einer Untergruppe zu einem Zwischenkörper kommt.

Definition 16.2 Sei L ein Körper und G eine Untergruppe von $\mathrm{Aut}(L)$. Dann nennt man $L^G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \forall\, \sigma \in G\}$ den ***Fixkörper*** von G.

Man überprüft unmittelbar, dass L^G ein Teilkörper von L ist: Wegen $\sigma(1_L) = 1_L$ für alle $\sigma \in G$ liegt 1_L in L^G. Sind $\alpha, \beta \in L^G$ und $\sigma \in G$, dann gilt

$$\sigma(\alpha-\beta) \quad = \quad \sigma(\alpha)-\sigma(\beta) \quad = \quad \alpha-\beta_1 \quad , \quad \sigma(\alpha\beta) \quad = \quad \sigma(\alpha)\sigma(\beta) \quad = \quad \alpha\beta.$$

Ist $\alpha \neq 0_L$, dann ist wegen $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$ für alle $\sigma \in G$ auch α^{-1} in L^G enthalten.

Proposition 16.3 Sei L ein Körper, $G \leq \mathrm{Aut}(L)$ eine endliche Untergruppe und $K = L^G$ der zugehörige Fixkörper.

(i) Sei $\alpha \in L$ und $G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$. Sind $\alpha_1, ..., \alpha_r$ die verschiedenen Elemente der Menge $G(\alpha)$, dann ist das Polynom $f = \prod_{i=1}^{r}(x - \alpha_i)$ das Minimalpolynom von α über dem Grundkörper K.

(ii) Die Erweiterung $L|K$ ist galoissch.

Beweis: zu (i) Zunächst zeigen wir, dass f in $K[x]$ liegt. Sei $\tau \in G$ ein beliebiges Element. Dann gilt $\tau(f) = \prod_{i=1}^{r}(x - \tau(\alpha_i))$. Ist $\beta \in G(\alpha)$, $\beta = \sigma(\alpha)$ für ein $\sigma \in G$, dann liegt $\tau(\beta) = (\tau \circ \sigma)(\alpha)$ ebenfalls in $G(\alpha)$. Die Menge $G(\alpha)$ wird also durch τ in sich abgebildet. Weil τ als Automorphismus injektiv und $G(\alpha)$ endlich ist, ist durch $\tau|_{G(\alpha)}$ eine Permutation von $G(\alpha)$ gegeben. Da die Elemente aus $G(\alpha)$ die verschiedenen Nullstellen von f sind, folgt $\tau(f) = f$. Dies bedeutet, dass sich die Koeffizienten von f durch Anwendung von τ nicht ändern. Weil $\tau \in G$ beliebig gewählt war, folgt $f \in L^G[x] = K[x]$.

Nun beweisen wir, dass es sich bei f um das Minimalpolynom von α über K handelt. Wegen $f(\alpha) = 0$ ist α algebraisch über K. Ist $g \in K[x]$ das Minimalpolynom von α über K, dann ist g ein Teiler von f. Für jedes $\sigma \in G$ ist $g(\sigma(\alpha)) = \sigma(g)(\alpha) = g(\alpha) = 0$. Dies bedeutet, dass g durch sämtliche Linearfaktoren $x - \sigma(\alpha)$ des Polynoms f teilbar ist. Also gilt auch $f|g$. Weil f und g beide normiert sind, erhalten wir insgesamt $f = g$.

zu (ii) Zunächst zeigen wir, dass $L|K$ normal ist. Sei $f \in K[x]$ ein irreduzibles, normiertes Polynom, dass in L eine Nullstelle α besitzt. Wie wir in Teil (i) gezeigt haben, gilt $f = \prod_{i=1}^{r}(x - \alpha_i)$, wobei $\alpha_1, ..., \alpha_r$ die verschiedenen Elemente der Menge $G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$ bezeichnen. Dies zeigt, dass f über L in Linearfaktoren zerfällt. Also ist $L|K$ normal.

Nun beweisen wir die Separabilität. Ist $\alpha \in L$ und $f \in K[x]$ das Minimalpolynom von α über K, dann gilt (wie soeben gezeigt) $f = \prod_{i=1}^{r}(x - \alpha_i)$ mit verschiedenen Elementen $\alpha_1, ..., \alpha_r \in L$. Also ist α separabel über K. Weil $\alpha \in L$ beliebig gewählt war, ist die Erweiterung $L|K$ separabel. □

Proposition 16.4 Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann gilt

$$|\mathrm{Aut}_K(L)| \quad \leq \quad |\mathrm{Hom}_K(L, \tilde{K})| \quad \leq \quad [L : K].$$

Beweis: Die erste Ungleichung folgt direkt aus der Inklusion $\mathrm{Aut}_K(L) \subseteq \mathrm{Hom}_K(L, \tilde{K})$, und die zweite Ungleichung ist ein Teil von Proposition 15.11. □

Satz 16.5 Für eine endliche Erweiterung $L|K$ sind folgende Aussagen äquivalent:

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

(ii) $|\mathrm{Aut}_K(L)| = [L:K]$

(iii) $L^{\mathrm{Aut}_K(L)} = K$

Beweis: Sei $\tilde{K}$ ein algebraischer Abschluss von L.

„(i) $\Rightarrow$ (ii)“ Weil $L|K$ normal ist, gilt $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,\tilde{K})$. Auf Grund der Separabilität von $L|K$ gilt außerdem $|\mathrm{Hom}_K(L,\tilde{K})| = [L:K]$, nach Proposition 15.11.

„(ii) $\Rightarrow$ (iii)“ Sei $K_0 = L^{\mathrm{Aut}_K(L)}$. Dann gilt $K \subseteq K_0$ nach Definition der Gruppe $\mathrm{Aut}_K(L)$, denn jedes $a \in K$ liegt im Fixkörper K_0 von $\mathrm{Aut}_K(L)$. Nach Definition gilt auch $\mathrm{Aut}_{K_0}(L) \subseteq \mathrm{Aut}_K(L)$, denn jeder Automorphismus von L, der alle Element aus K_0 auf sich selbst abbildet, tut dies erst recht für alle Element aus K. Andererseits gilt $\sigma(\alpha) = \alpha$ für alle $\sigma \in \mathrm{Aut}_K(L)$ und $\alpha \in K_0$. Daraus folgt $\mathrm{Aut}_K(L) \subseteq \mathrm{Aut}_{K_0}(L)$, insgesamt $\mathrm{Aut}_K(L) = \mathrm{Aut}_{K_0}(L)$. Wäre $K_0 \supsetneq K$, dann würde

$$[L:K] \quad > \quad [L:K_0] \quad \geq \quad |\mathrm{Aut}_{K_0}(L)| \quad = \quad |\mathrm{Aut}_K(L)|$$

gelten, im Widerspruch zur Voraussetzung.

„(iii) $\Rightarrow$ (i)“ Wegen $|\mathrm{Aut}_K(L)| \leq [L:K]$ ist $G = \mathrm{Aut}_K(L)$ eine endliche Gruppe. Nach Proposition 16.3 und wegen $K = L^G$ ist $L|K$ somit eine normale und separable Erweiterung. □

Ist $L|K$ eine endliche Erweiterung, aber nicht galoissch, dann sind demzufolge auch die Aussagen (ii) und (iii) ungültig. Als Beispiel betrachten wir die Erweiterung $L|K$ mit $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$. Jedes $\sigma \in \mathrm{Aut}_K(L)$ muss als $\mathbb{Q}$-Homomorphismus die Nullstelle $\sqrt[3]{2}$ von $f = x^3 - 2$ auf eine Nullstelle von f in L abbilden. Weil es aber in L neben $\sqrt[3]{2}$ keine weiteren Nullstellen von f gibt, muss $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ gelten, und wegen $L = \mathbb{Q}(\sqrt[3]{2})$ folgt daraus $\sigma = \mathrm{id}_L$. Aus $\mathrm{Aut}_K(L) = \{\mathrm{id}_L\}$ wiederum folgt $L^{\mathrm{Aut}_K(L)} = L^{\{\mathrm{id}_L\}} = L$, also insbesondere $L^{\mathrm{Aut}_K(L)} \neq K$. Auch (ii) ist nicht erfüllt, denn es gilt einerseits $|\mathrm{Aut}_K(L)| = |\{\mathrm{id}_L\}| = 1$, andererseits aber $[L:K] = 3$.

Proposition 16.6 Sei L ein Körper, $G \leq \mathrm{Aut}(L)$ eine endliche Untergruppe und $K = L^G$ der zugehörige Fixkörper. Dann ist $L|K$ eine endliche Galois-Erweiterung, und es gilt $G = \mathrm{Gal}(L|K)$.

Beweis: Nach Proposition 16.3 (ii) ist $L|K$ eine Galois-Erweiterung. Setzen wir $d = |G|$ und ist $\alpha \in L$, dann enthält die Menge $G(\alpha)$ höchstens d Elemente. Sei f das Minimalpolynom von α. Weil die Nullstellen von f nach Proposition 16.3 (i) gerade die Elemente der Menge $G(\alpha)$ sind, gilt $\mathrm{grad}(f) \leq d$. Es gilt also $[K(\alpha):K] \leq d$ für alle $\alpha \in L$.

Sei $\alpha \in L$ so gewählt, dass $[K(\alpha):K]$ maximal ist. Ist nun $\beta \in L$ beliebig, dann gibt es nach dem Satz 15.13 vom primitiven Element ein $\gamma \in L$ mit $K(\alpha,\beta) = K(\gamma)$. Auf Grund der Wahl von α ist $[K(\gamma):K] \leq [K(\alpha):K]$; wegen $K(\alpha) \subseteq K(\gamma)$ folgt $K(\alpha) = K(\gamma)$ und insbesondere $\beta \in K(\alpha)$. Weil β beliebig gewählt war, haben wir somit $L = K(\alpha)$ gezeigt. Es folgt $[L:K] \leq d$, insbesondere ist die Erweiterung $L|K$ endlich. Nach Definition ist G eine Untergruppe von $\mathrm{Gal}(L|K)$; andererseits ist $|\mathrm{Gal}(L|K)| = |\mathrm{Aut}_K(L)| = [L:K] \leq d = |G|$ nach Satz 16.5 (ii). Damit ist $G = \mathrm{Gal}(L|K)$ bewiesen. □

Satz 16.7 *(Hauptsatz der Galoistheorie)*

Sei $L|K$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L|K)$, $\mathscr{U}$ die Menge der Untergruppe von G und $\mathscr{Z}$ die Menge der Zwischenkörper von $L|K$. Dann sind durch die Zuordnungen

$$\phi : \mathscr{U} \longrightarrow \mathscr{Z} \quad , \quad U \mapsto L^U \qquad \text{und} \qquad \psi : \mathscr{Z} \longrightarrow \mathscr{U} \quad , \quad M \mapsto \mathrm{Gal}(L|M)$$

zueinander inverse Bijektionen zwischen $\mathscr{U}$ und $\mathscr{Z}$ gegeben.

Beweis: Sei $M \in \mathscr{Z}$ ein Zwischenkörper. Dann ist $L|M$ galoissch, und nach Satz 16.5 gilt

$$(\phi \circ \psi)(M) \quad = \quad \phi(\mathrm{Gal}(L|M)) \quad = \quad L^{\mathrm{Gal}(L|M)} \quad = \quad M.$$

Sei umgekehrt eine Untergruppe $U \in \mathscr{U}$ vorgegeben. Auf Grund von Proposition 16.6 ist dann $L|M$ mit $M = L^U$ eine Galois-Erweiterung, und es gilt $U = \mathrm{Gal}(L|M)$. Folglich ist

$$(\psi \circ \phi)(U) \quad = \quad \psi(M) \quad = \quad \mathrm{Gal}(L|M) \quad = \quad U.$$

Dies zeigt, dass die Abbildungen ϕ und ψ tatsächlich zueinander invers sind. □

Wir beweisen zum Hauptsatz der Galoistheorie noch einige ergänzende Aussagen, mit denen sich die bijektive Korrespondenz genauer beschreiben lässt.

Satz 16.8

(i) Sind $U_1, U_2 \in \mathscr{U}$ mit $U_1 \subseteq U_2$, dann folgt $L^{U_1} \supseteq L^{U_2}$.

(ii) Sind umgekehrt $M_1, M_2 \in \mathscr{Z}$ mit $M_1 \subseteq M_2$, dann ist $\mathrm{Gal}(L|M_1) \supseteq \mathrm{Gal}(L|M_2)$.

(iii) Es gilt $L^{\{\mathrm{id}_L\}} = L$, $L^G = K$ und $\mathrm{Gal}(L|L) = \{\mathrm{id}_L\}$, $\mathrm{Gal}(L|K) = G$.

(iv) Ist M ein Zwischenkörper und $U = \mathrm{Gal}(L|M)$ die zugehörige Untergruppe, dann gilt $[L : M] = |U|$ und $[M : K] = (G : U)$.

Beweis: Die Aussagen (i) und (ii) können unmittelbar nachgerechnet werden. Für (i) sei beispielsweise $\alpha \in L^{U_2}$ vorgegeben. Dann gilt $\sigma(\alpha) = \alpha$ für alle $\sigma \in U_2$, wegen $U_2 \supseteq U_1$ damit erst recht für alle $\sigma \in U_1$. Daraus folgt $\alpha \in L^{U_1}$. Unter (iii) ebenso offensichtlich sind die Gleichungen $L^{\mathrm{id}_L} = L$, $\mathrm{Gal}(L|K) = G$ und $\mathrm{Gal}(L|L) = \{\mathrm{id}_L\}$. Die Gleichung $L^G = L^{\mathrm{Aut}_K(L)} = K$ folgt aus Satz 16.5. Die erste Aussage unter (iv) folgt aus der Tatsache, dass $L|M$ eine Galois-Erweiterung ist und nach Satz 16.5 somit $|\mathrm{Gal}(L|M)| = |\mathrm{Aut}_L(M)| = [L : M]$ gilt. Die zweite Gleichung erhält man durch

$$[M : K] \quad = \quad \frac{[L : K]}{[L : M]} \quad = \quad \frac{|G|}{|U|} \quad = \quad (G : U).$$ □

Proposition 16.9 Sei M ein Zwischenkörper von $L|K$ und $U = \mathrm{Gal}(L|M)$ die zugehörige Untergruppe von $G = \mathrm{Gal}(L|K)$. Dann sind folgende Aussagen äquivalent:

(i) Die Erweiterung $M|K$ ist normal.

(ii) Die Untergruppe U ist Normalteiler von G.

In diesem Fall erhalten wir durch $\sigma \mapsto \sigma|_M$ eine Abbildung $G \to \mathrm{Gal}(M|K)$, und diese induziert einen natürlichen Isomorphismus $G/U \cong \mathrm{Gal}(M|K)$.

Beweis: Wir zeigen zunächst, dass für jedes $\sigma \in G$ die Gleichung $\mathrm{Gal}(L|\sigma(M)) = \sigma U \sigma^{-1}$ erfüllt ist. Für beliebiges $\tau \in G$ gilt die Äquivalenz

$$\tau \in \mathrm{Gal}(L|\sigma(M)) \quad \Leftrightarrow \quad \tau(\alpha) = \alpha \ \forall\ \alpha \in \sigma(M) \quad \Leftrightarrow \quad \tau(\sigma(\alpha)) = \sigma(\alpha) \ \forall\ \alpha \in M \quad \Leftrightarrow$$

$$(\sigma^{-1} \circ \tau \circ \sigma)(\alpha) = \alpha \ \forall\ \alpha \in M \quad \Leftrightarrow \quad \sigma^{-1} \circ \tau \circ \sigma \in U \quad \Leftrightarrow \quad \tau \in \sigma U \sigma^{-1}.$$

Sei nun $\tilde{L}$ ein algebraischer Abschluss von L.

„(i) ⇒ (ii)“ Sei $\sigma \in G$ vorgegeben. Zu zeigen ist $\sigma U \sigma^{-1} = U$. Schränken wir σ auf M ein, dann erhalten wir einen K-Homomorphismus $M \to \tilde{L}$. Weil $M|K$ normal ist, handelt es sich bei $\sigma|_M$ um einen K-Automorphismus von M (siehe Satz 15.3). Insbesondere gilt $\sigma(M) = M$. Es folgt

$$\sigma U \sigma^{-1} \quad = \quad \mathrm{Gal}(L|\sigma(M)) \quad = \quad \mathrm{Gal}(L|M) \quad = \quad U.$$

Weil $\sigma \in G$ beliebig gewählt war, erhalten wir $U \trianglelefteq G$.

“(ii) ⇒ (i)“ Wir zeigen, dass $M|K$ das Kriterium (iii) aus Satz 15.3 erfüllt. Sei dazu ein K-Homomorphismus $\tau : M \to \tilde{L}$ vorgegeben. Nach Proposition 13.9 existiert eine Fortsetzung $\sigma : L \to \tilde{L}$ von τ, also ein K-Homomorphismus mit $\sigma|_M = \tau$. Weil $L|K$ normal ist, gilt $\sigma \in \mathrm{Gal}(L|K)$, und weil U nach Voraussetzung ein Normalteiler von G ist, gilt $\sigma U \sigma^{-1} = U$. Es folgt

$$\mathrm{Gal}(L|\sigma(M)) \quad = \quad \sigma U \sigma^{-1} \quad = \quad U \quad = \quad \mathrm{Gal}(L|M).$$

Weil nach dem Hauptsatz der Galoistheorie die Zuordnung $\mathscr{Z} \to \mathscr{U}$, $M \mapsto \mathrm{Gal}(L|M)$ injektiv ist, erhalten wir $\sigma(M) = M$ und somit auch $\tau(M) = M$. Dies zeigt, dass τ in $\mathrm{Aut}_K(M)$ enthalten ist. Aus Satz 15.3 (iii) folgt, dass die Erweiterung $M|K$ normal ist.

Wir haben bereits festgestellt, dass durch $\sigma \mapsto \sigma|_M$ jedes $\sigma \in G$ nach $\mathrm{Gal}(M|K)$ abgebildet wird. Die Abbildung ist surjektiv, denn jedes $\tau \in \mathrm{Gal}(M|K)$ kann nach Proposition 13.9 zu einem K-Homomorphismus $\sigma : L \to \tilde{L}$ fortgesetzt werden, und weil $L|K$ normal ist, liegt das Element σ in $\mathrm{Aut}_K(L) = G$. Für jedes $\sigma \in G$ gilt offenbar $\sigma|_M = \mathrm{id}_M$ genau dann, wenn σ in $\mathrm{Gal}(L|M)$ enthalten ist. Somit ist $\mathrm{Gal}(L|M)$ genau der Kern der Abbildung $\sigma \mapsto \sigma|_M$, und der Isomorphismus $G/U \cong \mathrm{Gal}(M|K)$ folgt aus dem Homomorphiesatz für Gruppen. □

Anwendungsbeispiel 1
Wir bestimmen für $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ alle Zwischenkörper der Erweiterung $L|\mathbb{Q}$.

Zunächst überprüfen wir, dass es sich um eine Galois-Erweiterung handelt. Als Nullstellen des Polynoms $f \in \mathbb{Q}[x]$ gegeben durch $f = (x^2 - 2)(x^2 - 3)$ sind $\sqrt{2}, \sqrt{3}$ algbraisch über $\mathbb{Q}$. Nach Proposition 11.8 folgt daraus, dass die Erweiterung $L|\mathbb{Q}$ algebraisch ist. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist sie nach Satz 15.9 auch separabel. Darüber hinaus handelt es sich bei L um den Zerfällungskörper des Polynoms f über $\mathbb{Q}$, somit ist $L|\mathbb{Q}$ nach Satz 15.3 auch normal. Denn die

Nullstellen von f in $\mathbb{C}$ sind $\pm\sqrt{2}, \pm\sqrt{3}$, also ist $M = \mathbb{Q}(\{\pm\sqrt{2}, \pm\sqrt{3}\})$ nach Definition der Zerfällungskörper von f über $\mathbb{Q}$. Wegen $\{\pm\sqrt{2}, \pm\sqrt{3}\} \subseteq L$ und $\{\sqrt{2}, \sqrt{3}\} \subseteq M$ stimmen L und M überein.

Im nächsten Schritt bestimmen wir den Erweiterungsgrad $[L : \mathbb{Q}]$, der nach Satz 16.5 mit der Ordnung der Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$ übereinstimmt. Ist $d \in \mathbb{Z} \setminus \{0, 1\}$ kein Quadrat, dann ist die Erweiterung $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}]$ vom Grad 2. Denn $f = x^2 - d \in \mathbb{Q}[x]$ ist normiert und hat $\sqrt{d}$ als Nullstelle; wäre f über $\mathbb{Q}$ reduzibel, dann müssten wegen $\mathrm{grad}(f) = 2$ die beiden Nullstellen $\pm\sqrt{d}$ in $\mathbb{Q}$ liegen, im Widerspruch dazu, dass d in $\mathbb{Q}$ kein Quadrat ist. So aber ist f über $\mathbb{Q}$ irreduzibel, es gilt $f = \mu_{\mathbb{Q},\sqrt{d}}$ und somit $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = \mathrm{grad}(f) = 2$. Nach Satz 11.13 gilt für jede zwei verschiedene quadratfreie Zahlen $d, d' \in \mathbb{Z} \setminus \{1\}$ außerdem jeweils $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{d'}) : \mathbb{Q}] = 2$ und $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$ gilt. Insbesondere gilt also $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ und

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \quad = \quad 2.$$

Darüber hinaus ist $g = x^2 - 3$ das Minimalpolynom von $\sqrt{3}$ über $K = \mathbb{Q}(\sqrt{2})$. Denn wäre g in $K[x]$ irreduzibel, dann würde wegen $\mathrm{grad}(g) = 2$ die Nullstelle $\sqrt{3}$ von g in K liegen. Daraus würde $\mathbb{Q}(\sqrt{3}) \subseteq K$ folgen, und wegen

$$2 \quad = \quad [K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(\sqrt{3})] \cdot 2$$

würden wir $[K : \mathbb{Q}(\sqrt{3})] = 1$ und $\mathbb{Q}(\sqrt{2}) = K = \mathbb{Q}(\sqrt{3})$ erhalten, was aber bereits ausgeschlossen ist. Da g also in $K[x]$ irreduzibel und normiert ist, folgt aus $g(\sqrt{3}) = 0$ tatsächlich die Gleichung $g = \mu_{K,\sqrt{3}}$. Wir erhalten

$$[L : K] \quad = \quad [K(\sqrt{3}) : K] \quad = \quad \mathrm{grad}(\mu_{K,\sqrt{3}}) \quad = \quad 2$$

und mit der Gradformel $|G| = [L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 2 \cdot 2 = 4$.

Nun bestimmen wir den Isomorphietyp der Galoisgruppe G. Aus der Gruppentheorie wissen wir, dass alle Gruppen, deren Ordnung ein Primzahlquadrat ist, abelsch sind. Als endliche abelsche Gruppe ist G isomorph zu einem kartesischen Produkt zyklischer Gruppen. Daraus folgt

$$G \cong \mathbb{Z}/4\mathbb{Z} \qquad \text{oder} \qquad G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Mit dem Hauptsatz der Galoistheorie ermitteln wir nun den korrekten Isomorphietyp. Mit $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ besitzt $L|\mathbb{Q}$ mindestens zwei verschiedene Zwischenkörper, wobei der Erweiterungsgrad über $\mathbb{Q}$ jeweils gleich 2 ist. Seien $U_1 = \mathrm{Gal}(L|\mathbb{Q}(\sqrt{2}))$ und $U_2 = \mathrm{Gal}(L|\mathbb{Q}(\sqrt{3}))$ die zugehörigen Untergruppen. Nach dem Hauptsatz sind diese voneinander verschieden, und nach Satz 16.8 (iv) gilt $|U_1| = [L : \mathbb{Q}(\sqrt{2})] = 2$ und ebenso $|U_2| = [L : \mathbb{Q}(\sqrt{3})] = 2$. Also besitzt G mindestens zwei verschiedene Untergruppen der Ordnung 2. Aber als zyklische Gruppe besitzt $\mathbb{Z}/4\mathbb{Z}$ nur eine Untergruppe dieser Ordnung. Also muss $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gelten.

Im letzten Schritt können wir nun den Hauptsatz der Galoistheorie anwenden, um alle Zwischenkörper der Erweiterung $L|\mathbb{Q}$ anzugeben. Wegen $|G| = 4$ besitzt G nur Untergruppen der Ordnung 1, 2 und 4. Der einzigen Untergruppe $\{\mathrm{id}_L\}$ der Ordnung 1 entspricht nach Satz 16.8 ein eindeutig bestimmter Zwischenkörper von $L|\mathbb{Q}$ vom Grad $(G : \{\mathrm{id}_L\}) = 4$ über $\mathbb{Q}$. Wegen $[L : \mathbb{Q}] = 4$ ist dies offenbar der Körper L. Die einzige Untergruppe von G der Ordnung 4 ist G selbst, und diese entspricht dem Zwischenkörper $\mathbb{Q}$ der Erweiterung $L|\mathbb{Q}$.

Die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ besitzt genau drei Untergruppen der Ordnung 2, nämlich $\langle(\bar{1}, \bar{0})\rangle$, $\langle(\bar{0}, \bar{1})\rangle$ und $\langle(\bar{1}, \bar{1})\rangle$. (Da es sich bei 2 um eine Primzahl handelt, ist jede Untergruppe der Ordnung 2 zyklisch, wird also von einem Element der Ordnung 2 erzeugt.) Wegen $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gibt es also auch in G genau drei Untergruppen U_1, U_2, U_3 der Ordnung 2. Diese entsprechen nach dem Hauptsatz der Galoistheorie drei verschiedenen Zwischenkörpern K_1, K_2, K_3

von $L|\mathbb{Q}$ mit $[K_i : \mathbb{Q}] = (G : U_i) = 2$ für $i = 1,2,3$. Zwei davon sind $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$. Wegen $\sqrt{6} = \sqrt{2} \cdot \sqrt{3} \in L$ muss $\mathbb{Q}(\sqrt{6})$ der dritte dieser Zwischenkörper sein. □

Für die Arbeit mit Galoisgruppen von konkret vorgegebenen Körpererweiterungen ist es oft hilfreich, sie als Untergruppen der symmetrischen Gruppen S_n darzustellen.

Definition 16.10 Sei K ein Körper und $f \in K[x]$ ein nicht-konstantes Polynom, dessen irreduzible Faktoren alle separabel sind, und sei L ein Zerfällungskörper von f über K. Dann bezeichnet man $\mathrm{Gal}(L|K)$ auch als die Galoisgruppe $\mathrm{Gal}(f|K)$ ***des Polynoms*** f.

Man beachte, dass das Polynom f selbst in der Definition nicht irreduzibel zu sein braucht. Die Bedinung an die irreduziblen Faktoren ist auf Grund der Sätze 15.9 und 15.10 immer erfüllt, falls $\mathrm{char}(K) = 0$ gilt oder K ein endlicher Körper ist.

Satz 16.11 Sei $f \in K[x]$ ein Polynom wie in Definition 16.10 und L ein Zerfällungskörper von f über K. Seien $\alpha_1, ..., \alpha_n \in L$ die verschiedenen Nullstellen von f in L. Dann gibt es einen injektiven Homomorphismus

$$\phi : \mathrm{Gal}(f|K) \longrightarrow S_n \qquad \text{mit} \qquad \sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)} \quad \text{für} \quad 1 \le k \le n.$$

Beweis: Sei $G = \mathrm{Gal}(f|K)$ und $S = \{\alpha_1, ..., \alpha_n\} \subseteq L$ die n-elementige Menge der Nullstellen von f. Jedes $\sigma \in G$ ist ein K-Homomorphismus, deshalb ist für jedes $k \in \{1, ..., n\}$ nach Satz 12.3 auch $\sigma(\alpha_k)$ eine Nullstelle von f; es gilt also $\sigma(S) \subseteq S$. Mit σ ist auch $\sigma|_S : S \to S$ eine injektive Abbildung, und als injektive Abbildung zwischen endlichen, gleichmächtigen Mengen ist $\sigma|_S$ auch surjektiv, insgesamt also eine Permutation.

Somit ist durch $\phi_1(\sigma) = \sigma|_S$ also eine Abbildung $G \to \mathrm{Per}(S)$ definiert. Darüber hinaus handelt es sich um einen Gruppenhomomorphismus, denn für alle $\sigma, \tau \in G$ und $k \in \{1, ..., n\}$ gilt $\tau(\alpha_k) \in S$ und somit

$$(\sigma \circ \tau)|_S(\alpha_k) \;=\; (\sigma \circ \tau)(\alpha_k) \;=\; \sigma(\tau(\alpha_k)) \;=\; \sigma|_S(\tau|_S(\alpha_k)) \;=\; (\sigma|_S \circ \tau|_S)(\alpha_k) \quad ,$$

also $\phi_1(\sigma \circ \tau) = (\sigma \circ \tau)|_S = \sigma|_S \circ \tau|_S = \phi_1(\sigma) \circ \phi_1(\tau)$. Nun zeigen wir noch, dass ϕ_1 injektiv ist. Sei $\sigma \in G$ mit $\phi_1(\sigma) = \mathrm{id}_S$. Dann gilt $\sigma(\alpha_k) = \mathrm{id}_S(\alpha_k) = \alpha_k$ für $1 \le k \le n$. Wegen $L = K(\alpha_1, ..., \alpha_k)$ folgt daraus $\sigma = \mathrm{id}_L$; damit ist die Injektivität von ϕ_1 nachgewiesen.

Wie aus der Gruppentheorie bekannt, liefert die Bijektion $\iota : M_n \to S$, $k \mapsto \alpha_k$ einen Isomorphismus $\psi : S_n \to \mathrm{Per}(S)$ von Gruppen, gegeben durch $\tau \mapsto \iota \circ \tau \circ \iota^{-1}$. Somit ist $\phi = \psi^{-1} \circ \phi_1$ ein Monomorphismus von G nach S_n. Zum Schluss beweisen wir noch die Gleichung $\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)}$ für beliebig vorgegebenes $k \in \{1, ..., n\}$ und $\sigma \in G$. Sei ℓ die Nummer der Nullstelle $\alpha_\ell = \sigma(\alpha_k)$. Dann gilt

$$\begin{aligned} \phi(\sigma)(k) \;&=\; (\psi^{-1} \circ \phi_1)(\sigma)(k) \;=\; \psi^{-1}(\phi_1(\sigma))(k) \;=\; \psi^{-1}(\sigma|_S)(k) \;= \\ (\iota^{-1} \circ (\sigma|_S) \circ \iota)(k) \;&=\; (\iota^{-1} \circ (\sigma|_S))(\alpha_k) \;=\; \iota^{-1}(\sigma(\alpha_k)) \;=\; \iota^{-1}(\alpha_\ell) \;=\; \ell. \end{aligned}$$

Es folgt $\alpha_{\phi(\sigma)(k)} = \alpha_\ell = \sigma(\alpha_k)$. □

Anwendungsbeispiel 2
Wir bestimmen alle Zwischenkörper des Zerfällungskörpers von $f = x^3 - 2$ über $\mathbb{Q}$.

Aus den vorherigen Abschnitten wissen wir bereits, dass $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ der Zerfällungskörper von f über $\mathbb{Q}$ in den komplexen Zahlen ist, mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Ebenfalls ist bereits $[L : \mathbb{Q}] = 6$ bekannt. Die Nullstellen des Polynoms f in $\mathbb{C}$ sind gegeben durch

$$\alpha_1 = \sqrt[3]{2} \quad , \quad \alpha_2 = \zeta\sqrt[3]{2} \quad \text{und} \quad \alpha_3 = \zeta^2\sqrt[3]{2}.$$

Sei $G = \mathrm{Gal}(f|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q})$. Nach Satz 16.11 gibt es einen Monomorphismus $\phi : G \to S_3$ mit $\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)}$ für alle $\sigma \in K$ und $k \in \{1, 2, 3\}$. Wegen $|G| = [L : \mathbb{Q}] = 6 = |S_3|$ ist ϕ sogar ein Isomorphismus zwischen G und S_3.

Wir überlegen nun, welche Informationen uns der Hauptsatz der Galoistheorie über die Zwischenkörper der Erweiterung $L|\mathbb{Q}$ liefert. Aus unseren bisherigen Untersuchungen zur symmetrischen Gruppe S_3 wissen wir, dass diese genau sechs Untergruppen besitzt, nämlich

$$\{\ \mathrm{id}\ \} \quad , \quad \langle(1\ 2)\rangle \quad , \quad \langle(1\ 3)\rangle \quad , \quad \langle(2\ 3)\rangle \quad , \quad \langle(1\ 2\ 3)\rangle \quad \text{und} \quad S_3.$$

Somit hat die Erweiterung $L|\mathbb{Q}$ nach dem Hauptsatz genau sechs Zwischenkörper. Es ist in dieser Situation auch nicht schwierig, diese sechs Körper konkret anzugeben. Die „trivialen“ Zwischenkörper sind L und $\mathbb{Q}$. Es ist leicht zu sehen, dass $\mathbb{Q}(\zeta)$ mit $\mathbb{Q}(\sqrt{-3})$ übereinstimmt, dies ist ein Körper vom Grad 2 über $\mathbb{Q}$. Weil α_k für $k = 1, 2, 3$ jeweils $x^3 - 2$ als Minimalpolynom haben, sind $\mathbb{Q}(\alpha_1)$, $\mathbb{Q}(\alpha_2)$ und $\mathbb{Q}(\alpha_3)$ drei Zwischenkörper vom Grad 3 über $\mathbb{Q}$.

Wir überprüfen noch, dass diese drei Körper tatsächlich verschieden voneindander sind. Offensichtlich gilt $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$ und $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_3)$, denn im Gegensatz zu $\mathbb{Q}(\alpha_2)$ und $\mathbb{Q}(\alpha_3)$ ist $\mathbb{Q}(\alpha_1)$ in $\mathbb{R}$ enthalten. Nehmen wir nun an, dass $\mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3)$ ist. Dann wären mit α_2, α_3 auch die Elemente $\zeta = \alpha_3/\alpha_2$ und $\sqrt[3]{2} = \alpha_2/\zeta$ in $\mathbb{Q}(\alpha_2)$ enthalten. Insgeesamt wäre also $L = \mathbb{Q}(\sqrt[3]{2}, \zeta) \subseteq \mathbb{Q}(\alpha_2)$, was aber wegen $[L : \mathbb{Q}] = 6$ und $[\mathbb{Q}(\alpha_2) : \mathbb{Q}] = 3$ unmöglich ist. Also haben wir tatsächlich alle sechs Zwischenkörper der Erweiterung $L|\mathbb{Q}$ gefunden.

Wir beenden das Kapitel mit einer Ergänzung zum Hauptsatz der Galoistheorie, die wir in einem späteren Abschnitt (zur Auflösbarkeit von Gleichungen) benötigen werden. Um ihn formulieren zu können, benötigen wir den Begriff des Kompositums zweier Körper.

Proposition 16.12 Ist $\tilde{K}$ ein Körper mit Teilkörpern L und M, dann gilt

$$L(M) \quad = \quad M(L).$$

Man bezeichnet $L \cdot M = L(M) = M(L)$ als das ***Kompositum*** der Körper L und M in $\tilde{K}$. Es handelt sich dabei um den kleinsten Teilkörper von $\tilde{K}$, der $L \cup M$ enthält.

Beweis: Zunächst beweisen wir die Gleichung $L(M) = M(L)$. „$\subseteq$“ Nach Definition ist $M(L)$ ein Zwischenkörper von $\tilde{K}|M$ mit $M(L) \supseteq L$. Dies zeigt, dass $M(L)$ auch ein Zwischenkörper von $\tilde{K}|L$ mit $M(L) \supseteq M$ ist, und daraus folgt $M(L) \supseteq L(M)$ nach Definition von $L(M)$. Der Beweis der Inklusion „$\supseteq$“ läuft analog. Dass $M(L) \supseteq L \cup M$ gilt, haben wir bereits festgestellt. Ist nun L_1 ein beliebiger Teilkörper von $\tilde{K}$ mit $L_1 \supseteq L \cup M$, dann ist L_1 ein Zwischenkörper von $\tilde{K}|L$ mit $L_1 \supseteq M$. Daraus folgt $L_1 \supseteq L(M)$. Also ist $L \cdot M = L(M)$ tatsächlich der kleinste Teilkörper von $\tilde{K}$, der $L \cup M$ enthält. □

Satz 16.13 *(Verschiebungssatz der Galoistheorie)*

Sei $L|K$ eine endliche Galois-Erweiterung und $M|K$ eine weitere Körpererweiterung mit der Eigenschaft, dass L und M in einem gemeinsamen Erweiterungskörper $\tilde{K}$ enthalten sind. Dann sind auch $L \cdot M|M$ und $L|L \cap M$ Galois-Erweiterungen, und es gibt einen Isomorphismus

$$\phi : \mathrm{Gal}(L \cdot M|M) \longrightarrow \mathrm{Gal}(L|L \cap M)$$

von Gruppen mit $\phi(\tau) = \tau|_L$ für alle $\tau \in \mathrm{Gal}(L \cdot M|M)$.

Beweis: Dass mit $L|K$ auch $L|(L \cap M)$ eine Galois-Erweiterung ist, folgt direkt aus den Propositionen 15.5 und 15.8. Nun zeigen wir, dass $L \cdot M|M$ galoissch ist. Da $L|K$ endlich und separabel ist, gibt es nach dem Satz 15.13 vom primitiven Element ein $\alpha \in L$, so dass $L = K(\alpha)$ erfüllt ist. Wir beweisen nun zunächst die Gleichung $L \cdot M = M(\alpha)$, die nach Definition des Kompositums zu $M(L) = M(\alpha)$ äquivalent ist. Die Inklusion „$\supseteq$“ folgt direkt aus $\alpha \in L$. Für die umgekehrte Inklusion genügt es zu bemerken, dass M mit K und α auch den Körper $L = K(\alpha)$ enthält. Aus $M \subseteq M(\alpha)$ und $L \subseteq M(\alpha)$ folgt dann $M(L) \subseteq M(\alpha)$.

O.B.d.A. können wir annehmen, dass der Körper $\tilde{K}$ algebraisch abgeschlossen ist; ansonsten ersetzen wir ihn durch seinen algebraischen Abschluss. Weil $L|K$ separabel ist und α in L liegt, ist das Minimalpolynom $f = \mu_{\alpha,K}$ separabel. Setzen wir $g = \mu_{\alpha,M}$, dann ist g wegen $f \in M[x]$ und $f(\alpha) = 0$ ein Teiler von f, und mit f ist auch g separabel. Dies zeigt, dass α auch über M separabel ist. Ist $m = \mathrm{grad}(g) = [M(\alpha) : M] = [L \cdot M : M]$, dann besitzt g in $\tilde{K}$ also m verschiedene Nullstellen. Nach Folgerung 12.4 gibt es m verschiedene M-Homomorphismen $L \cdot M \to \tilde{K}$. Der Separabilitätsgrad $[L \cdot M : M]_s$ stimmt also mit dem Erweiterungsgrad $[L \cdot M : M]$ überein, und nach Proposition 15.11 ist $L \cdot M|M$ somit eine separable Erweiterung.

Da $L|K$ normal ist, handelt es sich bei L um den Zerfällungskörper eines Polynoms $h \in K[x]$. Das Polynom h zerfällt über L also in Linearfaktoren, und es gilt $L = K(\alpha_1, ..., \alpha_r)$, wobei $\alpha_1, ..., \alpha_r$ die Nullstellen von f in L sind. Damit zerfällt h auch über $L \cdot M$ in Linearfaktoren, und es gilt $L \cdot M = M(\alpha_1, ..., \alpha_r)$. Dies zeigt, dass auch $L \cdot M|M$ normal ist. Ingesamt ist $L \cdot M|M$ also eine Galois-Erweiterung.

Sei $G = \mathrm{Gal}(L \cdot M|M)$ und $\tau \in G$. Aus $\tau(\alpha) = \alpha$ für alle $\alpha \in M$ folgt $(\tau|_L)(\alpha) = \alpha$ für alle $\alpha \in L \cap M$. Also ist $\tau|_L$ ein $(L \cap M)$-Homomorphismus. Die Erweiterung $L|L \cap M$ ist normal, somit ist $\tau|_L$ als $(L \cap M)$-Homomorphismus $L \to \tilde{K}$ nach Satz 15.3 ein $(L \cap M)$-Automorphismus von L. Damit haben wir gezeigt, dass durch $\tau \mapsto \tau|_L$ tatsächlich eine Abbildung $G \to \mathrm{Gal}(L|L \cap M)$ definiert ist.

Dass ϕ ein Homomorphismus von Gruppen ist, kann unmittelbar überprüft werden. Wir zeigen, dass ϕ injektiv und surjektiv ist. Ist $\tau \in G$ mit $\phi(\tau) = \mathrm{id}_L$, dann gilt sowohl $\tau(\alpha) = \alpha$ für alle $\alpha \in L$ als auch $\tau(\alpha) = \alpha$ für alle $\alpha \in M$. Daraus folgt $\tau = \mathrm{id}_{L \cdot M}$, und folglich ist ϕ injektiv. Die Surjektivität von ϕ ist gleichbedeutend mit $\phi(G) = \mathrm{Gal}(L|L \cap M)$. Nach dem Hauptsatz der Galoistheorie, angewendet auf die Erweiterung $L|L \cap M$, ist dies wiederum äquivalent zu $L^{\phi(G)} = L \cap M$. Die Inklusion „$\supseteq$“ ist offensichtlich, da für jede Untergruppe U von $\mathrm{Gal}(L|L \cap M)$ der Fixkörper L^U ein Zwischenkörper von $L|L \cap M$ ist. Zum Beweis von „$\subseteq$“ sei $\alpha \in L$ ein Element mit $\sigma(\alpha) = \alpha$ für alle $\sigma \in \phi(G)$. Dann gilt $\tau(\alpha) = (\tau|_L)(\alpha) = \alpha$ für alle $\tau \in G$. Dies zeigt, dass α im Fixkörper $(L \cdot M)^G$ von G liegt. Nach dem Hauptsatz der Galoistheorie, diesmal angewendet auf die Erweiterung $L \cdot M|M$, gilt $(L \cdot M)^G = M$. Also liegt α in M, insgesamt in $L \cap M$. □

§ 17. *Galoisgruppen spezieller Erweiterungen*

Zusammenfassung. In diesem Kapitel bestimmen wir die Galois-Gruppen von Erweiterungen endlicher Körper und von Kreisteilungserweiterungen. Erstere sind immer zyklisch und werden von dem bereits aus § 14 bekannten Frobenius-Automorphismus erzeugt. Die Galois-Gruppen von Kreisteilungserweiterungen sind zu isomorph zu Untergruppen der primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$, die wir aus der Zahlentheorie-Vorlesung kennen, und somit stets abelsch.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Frobenius-Automorphismus $\varphi_{\mathbb{F}_{q^n}\mid\mathbb{F}_q}$	– Es gilt $\mathrm{Gal}(\mathbb{F}_{q^n}\mid\mathbb{F}_q)\cong\mathbb{Z}/n\mathbb{Z}$ (q Primzahlpotenz, $n\in\mathbb{N}$). – Es gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_n)\mid\mathbb{Q})\cong(\mathbb{Z}/n\mathbb{Z})^\times$ für alle $n\in\mathbb{N}$, $n\geq 2$.

Zuächst untersuchen wir in diesem Abschnitt die Galoisgruppen von Erweiterungen endlicher Körper. Sei p eine Primzahl, $r\in\mathbb{N}$ und $q=p^r$. Sei $\mathbb{F}_p^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Wie in § 14 festgelegt, bezeichnen wir mit $\mathbb{F}_q$ den eindeutig bestimmten Teilkörper von $\mathbb{F}_p^{\mathrm{alg}}$ mit q Elementen. In diesem Kapitel haben wir auch gesehen, dass für jeden endlichen Körper K der Charakteristik p durch $x\mapsto x^p$ ein Automorphismus definiert ist, den wir als *Frobenius-Automorphismus* von K bezeichnet haben.

Definition 17.1 Sei $n\in\mathbb{N}$ und φ der Frobenius-Automorphismus von $\mathbb{F}_{q^n}$. Dann bezeichnen wir $\varphi_{\mathbb{F}_{q^n}\mid\mathbb{F}_q}=\varphi^r$ als den ***Frobenius-Automorphismus*** der Erweiterung $\mathbb{F}_{q^n}\mid\mathbb{F}_q$.

Die Galoistheorie endlicher Körper kann im folgenden Satz zusammengefasst werden.

Satz 17.2 Sei $n\in\mathbb{N}$.

(i) Die Erweiterung $\mathbb{F}_{q^n}\mid\mathbb{F}_q$ ist eine Galois-Erweiterung.

(ii) Die Galois-Gruppe $G=\mathrm{Gal}(\mathbb{F}_{q^n}\mid\mathbb{F}_q)$ wird vom Frobenius-Automorphismus $\varphi_{\mathbb{F}_{q^n}\mid\mathbb{F}_q}$ der Erweiterung $\mathbb{F}_{q^n}\mid\mathbb{F}_q$ erzeugt.

(iii) Durch $\mathbb{Z}/n\mathbb{Z}\to G$, $a+n\mathbb{Z}\mapsto\varphi^a$ ist ein Isomorphismus von Gruppen definiert.

Beweis: Nach Satz 15.10 ist die Erweiterung $\mathbb{F}_{q^n}\mid\mathbb{F}_q$ separabel. Nach Proposition 14.4 ist $\mathbb{F}_{q^n}$ wegen $q^n=p^{rn}$ der Zerfällungskörper des Polynoms $x^{p^{rn}}-x$ über $\mathbb{F}_p$, die Erweiterung $\mathbb{F}_{q^n}\mid\mathbb{F}_p$ ist also normal. Da $\mathbb{F}_q$ ein Zwischenkörper von $\mathbb{F}_{q^n}\mid\mathbb{F}_p$ ist, handelt es sich nach Proposition 15.5 auch bei $\mathbb{F}_{q^n}\mid\mathbb{F}_q$ um eine normale Erweiteriung. Insgesamt ist $\mathbb{F}_{q^n}\mid\mathbb{F}_q$ also eine Galois-Erweiterung, damit ist (i) bewiesen.

Im Beweis von Proposition 14.7 wurde gezeigt, dass für jedes $m \in \mathbb{N}$ die Elemente von $\mathbb{F}_{p^m}$ genau die Nullstellen des Polynoms $x^{p^m} - x \in \mathbb{F}_p$ sind. Insbesondere sind innerhalb des Körpers $\mathbb{F}_{q^n}$ die Elemente von $\mathbb{F}_q$ genau die Nullstellen von $x^q - x$; dies sind zugleich diejenigen Elemente $\alpha \in \mathbb{F}_{q^n}$, für die $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \alpha$ gilt. Dies zeigt, dass $\varpi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ nicht nur ein Automorphismus, sondern ein $\mathbb{F}_q$-Automorphismus von $\mathbb{F}_{q^n}$, und somit ein Element der Galoisgrupppe G, ist. Für $1 \leq s \leq n$ und alle $\alpha \in \mathbb{F}_{q^n}$ gilt jeweils $\varphi^s_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \alpha^{q^s}$. Die Elemente, die unter $\varphi^s_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ fest bleiben, also auf sich selbst abgebildet werden, sind jeweils genau die Elemente des Teilkörpers $\mathbb{F}_{q^s}$. Insbesondere ist $\varphi^n_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ die kleinste Potenz von $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$, die alle Elemente von $\mathbb{F}_{q^n}$ festhält. Also ist $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ in G ein Element der Ordnung n. Nach Satz 16.5 gilt $|G| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n = \mathrm{ord}(\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q})$. Dies zeigt, dass G tatsächlich von $\mathrm{ord}(\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q})$ erzeugt wird, also Aussage (ii).

Weil $\bar{1} = 1 + n\mathbb{Z}$ in der Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ein Element der Ordnung n ist, folgt aus Proposition 3.12 die Existenz eines Homomorphismus $\mathbb{Z}/n\mathbb{Z} \to G$, der $\bar{1}$ auf $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ abbildet. Das Bild von $\bar{a} = a + n\mathbb{Z} = a(1 + n\mathbb{Z})$ unter diesem Homomorphismus ist dann jeweils $\varphi^a_{\mathbb{F}_{q^n}|\mathbb{F}_q}$, für jedes $a \in \mathbb{Z}$. Weil G von $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ erzeugt wird, ist der Homomorphismus surjektiv, auf Grund der Gleichheit der Ordnungen von $\mathbb{Z}/n\mathbb{Z}$ und G somit auch bijektiv. Damit ist auch Punkt (iii) bewiesen. □

Bei einer Galois-Erweiterung der Form $\mathbb{F}_{q^n}|\mathbb{F}_q$ lässt sich die bijektive Korrespondenz aus dem Hauptsatz der Galoistheorie zwischen der Menge $\mathscr{U}$ der Untergruppen von $G = \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) = \langle \varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q} \rangle$ und der Menge $\mathscr{Z}$ der Zwischenkörper von $\mathbb{F}_{q^n}|\mathbb{F}_q$ besonders einfach und explizit beschreiben. Wie aus der Theorie der zyklischen Gruppen bekannt, sind die Untergruppen von G alle von der Form $\langle \varphi^d_{\mathbb{F}_{q^n}|\mathbb{F}_q} \rangle$, wobei $d \in \mathbb{N}$ die Teiler von n durchläuft. Dabei ist die Ordnung von $\langle \varphi^d_{\mathbb{F}_{q^n}|\mathbb{F}_q} \rangle$ jeweils gleich n/d, und der Index dieser Untergruppe in G ist gleich d. Nun ist nach Satz 16.8 (iv) der Fixkörper von $\langle \varphi^d \rangle$ ein Zwischenkörper Z_d von $\mathbb{F}_{q^n}|\mathbb{F}_q$ mit $[Z_d : \mathbb{F}_q] = d$ und $[\mathbb{F}_{q^n} : Z_d] = n/d$. Offenbar handelt es sich dabei um den Körper $\mathbb{F}_{p^d}$.

Mit den ***Kreisteilungskörpern*** wenden wir uns nun einer weiteren Klasse algebraischer Erweiterungen zu, bei der sich die Galoisgruppen auf einfache Weise beschreiben lassen. Hierfür greifen wir auf Ergebnisse und Definitionen aus der Zahlentheorie-Vorlesung zurück.

Ist $n \in \mathbb{N}$ und $n \geq 2$. Eine ***n-te Einheitswurzel*** in $\mathbb{C}$ ist ein Element $\zeta \in \mathbb{C}^\times$ der multiplikativen Gruppe mit $\zeta^n = 1$. Hat ζ darüber hinaus in $\mathbb{C}^\times$ die Ordnung n, dann spricht man von einer ***primitiven*** n-ten Einheitswurzel. Zum Beispiel ist $\zeta_n = e^{2\pi i/n}$ ein solches Element. Der Körper $\mathbb{Q}(\zeta_n)$ wird ***n-ter Kreisteilungskörper*** genannt.

In der Zahlentheorie werden die Minimalpolynome der Elemente ζ_n definiert, die sogenannten ***Kreisteilungspolynome*** $\Phi_n \in \mathbb{Z}[x]$. Es handelt sich dabei um irreduzible Polynome vom Grad $\varphi(n)$ (wobei φ die Eulersche ϕ-Funktion bezeichnet), deren Nullstellen genau die Elemente ζ_n^k mit $k \in \mathbb{Z}$, $1 < k < n$ und $\mathrm{ggT}(k, n) = 1$ sind. Auf Grund dieser Tatsache ist $\mathbb{Q}(\zeta_n)$ bereits der Zerfällungskörper von Φ_n über $\mathbb{Q}$, also $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ eine normale Erweiterung vom Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \mathrm{grad}(\Phi_n) = \varphi(n)$. Als algebraische Erweiterung eines Körpers der Charakteristik 0 ist $\mathbb{Q}(\zeta_n)$ auch separabel über $\mathbb{Q}$, insgesamt also eine endliche Galois-Erweiterung.

Satz 17.3 Sei $n \in \mathbb{N}$ mit $n \geq 2$ und $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$.

(i) Für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ gibt es ein eindeutig bestimmtes Element $\sigma_a \in G$ definiert durch $\sigma_a(\zeta_n) = \zeta_n^a$.

(ii) Es gibt einen Gruppenisomorphismus $\phi_n : (\mathbb{Z}/n\mathbb{Z})^\times \to G$ mit $\phi_n(a + n\mathbb{Z}) = \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$.

Beweis: zu (i) Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Weil ζ_n und ζ_n^a beides Nullstellen des Kreisteilungspolynoms Φ_n sind und dieses über $\mathbb{Q}$ irreduzibel ist, gibt es auf Grund des Fortsetzungssatzes, Satz 12.2, einen eindeutig bestimmten $\mathbb{Q}$-Homomorphismus $\sigma_a : \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \to \mathbb{Q}^{\mathrm{alg}}$ in den algebraischen $\mathbb{Q}^{\mathrm{alg}}$ von $\mathbb{Q}$ mit $\sigma_a(\zeta_n) = \zeta_n^a$. Da $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ normal ist, handelt es sich bei σ_a nach Satz 15.3 um einen $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\zeta_n)$, also um ein Element der Grupe G.

zu (ii) Wir definieren die Abbildung ϕ_n, indem wir für jedes $a \in \mathbb{Z}$ mit $0 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$ das Bild von $a + n\mathbb{Z}$ jeweils durch $\phi_n(a + n\mathbb{Z}) = \sigma_a$ festlegen. Für alle $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = \mathrm{ggT}(b,n) = 1$ stimmen σ_a und σ_b jeweils genau dann überein, wenn $a \equiv b \mod n$ gilt. Denn die Gleichung $\sigma_a = \sigma_b$ ist äquivalent zu $\zeta_n^a = \sigma_a(\zeta_n) = \sigma_b(\zeta_n) = \zeta_n^b$, weil jedes $\sigma \in G$ durch das Bild $\sigma(\zeta_n)$ eindeutig festgelegt ist, und damit auch zu $\zeta_n^{b-a} = 1$. Weil ζ_n in $\mathbb{C}^\times$ ein Element der Ordnung n ist, ist dies wiederum äquivalent zu $n \mid (b-a)$ und damit zu $a \equiv b \mod n$. Die Äquivalenz $a \equiv b \mod n \Leftrightarrow \sigma_a = \sigma_b$ zeigt einerseits, dass die Gleichung $\phi_n(a + n\mathbb{Z}) = \sigma_a$ für alle $a \in Z$ mit $\mathrm{ggT}(a,n) = 1$ erfüllt ist, und andererseits, dass ϕ_n injektiv ist. Nach Satz 16.5 gilt für die Ordnung der beiden Gruppen die Gleichheit $|G| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$; somit ist ϕ_n auch bijektiv.

Nun überprüfen wir noch, dass durch ϕ_n ein Gruppenhomomorphismus definiert ist. Für alle $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = \mathrm{ggT}(b,n) = 1$ gilt

$$(\sigma_a \circ \sigma_b)(\zeta_n) \quad = \quad \sigma_a(\zeta_n^b) \quad = \quad \sigma_a(\zeta_n)^b \quad = \quad (\zeta_n^a)^b \quad = \quad \zeta_n^{ab} \quad = \quad \sigma_{ab}(\zeta_n).$$

Es folgt $\phi_n(\bar{a}\bar{b}) = \sigma_{ab} = \sigma_a \circ \sigma_b = \phi_n(\bar{a}) \circ \phi_n(\bar{b})$. Damit ist nachgewiesen, dass es sich bei ϕ_n um einen Homomorphismus von Gruppen handelt, insgesamt um einen Isomorphismus. □

Beispielsweise gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, wobei der letzte Isomorphismus aus dem Kapitel der Zahlentheorie-Vorlesung über die primen Restklassengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ stammt. Wie wir bereits am Ende von § 7 verwendet haben, gibt es in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ genau drei Untergruppen der Ordnung 2, die nach dem Hauptsatz der Galoistheorie genau drei Zwischenkörpern M_1, M_2, M_3 von $\mathbb{Q}(\zeta_8)|\mathbb{Q}$ vom Grad $[M_i : \mathbb{Q}] = 2$ für $i = 1,2,3$ entsprechen. Durch Potenzieren überprüft man, dass $\zeta_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ eine primitive achte Einheitswurzel ist. Damit kann man leicht zeigen, dass die drei gesuchten Zwischenkörper durch $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(\sqrt{-2})$ gegeben sind.

Später werden wir eine Verallgemeinerung dieses Satzes von $\mathbb{Q}$ auf beliebige Grundkörper K der Charakteristik 0 benötigen. Über einem solchen Körper werden die n-ten Kreisteilungspolynome durch dieselbe Rekursionsformel wie über $\mathbb{Q}$ definiert, und genau wie dort zeigt man, dass die Nullstellen des n-ten Kreisteilungspolynoms $\Phi_n \in K[x]$ genau die primitiven n-ten Einheitswurzeln in einem beliebigen algebraischen Abschluss von K sind. Der Hauptunterschied zu Satz 17.3 kommt dadurch zu Stande, dass nicht mehr erwartet werden kann, dass Φ_n in $K[x]$ irreduzibel ist. Dies ist zum Beispiel im Fall $K = \mathbb{C}$ offensichtlich, denn über diesem Körper zerfällt Φ_n in Linearfaktoren.

Satz 17.4 Sei $n \in \mathbb{N}$ mit $n \geq 2$, K ein Körper der Charakteristik 0, $L|K$ eine Körpererweiterung und $\zeta_n \in L$ eine primitive n-te Einheitswurzel, also ein Element in $L^\times$ der Ordnung n. Dann ist $K(\zeta_n)|K$ eine Galois-Erweiterung, und die Galoisgruppe $G = \mathrm{Gal}(K(\zeta_n)|K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis: Wie bereits oben erwähnt, sind die verschiedenen Nullstellen von Φ_n genau die primitiven n-ten Einheitswurzeln in einem algebraischen Abschluss von $\tilde{L}$. Dies sind genau die Elemente der Form ζ_n^a mit $0 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$. Dies zeigt, dass $K(\zeta_n)$ der Zerfällungskörper von Φ_n über K, die Erweiterung $K(\zeta_n)|K$ also normal ist. Wegen $\mathrm{char}(K) = 0$ ist die Erweiterung auch separabel, insgesamt also eine Galois-Erweiterung.

Jedes $\sigma \in G$ bildet ζ_n auf eine Nullstelle von Φ_n, also ein Element der Form ζ_n^a mit $0 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$, ab. Dieses $a \in \mathbb{Z}$ ist durch σ eindeutig festgelegt; wir definieren eine Abbildung $\psi_n : G \to (\mathbb{Z}/n\mathbb{Z})^\times$, indem wir $\psi_n(\sigma) = a + n\mathbb{Z}$ setzen. Diese Zuordnung ψ_n ist injektiv, denn werden zwei Elemente σ, τ auf dieselbe Restklasse abgebildet, dann folgt daraus $\sigma(\zeta_n) = \tau(\zeta_n)$ und damit $\sigma = \tau$, denn jedes Element aus G ist durch das Bild von ζ_n eindeutig festgelegt. Bezeichnen wir für jedes $a \in \mathbb{Z}$ mit $a + n\mathbb{Z} \in \psi_n(G)$ jeweils das eindeutig bestimmte Urbild mit σ_a, dann gilt $(\sigma_a \circ \sigma_b)(\zeta_n) = \zeta_n^{ab}$ für alle $a, b \in Z$ mit $a+n\mathbb{Z}, b+n\mathbb{Z} \in \psi_n(G)$; dies rechnet man wie im Beweis von Satz 17.3 nach. Dies zeigt, dass auch $ab + n\mathbb{Z}$ in $\psi_n(G)$ enthalten ist, und dass $\psi_n(\sigma_a \circ \sigma_b) = ab + n\mathbb{Z} = \psi_n(\sigma_a)\psi_n(\sigma_b)$ gilt. Dies zeigt insgesamt, dass durch ψ_n ein Isomorphismus zwischen G und der Untergruppe $\psi_n(G)$ von $(\mathbb{Z}/n\mathbb{Z})^\times$ gegeben ist. □

§ 18. *Reine Gleichungen und zyklische Erweiterungen*

Zusammenfassung. Wir zeigen, dass unter geeigneten Voraussetzungen an den Grundkörper K eine Galois-Erweiterung $L|K$ genau dann eine zyklische Galoisgruppe hat, wenn L durch Adjunktion einer n-ten Wurzel eines Elements aus K entsteht.

Wichtige Grundbegriffe

- n-te Wurzel eines Körperelements
- Verwendung der Notation $\sqrt[n]{a}$
- Definition reine Gleichungen über einem Körper K
- Lagrange-Resolvente (eines Körperelements bezüglich eines Elements der Galoisgruppe)

Zentrale Sätze

- Dedekindsches Lemma (zur linearen Unabhängigkeit von Halbgruppen-Homomorphismen)
- Die zyklischen Galoisgruppen sind genau die Galoisgruppen reiner Gleichungen (wenn K genügend viele n-te Einheitswurzeln enthält).

Definition 18.1 Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Ein Element $\alpha \in K$ wird eine ***n-te Wurzel*** von a genannt, falls $\alpha^n = a$ gilt. Im Fall $n = 2$ spricht man von Quadrat-, im Fall $n = 3$ von Kubikwurzeln.

Ein Element α ist also genau dann n-te Wurzel von a, wenn es die Gleichung $x^n - a = 0$ löst. Eine solche Gleichung wird als ***reine Gleichung*** bezeichnet.

An dieser Stelle sind ein paar Anmerkungen zur Verwendung des Wurzelzeichens angebracht. Auch in der Algebra wird eine n-Wurzel eines Elements $a \in K$ häufig mit dem Ausdruck $\sqrt[n]{a}$ bezeichnet. Allerdings darf man dabei nicht vergessen, dass die Gleichung $x^n = a$ in einem Körper K sowohl keine als auch mehrere Lösungen haben kann. Nach unserer Definition wären im Körper $K = \mathbb{Q}$ beispielsweise ± 3 beides Quadratwurzeln der Zahl 9, während 7 in $\mathbb{Q}$ keine Quadratwurzel besitzt. Will man die Bezeichnung $\sqrt{9}$ verwenden, muss man willkürlich festlegen, welche Lösung der Gleichung $x^2 = 9$ in $\mathbb{Q}$ damit gemeint sein soll.

In vielen Körpern gibt es eine mehr oder weniger „kanonische“ Definition der Wurzelsymbole. Solange K einen Teilkörper von $\mathbb{R}$ bezeichnet, legt man beispielsweise fest, dass für ein positives Element $a \in K$ und beliebiges $n \in \mathbb{N}$ das Element $\sqrt[n]{a}$ die eindeutig bestimmte *positive* reelle Lösung der Gleichung $x^n = a$ bezeichnet. (Diese muss natürlich nicht im Körper K enthalten sein.) Ist n ungerade und a negativ, dann bezeichnet $\sqrt[n]{a}$ ebenfalls die eindeutig bestimmte reelle Lösung von $x^n = a$. Diese ist dann zwangsläufig negativ; beispielsweise ist $\sqrt[3]{-8} = -2$. Außerdem setzt man $\sqrt[n]{0} = 0$ für alle $n \in \mathbb{N}$.

Ist K ein Teilkörper von $\mathbb{C}$, dann kann sich mit der Polarkoordinaten-Darstellung behelfen. Zur Erinnerung: Das ***Argument*** $\arg(z)$ von $z \in \mathbb{C}^\times$ ist die eindeutig bestimmte reelle Zahl $\varphi \in]-\pi, \pi]$ mit der Eigenschaft, dass die Gleichung

$$z \quad = \quad |z|e^{i\varphi} \quad = \quad |z|(\cos(\varphi) + i\sin(\varphi))$$

erfüllt ist. Man definiert dann $\sqrt[n]{z} = \sqrt[n]{|z|}e^{(i\varphi)/n}$ und setzt wiederum $\sqrt[n]{0} = 0$. Zu beachten ist dabei aber, dass diese Definition nur auf $\mathbb{R}^+$ mit der zuvor gegebenen übereinstimmt, während für ungerades n und negative reelle Zahlen die beiden Definitionen voneinander abweichen.

Wendet man beispielsweise die reelle dritte Wurzelfunktion auf -8 an, so erhält man (wie oben festgestellt) den Wert -2. Die Anwendung der komplexen dritten Wurzelfunktion dagegen liefert den nicht-reellen Wert $2e^{(i\pi)/3}$, denn die Polarkoordinaten-Darstellung von -8 ist gegeben durch $-8 = 8e^{i\pi}$. Darüber hinaus war bereits in der Zahlentheorie-Vorlesung darauf hingewiesen worden, dass die Gleichung $\sqrt{zw} = \sqrt{z}\sqrt{w}$ für $z, w \in \mathbb{C}$ im allgemeinen nicht mehr erfüllt ist. Beispielsweise gilt $\sqrt{-3}\sqrt{-5} = (i\sqrt{3})(i\sqrt{5}) = -\sqrt{15} < 0$, aber $\sqrt{(-3)(-5)} = \sqrt{15} > 0$.

Man merkt an diesen Beispielen, dass die Festlegung von n-ten Wurzeln immer mit einer gewissen Willkür behaftet ist, die sich in diversen „Schönheitsfehlern“ äußert. Bei den komplexen Zahlen besteht diese Willkür darin, dass das Argument einer komplexen Zahl auf das Intervall $]-\pi, \pi]$ festgelegt wurde. Würde man zum Beispiel statt dessen definieren, dass das Argument stets im Intervall $[0, 2\pi[$ liegen soll, was auf Grund der Gleichung $e^{i\varphi} = e^{i(\varphi+2\pi)}$ für alle $\varphi \in \mathbb{R}$ ohne Weiteres möglich wäre, dann würde die Gleichung $\sqrt[n]{z} = \sqrt[n]{|z|}e^{(i\varphi)/n}$ zu einer anderen Definition der n-ten Wurzel führen.

Vollends unmöglich wird die Festlegung einer „kanonischen“ n-ten Wurzelfunktion auf den endlichen Körpern. Betrachten wir beispielsweise den Körper $\mathbb{F}_7 = \{\bar{0}, \bar{1}, ..., \bar{6}\}$ bestehend aus sieben Elementen. Die Gleichungen

$$\bar{0}^2 = \bar{0} \quad , \quad \bar{1}^2 = \bar{1} \quad , \quad \bar{2}^2 = \bar{4} \quad , \quad \bar{3}^2 = \bar{2} \quad , \quad \bar{4}^2 = \bar{2} \quad , \quad \bar{5}^2 = \bar{4} \quad , \quad \bar{6}^2 = \bar{1}$$

zeigen, dass nur die Elemente $\bar{0}, \bar{1}, \bar{2}$ und $\bar{4}$ Quadratwurzeln besitzen. Man könnte nun beispielsweise auf der Teilmenge $\{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$ von $\mathbb{F}_7$ eine Quadratwurzelfunktion durch $\sqrt{\bar{0}} = \bar{0}$, $\sqrt{\bar{1}} = \bar{1}$, $\sqrt{\bar{2}} = \bar{3}$ und $\sqrt{\bar{4}} = \bar{2}$ definieren. Weil aber jedes der Elemente $\bar{1}, \bar{2}, \bar{4}$ zwei verschiedene Quadratwurzeln besitzt, ist dies nur eine von insgesamt acht Möglichkeiten zur Festlegung der Funktion $\sqrt{\cdot} : \mathbb{F}_7 \to \mathbb{F}_7$.

Andererseits ist die Verwendung des Wurzelzeichens so bequem und eingängig, dass wir im weiteren Verlauf nicht vollständig darauf verzichten wollen. Deshalb legen wir folgendes fest: Sei K ein beliebiger Körper, $n \in \mathbb{N}$ und $R_K^{(n)} \subseteq K$ die Teilmenge aller $a \in K$ mit der Eigenschaft, dass die Gleichung $x^n = a$ in K eine Lösung besitzt; ist K algebraisch abgeschlossen, dann gilt natürlich $R_K^{(n)} = K$. Dann bezeichnet $\sqrt[n]{\cdot} : R_K^{(n)} \to K$ stets eine Funktion mit der Eigenschaft $(\sqrt[n]{a})^n = a$ für alle $a \in R_K^{(n)}$, mit anderen Worten, für jedes $a \in R_K^{(n)}$ ist $\sqrt[n]{a}$ eine n-te Wurzel von a. Die beiden oben angebenen Festlegungen für die Körper $K = \mathbb{R}$ bzw. $K = \mathbb{C}$ sind konkrete Beispiele für solche Wurzelfunktionen. Dabei ist $R_{\mathbb{R}}^{(n)} = \mathbb{R}$ für ungerades und $R_{\mathbb{R}}^{(n)} = \mathbb{R}_0^+ = \mathbb{R}^+ \cup \{0\}$ für gerades $n \in \mathbb{N}$. Im Fall $K = \mathbb{F}_7$ ist $R_K^{(2)} = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$, und die dort angegebene Abbildung $\sqrt{\cdot} : R_{\mathbb{F}_7}^{(2)} \to \mathbb{F}_7$ ist ein Beispiel für eine zweite Wurzelfunktion. Man beachte, dass im Allgemeinen weder $\sqrt[n]{ab} = \sqrt[n]{a} \cdot \sqrt[n]{b}$ noch $\sqrt[n]{a^n} = a$ für $a, b \in K$ gelten muss. Zumindest aber ist nach Definition $\sqrt[1]{a} = a$ für alle $a \in K$ erfüllt.

Wir untersuchen nun die Galoisgruppen von Erweiterungen, die durch Adjunktion von einer n-ten Wurzel zu Stande kommen. Dazu führen wir die folgende Sprechweise ein: Wir sagen, ein Körper K enthält eine primitive n-te Einheitswurzel, wenn in der multiplikativen Gruppe $K^\times$ ein Element ζ der Ordnung n existiert.

Satz 18.2 Sei $n \in \mathbb{N}$ mit $n \geq 2$ und K ein Körper mit $\mathrm{char}(K) \nmid n$, was $\mathrm{char}(K) = 0$ einschließt. Wir setzen voraus, dass K eine primitive n-te Einheitswurzel ζ enthält. Weiter sei $a \in K^\times$, L ein Erweiterungskörper von K und $\alpha \in L$ eine n-te Wurzel von a.

(i) Die Erweiterung $K(\alpha)|K$ ist eine Galois-Erweiterung.

(ii) Sei G die Galoisgruppe von $K(\alpha)|K$. Dann gibt es einen Teiler d von n mit der Eigenschaft, dass G isomorph zu $\mathbb{Z}/d\mathbb{Z}$ ist.

(iii) Es gilt $G \cong \mathbb{Z}/n\mathbb{Z}$ genau dann, wenn das Polynom $f = x^n - a$ in $K[x]$ irreduzibel ist.

Beweis: zu (i) Das Element α ist Nullstelle von $f = x^n - a \in K[x]$, denn es gilt $f(\alpha) = \alpha^n - a = a - a = 0$. Wegen $f' = nx^{n-1}$ und $n \neq 0$ in K gilt $\mathrm{ggT}(f, f') = 1$. Nach Proposition 14.3 zeigt dies, dass f in jeder Erweiterung von K nur einfache Nullstellen besitzt. Das Minimalpolynom $g = \mu_{K,\alpha}$ ist nach Satz 11.3 ein Teiler von f und besitzt somit ebenfalls nur einfache Nullstellen in jeder Erweiterung von K. Also ist α separabel über K. In den Übungen wurde gezeigt, dass die über K separablen Elemente einen Teilkörper von L bilden. Der kleinste Teilkörper von L, der das separable Element α enthält, ist $K(\alpha)$. Dies zeigt, dass $K(\alpha)|K$ separabel ist.

Um zu zeigen, dass $K(\alpha)|K$ auch normal ist, weisen wir nach, dass $K(\alpha)$ der Zerfällungskörper von f über K ist. Wegen $\mathrm{ord}(\zeta) = n$ in $K^\times$ und $\alpha \neq 0$ sind durch $\alpha_j = \zeta^j \alpha$ mit $0 \leq j \leq n-1$ genau n verschiedene Elemente von $K(\alpha)$ gegeben. Wegen $f(\alpha_j) = (\zeta^j\alpha)^n - a = (\zeta^n)^j \alpha^n - a = 1^j \cdot a - a = 0$ sind dies alles Nullstellen von f. Wegen $\mathrm{grad}(f) = n$ zerfällt f über $K(\alpha)$ also in Linearfaktoren. Andererseits wird $K(\alpha)|K$ über K von den Elementen $\alpha_0, \ldots, \alpha_{n-1}$ erzeugt, da die Erweiterung bereits von $\alpha_0 = \alpha$ erzeugt wird. Also ist $K(\alpha)$ tatsächlich der Zerfällungskörper von f über K.

zu (ii) Jedes Element $\sigma \in G$ ist ein K-Homomorphismus $K(\alpha) \to K(\alpha)$ und bildet somit nach Satz 12.3 Nullstellen von f auf Nullstellen von f ab. Somit gibt es für jedes $\sigma \in G$ ein eindeutig bestimmtes $j \in \{0, \ldots, n-1\}$ mit $\sigma(\alpha) = \alpha_j$. Weil jeder K-Homomorphismus auf $K(\alpha)$ nach Satz 12.1 durch das Bild von α eindeutig festgelegt ist, gibt es für jedes j höchstens ein Element $\sigma_j \in G$ mit $\sigma_j(\alpha) = \alpha_j$. Aus $\sigma(\alpha) = \alpha_j$ folgt also $\sigma = \sigma_j$ für dieses j.

Wir definieren nun eine Abbildung $\phi : G \to \mathbb{Z}/n\mathbb{Z}$, indem wir jedem $\sigma_j \in G$ die Restklasse $j + n\mathbb{Z}$ zuordnen. Diese Abbildung ist dann offenbar injektiv. Außerdem handelt es sich um einen Homomorphismus von Gruppen. Zum Nachweis seien $j, k \in \{0, \ldots, n-1\}$ vorgegeben, und $\ell \in \mathbb{Z}$ die eindeutig bestimmte Zahl mit $0 \leq \ell \leq n-1$ und $j + k \equiv \ell \mod n$. Wegen $\mathrm{ord}(\zeta) = n$ gilt

$$\begin{aligned}(\sigma_j \circ \sigma_k)(\alpha) &= \sigma_j(\sigma_k(\alpha)) = \sigma_j(\zeta^k\alpha) = \sigma_j(\zeta^k)\sigma_j(\alpha) = \zeta^k\sigma_j(\alpha) = \\ &\zeta^k\zeta^j\alpha = \zeta^{j+k}\alpha = \zeta^\ell\alpha = \alpha_\ell \ ,\end{aligned}$$

also $\sigma_j \circ \sigma_k = \sigma_\ell$ und $\phi(\sigma_j \circ \sigma_k) = \phi(\sigma_\ell) = \ell + n\mathbb{Z} = (j+k) + n\mathbb{Z} = (j + n\mathbb{Z}) + (k + n\mathbb{Z}) = \phi(\sigma_j) + \phi(\sigma_k)$. Weil ϕ injektiv ist, ist G isomorph zur Untergruppe $\phi(G)$ von $\mathbb{Z}/n\mathbb{Z}$. Als Untergruppe einer endlichen zyklischen Gruppe ist auch $\phi(G)$ endlich und zyklisch, also isomorph zu $\mathbb{Z}/d\mathbb{Z}$ für ein $d \in \mathbb{N}$. Nach dem Satz von Lagrange muss d ein Teiler von n sein. Mit $\phi(G)$ ist auch G isomorph zu $\mathbb{Z}/d\mathbb{Z}$.

zu (iii) Sei g das Minimalpolynom von α über K. Wegen $f(\alpha) = 0$ ist g ein Teiler von f. Da $K(\alpha)|K$ eine Galois-Erweiterung ist, gilt $d = |G| = [K(\alpha) : K] = \mathrm{grad}(g)$. Ist nun f über K irreduzibel, dann gilt $f = g$ und somit $d = \mathrm{grad}(g) = \mathrm{grad}(f) = n$, also $G \cong \mathbb{Z}/n\mathbb{Z}$. Setzen wir umgekehrt $G \cong \mathbb{Z}/n\mathbb{Z}$ voraus, dann folgt $\mathrm{grad}(g) = d =$

$|G| = n = \text{grad}(f)$. Wegen $g \mid f$, und weil g und f beide normiert sind, folgt daraus $f = g$. Mit g ist also auch f irreduzibel über K. □

Wir zeigen nun, dass umgekehrt jede zyklische Galois-Erweiterung $L|K$ durch Adjunktion einer n-ten Wurzel zu Stande kommt, vorausgesetzt, der Grundkörper K enthält eine primitive n-te Einheitswurzel. Dazu benötigen wir als Voraussetzung das sog. Dedekindsche Lemma. Es besagt, dass für eine Halbgruppe H und einen Körper K eine beliebige endliche Menge von Halbgruppen-Homomorphismen $H \to K^\times$ im K-Vektorraum $\text{Abb}(H,K)$ der Abbildungen $H \to K$ linear unabhängig ist.

Satz 18.3 *(Dedekindsches Lemma)*

Sei H eine Halbgruppe und K ein Körper. Dann ist jede endliche Menge von Halbgruppen-Homomorphismen $H \to K^\times$ im K-Vektorraum $\text{Abb}(H,K)$ der Abbildungen $H \to K$ linear unabhängig.

Beweis: Wir zeigen durch vollständige Induktion über n: Sind $\tau_1, ..., \tau_n$ verschiedene Halbgruppen-Homomorphismen $H \to K^\times$, dann sind diesen in $\text{Abb}(H,K)$ linear unabhängig. Zum Beweis des Induktionsanfangs sei τ_1 ein solcher Homomorphismus und $c_1 \in K$ mit $c_1\tau_1 = 0$. Ist $a \in H$ beliebig gewählt, dann gilt einerseits $\tau_1(a) \neq 0$, andererseits aber $c_1\tau_1(a) = 0$. Daraus folgt $c_1 = 0$, wodurch die lineare Unabhängigkeit bewiesen ist.

Für den Induktionsschritt sei $n \in N$ seien $n+1$ verschiedene Halbgruppen-Homomorphismen $\tau_1, ..., \tau_{n+1} : H \to K^\times$ vorgegeben. Seien $c_1, ..., c_{n+1} \in K$ mit $\sum_{k=1}^{n+1} c_k\tau_k = 0$. Wegen $\tau_1 \neq \tau_{n+1}$ gibt es ein $a \in H$ mit $\tau_1(a) \neq \tau_{n+1}(a)$. Für alle $b \in H$ folgt dann

$$\sum_{k=2}^{n+1} c_k(\tau_k(a)-\tau_1(a))\tau_k(b) = \sum_{k=1}^{n+1} c_k(\tau_k(a)-\tau_1(a))\tau_k(b) = \sum_{k=1}^{n+1} c_k\tau_k(a)\tau_k(b) - \sum_{k=1}^{n+1} c_k\tau_1(a)\tau_k(b)$$
$$= \sum_{k=1}^{n+1} c_k\tau_k(ab) - \tau_1(a)\sum_{k=1}^{n+1} c_k\tau_k(b) = 0 - \tau_1(a)\cdot 0 = 0.$$

Es gilt also $\sum_{k=2}^{n+1} c_k(\tau_k(a)-\tau_1(a))\tau_k = 0$, und weil die Menge $\{\tau_2, ..., \tau_{n+1}\}$ nach Induktionsvoraussetzung linear unabhängig ist, folgt $c_k(\tau_k(a)-\tau_1(a)) = 0$ für $2 \leq k \leq n+1$. Wegen $\tau_{n+1}(a)-\tau_1(a) \neq 0$ folgt weiter $c_{n+1} = 0$. Setzen wir dies in die Gleichung zu Beginn des Induktionsschritts ein, so erhalten wir $\sum_{k=1}^{n} c_k\tau_k = 0$. Daraus wiederum folgt $c_k = 0$ für $1 \leq k \leq n$. □

Definition 18.4 Sei $L|K$ eine endliche Galois-Erweiterung mit einer zyklischen Galoisgruppe G der Ordnung n, wobei K ein primtive n-te Einheitswurzel ζ enthält. Sei $\sigma \in G$ ein Element mit $G = \langle\sigma\rangle$. Dann nennt man für beliebiges $\alpha \in L$ das Element

$$\vartheta(\sigma,\alpha) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + ... + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

die ***Lagrangesche Resolvente*** von α bezüglich σ.

Nun können wir eine Umkehrung von Satz 18.2 formulieren und beweisen.

Satz 18.5 Sei $n \in \mathbb{N}$, K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält, und $L|K$ eine Galois-Erweiterung vom Grad n mit zyklischer Galoisgruppe G. Dann gibt es ein Element $\vartheta \in L$ mit $L = K(\vartheta)$ und $\vartheta^n \in K$.

Beweis: Sei $\sigma \in G$ ein Element mit $G = \langle \sigma \rangle$. Auf Grund von Satz 18.3 gibt es ein $\alpha \in L$ mit der Eigenschaft, dass $\vartheta = \vartheta(\sigma, \alpha)$ ungleich null ist. Denn ansonsten wäre die Abbildung $L^\times \to L$ gegeben durch $\sum_{k=0}^{n-1} \zeta^k \sigma^k = 0$ konstant null, die Elemente σ^k mit $0 \leq k < n$ aufgefasst als Halbgruppen-Homomorphismen $L^\times \to L^\times$ im L-Vektorraum $\mathrm{Abb}(L^\times, L)$ also linear abhängig. Es gilt nun $K(\vartheta) \subseteq L$ und

$$\begin{aligned} \sigma(\vartheta) &= \sigma\left(\sum_{k=0}^{n-1} \zeta^k \sigma^k(\alpha)\right) = \sum_{k=0}^{n-1} \zeta^k \sigma^{k+1}(\alpha) = \zeta^{-1}\left(\sum_{k=0}^{n-1} \zeta^{k+1} \sigma^{k+1}(\alpha)\right) = \\ &\zeta^{-1}\left(\sum_{k=1}^{n} \zeta^k \sigma^k(\alpha)\right) = \zeta^{-1}\left(\sum_{k=0}^{n-1} \zeta^k \sigma^k(\alpha)\right) = \zeta^{-1}\vartheta \quad , \end{aligned}$$

wobei wir im vorletzten Schritt verwendet haben, dass $\zeta^n \sigma^n(\alpha) = \zeta^0 \sigma^0(\alpha)$ gilt. Setzen wir $a = \vartheta^n$, dann gilt $\sigma(a) = \sigma(\vartheta^n) = \sigma(\vartheta)^n = (\zeta\vartheta)^n = \zeta^n \vartheta^n = 1 \cdot a = a$. Dies zeigt, dass a in $L^{\langle\sigma\rangle} = L^G = K$ liegt. Somit ist ϑ eine Nullstelle des Polynoms $f = x^n - a \in K[x]$.

Sei nun $g = \mu_{K,\vartheta}$ das Minimalpolynom von ϑ über K. Wegen $f(\vartheta) = 0$ ist g ein Teiler von f. Andererseits sind mit ϑ auch die $n-1$ weiteren Elemente $\zeta^{-k}\vartheta = \sigma^k(\vartheta)$ Nullstellen von g, denn nach Satz 12.3 ist das Bild einer Nullstelle von $g \in K[x]$ unter dem K-Homomorphisus σ^k jeweils ebenfalls eine Nullstelle von g. Dies zeigt, dass der Grad von g mindestens so groß wie der Grad von f ist, woraus $g = f$ folgt. Damit gilt $[K(\vartheta) : K] = \mathrm{grad}(f) = n = [L : K]$. Aus $K(\vartheta) \subseteq L$ und $[K(\vartheta) : K] = [L : K]$ folgt $L = K(\vartheta)$. □

§ 19. *Auflösbarkeit von Polynomgleichungen durch Radikale*

Zusammenfassung. Eine der populärsten klassischen Anwendung der Galoistheorie ist der Beweis der Nicht-Auflösbarkeit allgemeiner Polynomgleichungen fünften und höheren Grades. Dies kann zurückgeführt werden auf einen zentralen Satz, der die Frage nach der Auflösbarkeit einer beliebigen Polynomgleichung auf eine Eigenschaft der Galoisgruppe zurückzuführt, nämlich die Auflösbarkeit dieser Gruppe im Sinne von § 7. Im vorliegenden Kapitel soll dieser Satz bewiesen werden.

Wichtige Grundbegriffe

- Radikalerweiterung
- Auflösbarkeit eines Polynoms durch Radikale

Zentrale Sätze

- Jede galois'sche Radikalerweiterungen besitzt eine auflösbare Galoisgruppe.
- Ein Polynom f ist genau dann durch Radikale auflösbar, wenn seine Galoisgruppe $\mathrm{Gal}(f|K)$ auflösbar ist.

In gesamten Abschnitt betrachten wir der Einfachheit halber nur Körper der Charakteristik 0.

Definition 19.1 Eine ***Radikalerweiterung*** ist eine endliche Körpererweiterung $L|K$ mit folgenden Eigenschaften: Es gibt ein $r \in \mathbb{N}_0$, eine Kette von Zwischenkörpern

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$$

natürliche Zahlen $n_1, \ldots, n_r$ und für $1 \leq i \leq r$ Elemente $\gamma_i \in L_i$, so dass jeweils $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ erfüllt ist.

Die intuitive Vorstellung hinter dieser Definition besteht darin, dass die Elemente in einer Radikalerweiterung durch „beliebig tief verschachtelte Wurzelausdrücke“ dargestellt werden können. Ein typisches Element in einer Radikalerweiterung von $\mathbb{Q}$ ist beispielsweise

$$\alpha = \sqrt[3]{\sqrt{2+\sqrt{5}}+\sqrt{7}}.$$

Definieren wir nämlich die Elemente $\gamma_1 = \sqrt{5}$, $\gamma_2 = \sqrt{7}$, $\gamma_3 = \sqrt{2+\sqrt{5}}$ und $\gamma_4 = \alpha$, und setzen wir $K = L_0 = \mathbb{Q}$, $L_i = \mathbb{Q}(\gamma_1, \ldots, \gamma_i)$ für $1 \leq i \leq 4$ sowie $L = L_4$, dann ist $L|K$ eine Radikalerweiterung, die das Element α enthält. Tatsächlich gilt nach Definition $L_i = L_{i-1}(\gamma_i)$ für $1 \leq i \leq 4$ und außerdem $\gamma_1^2 = 5 \in L_0$, $\gamma_2^2 = 7 \in L_1$, $\gamma_3^2 = 2+\sqrt{5} \in L_2$ und $\gamma_4^3 = \alpha^3 = \gamma_3 + \gamma_2 \in L_3$.

Man beachte, dass insbesondere jede Erweiterung, die durch Adjunktion von endlich vielen Einheitswurzeln zu Stande kommt, eine Radikalerweiterung ist. Elemente, die in einer Radikalerweiterung $L|K$ enthalten sind, werden auch aus ***Radikale*** über K bezeichnet.

Definition 19.2 Man sagt, ein nicht-konstantes Polynom $f \in K[x]$ ist ***durch Radikale auflösbar***, wenn eine Radikalerweiterung $L|K$ existiert, so dass f über L in Linearfaktoren zerfällt.

Intuitiv ist ein nicht-konstantes Polynom also genau dann durch Radikale auflösbar, wenn all seine Nullstellen durch verschachtelte Wurzeln darstellbar sind. Das Hauptziel dieses Kapitels ist der Nachweis, dass diese Eigenschaft an der Galoisgruppe $\mathrm{Gal}(f|K)$ des Polynoms abgelesen werden kann. Auf Grund der Generalvoraussetzung dieses Kapitels, dass wir nur Körper der Charakteristik 0 betrachten, ist für einen Zerfällungskörper L von f über K die Erweiterung stets eine Galois-Erweiterung, siehe Satz 15.3 und Satz 15.9.

Satz 19.3 Sei $f \in K[x]$ ein nicht-konstantes Polynom mit auflösbarer Galoisgruppe $G = \mathrm{Gal}(f|K)$. Dann ist f durch Radikale auflösbar.

Beweis: Sei L ein Zerfällungskörper von f über K, so dass $G = \mathrm{Gal}(L|K)$ gilt. Auf Grund der Auflösbarkeit von G existiert nach Satz 7.14 eine Kette $G = U_0 \supseteq U_1 \supseteq \ldots \supseteq U_r = \{\mathrm{id}_L\}$ mit $U_i \trianglelefteq U_{i-1}$ und der Eigenschaft, dass U_{i-1}/U_i zyklisch ist, für $1 \leq i \leq r$. Nach dem Hauptsatz der Galoistheorie entspricht diese Untergruppenkette einer Kette $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$ von Zwischenkörpern $L_i = L^{U_i}$. Weil die Zuordnungen $U \mapsto L^U$ und $M \mapsto \mathrm{Gal}(L|M)$ zueinander invers sind, gilt $\mathrm{Gal}(L|L_i) = U_i$ für $0 \leq i \leq r$. Nach Satz 16.9 liefert die Einschränkungsabbildung $\sigma \mapsto \sigma|_{L_i}$ jeweils einen Isomorphismus

$$U_{i-1}/U_i \quad = \quad \mathrm{Gal}(L|L_{i-1})/\mathrm{Gal}(L|L_i) \quad \cong \quad \mathrm{Gal}(L_i|L_{i-1}).$$

Dies zeigt, dass es sich bei Gruppen $\mathrm{Gal}(L_i|L_{i-1})$ um endliche zyklische Gruppen handelt. Es ist nun naheliegend, Satz 18.5 auf diese Erweiterungen anzuwenden, aber leider ist das nicht möglich, weil wir nicht davon ausgehen können, dass der Grundkörper L_{i-1} jeweils die dazu notwendige Einheitswurzel enthält.

Um diese Situation herbeizuführen, definieren wir $n_i = |U_{i-1}/U_i| = [L_i : L_{i-1}]$ für $1 \leq i \leq r$ und setzen $n = \mathrm{kgV}(n_1, \ldots, n_r)$. Es sei $\tilde{L}$ ein algebraischer Abschluss von L und $\zeta \in \tilde{L}$ eine primitive n-te Einheitswurzel. Wir definieren nun $L_i' = L_i(\zeta)$ für $1 \leq i \leq r$. Wegen $L_i' = L_i \cdot L_{i-1}(\zeta)$ und auf Grund des Verschiebungssatzes der Galoistheorie, Satz 16.13, existiert ein Isomorphismus

$$\mathrm{Gal}(L_i'|L_{i-1}') \quad \cong \quad \mathrm{Gal}(L_i|L_i \cap L_{i-1}(\zeta)).$$

Die Gruppe rechts ist eine Untergruppe von $\mathrm{Gal}(L_i|L_{i-1})$ und somit zyklisch; ihre Ordnung m_i ist nach dem Satz von Lagrange ein Teiler von $n_i = |\mathrm{Gal}(L_i|L_{i-1})|$. Also gilt dasselbe auch für $\mathrm{Gal}(L_i'|L_{i-1}')$. Da eine geeignete Potenz von ζ eine primitive m_i-te Einheitswurzel ist und in L_{i-1}' liegt, kann Satz 18.5 nun angewendet werden. Demnach existiert ein Element $\gamma_i \in L_i'$ und ein $k_i \in \mathbb{N}$, so dass $L_i' = L_{i-1}'(\gamma_i)$ und $\gamma_i^{k_i} \in L_{i-1}'$ erfüllt sind. Die Körperkette

$$K \quad = \quad L_0 \quad \subseteq \quad L_0' \quad \subseteq \quad L_1' \quad \subseteq \quad \ldots \quad \subseteq \quad L_r'$$

zeigt nun, dass $L_r'|K$ eine Radikalerweiterung ist. Wegen $L = L_r \subseteq L_r'$ zerfällt f über L_r' in Linearfaktoren. Also ist f durch Radikale auflösbar. □

Der Beweis der Umkehrung ist ein wenig aufwändiger. Hier benötigen wir zur Vorbereitung drei Hilfssätze.

Lemma 19.4 Seien $L_1|K$ und $L_2|K$ zwei normale Erweiterungen desselben Körpers K. Dann ist auch die Erweiterung $L_1 \cap L_2|K$ normal. Sind L_1 und L_2 in einem gemeinsamen Erweiterungskörper M enthalten, dann ist auch $L_1 \cdot L_2|K$ eine normale Erweiterung, wobei $L_1 \cdot L_2$ das Kompositum von L_1 und L_2 in M bezeichnet.

Beweis: Um zu zeigen, dass $L_1 \cap L_2|K$ normal ist, genügt es nach Satz 15.3, die Gleichung $\mathrm{Hom}_K(L_1 \cap L_2, \tilde{K}) = \mathrm{Aut}_K(L_1 \cap L_2)$ zu beweisen, wobei $\tilde{K}$ einen algebraischen Abschluss von L_1 bezeichnet. Dabei ist die Inklusion „$\supseteq$“ offensichtlich; für den Nachweis der umgekehrten Inklusion sei $\sigma \in \mathrm{Hom}_K(L_1 \cap L_2, \tilde{K})$ vorgegeben. Weil $L_1|K$ und $L_2|K$ algebraisch und $\tilde{K}$ algebraisch abgeschlossen ist, existieren nach Satz 13.9 Fortsetzungen σ_1 und σ_2 von σ auf L_1 bzw. L_2. Weil $L_1|K$ und $L_2|K$ normal sind, gilt $\sigma_1(L_1) \subseteq L_1$ und $\sigma_2(L_2) \subseteq L_2$. Ist nun $\alpha \in L_1 \cap L_2$, dann gilt $\sigma(\alpha) = \sigma_1(\alpha) \in L_1$ und $\sigma(\alpha) = \sigma_2(\alpha) \in L_2$, also $\sigma(L_1 \cap L_2) \subseteq L_1 \cap L_2$ und damit $\sigma \in \mathrm{Aut}_K(L_1 \cap L_2)$.

Für den Beweis der zweiten Aussage zeigen wir $\mathrm{Hom}_K(L_1 \cdot L_2, \tilde{K}) = \mathrm{Aut}_K(L_1 \cdot L_2)$, wobei $\tilde{K}$ diesmal einen algebraischen Abschluss von M bezeichnet. Wieder genügt es, die Inklusion „$\subseteq$“ zu überprüfen. Sei also $\sigma \in \mathrm{Hom}_K(L_1 \cdot L_2, \tilde{K})$ vorgegeben. Dann gilt $\sigma|_{L_i} \in \mathrm{Hom}_K(L_i, \tilde{K})$ für $i = 1, 2$. Weil $L_i|K$ jeweils normal ist, folgt $\sigma(L_i) \subseteq L_i$ für $i = 1, 2$. Der Körper $L_1 \cdot L_2$ enthält also $\sigma(L_1)$ und $\sigma(L_2)$. Aus $\sigma^{-1}(L_1 \cdot L_2) \supseteq L_1$ und $\sigma^{-1}(L_1 \cdot L_2) \supseteq L_2$ folgt $\sigma^{-1}(L_1 \cdot L_2) \supseteq L_1 \cdot L_2$ und damit $\sigma(L_1 \cdot L_2) \subseteq L_1 \cdot L_2$. Damit ist $\sigma \in \mathrm{Aut}_K(L_1 \cdot L_2)$ nachgewiesen. □

Proposition 19.5

(i) Sei $L|K$ eine Radikalerweiterung, $\tilde{K}$ ein algebraischer Abschluss von K und $\sigma : L \to \tilde{K}$ ein K-Homomorphismus. Dann ist auch $\sigma(L)|K$ eine Radikalerweiterung.

(ii) Ein Kompositum zweier Radikalerweiterungen ist eine Radikalerweiterung.

(iii) Ist $L|K$ eine Radikalerweiterung, so gibt es einen Erweiterungskörper M von L mit der Eigenschaft, das $M|K$ eine Galois-Erweiterung und zugleich eine Radikalerweiterung ist.

Beweis: zu (i) Nach Voraussetzung gibt es ein $r \in \mathbb{N}_0$, eine Kette $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$ von Zwischenkörpern, Zahlen $n_i \in \mathbb{N}$ und Elemente $\gamma_i \in L_i$ mit $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ für $1 \leq i \leq r$. Durch Anwendung von σ erhalten wir eine Körperkette $K = \sigma(L_0) \subseteq \sigma(L_1) \subseteq \ldots \subseteq \sigma(L_r) = \sigma(L)$. Außerdem gilt $\sigma(L_i) = \sigma(L_{i-1})(\sigma(\gamma_i))$ und $\sigma(\gamma_i)^{n_i} \in \sigma(L_{i-1})$ für $1 \leq i \leq r$. Dies zeigt, dass $\sigma(L)|K$ eine Radikalerweiterung ist.

zu (ii) Seien $L|K$ und $M|K$ zwei Radikalerweiterungen, wobei L und M in einem gemeinsamen Erweiterungskörper $\tilde{K}$ enthalten sind. Dann existieren $r, s \in N_0$, Ketten $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$ und $K = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_s = M$ von Zwischenkörpern, Zahlen $m_i, n_i \in \mathbb{N}$ und Elemente $\gamma_i \in L_i$, $\delta_i \in M_i$ mit $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{m_i} \in L_{i-1}$ für $1 \leq i \leq r$ und $M_i = M_{i-1}(\delta_i)$ sowie $\delta_i^{n_i} \in M_{i-1}$ für $1 \leq i \leq s$. Setzen wir $M_i' = L \cdot M_i$ für $0 \leq i \leq s$, dann erhalten wir eine Kette

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L = M_0' \subseteq M_1' \subseteq \ldots \subseteq M_s' = L \cdot M.$$

Dabei gilt jeweils $M_i' = L \cdot M_i = L \cdot M_{i-1}(\delta_i) = M_{i-1}'(\delta_i)$ und $\delta_i^{n_i} \in M_{i-1}'$. Damit ist nachgewiesen, dass es sich bei $L \cdot M|K$ um eine Radikalerweiterung handelt.

zu (iii) Sei $\tilde{K}$ ein algebraischer Abschluss von L. Nach dem Satz vom primitiven Element gilt $L = K(\alpha)$ für ein $\alpha \in L$. Sei $f = \mu_{K,\alpha}$ das Minimalpolynom von α über K, und seien $\alpha_1 = \alpha, \ldots, \alpha_r$ die verschiedenen Nullstellen von f in $\tilde{K}$. Setzen wir $M = K(\alpha_1, \ldots, \alpha_r)$, dann ist M Zerfällungskörper von f über K und $M|K$ somit eine Galois-Erweiterung; es sei daran erinnert, dass auf Grund unserer Generalvoraussetzung $\mathrm{char}(K) = 0$ jede algebraische Erweiterung auch

separabel ist. Man überprüft leicht, dass M das Kompositum der Körper $K(\alpha_1) = L$, $K(\alpha_2), \ldots, K(\alpha_r)$ in $\tilde{K}$ ist. Auf Grund des Fortsetzungssatzes 12.2 gibt es jeweils einen K-Isomorphismus $\sigma_i : L \to K(\alpha_i)$ mit $\sigma_i(\alpha) = \alpha_i$. Aus Teil (i) folgt nun, dass mit $L|K$ auch $K(\alpha_i)|K$ eine Radikalerweiterung ist, und nach Teil (ii) ist damit auch $M|K$ eine Radikalerweiterung. □

Proposition 19.6 Ist $L|K$ eine galoissche Radikalerweiterung, dann ist $G = \mathrm{Gal}(L|K)$ eine auflösbare Gruppe.

Beweis: Weil $L|K$ eine Radikalerweiterung ist, gibt es ein $r \in \mathbb{N}_0$, eine Kette $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$ von Zwischenkörpern, natürliche Zahlen $n_1, \ldots, n_r$ und Elemente $\gamma_i \in L_i$, so dass $L_i = L_{i-1}(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}$ für $1 \leq i \leq r$ erfüllt ist. Es sei $n = \mathrm{kgV}(n_1, \ldots, n_r)$ und $\tilde{L}$ ein algebraischer Abschluss von L. Weiter sei $\zeta \in \tilde{L}$ eine primitive n-te Einheitswurzel und $L_i' = L_i(\zeta)$ für $0 \leq i \leq r$; außerdem setzen wir $K' = K(\zeta) = L_0'$ und $L' = L(\zeta) = L_r'$. Nach Satz 17.4 ist $K(\zeta)|K$ eine Galois-Erweiterung, ebenso $L|K$. Wegen $L' = L \cdot K' = L \cdot K(\zeta)$ und Lemma 19.4 ist auch $L'|K$ eine Galois-Erweiterung, und damit auch die Erweiterung $L'|K'$; dabei ist zu beachten, dass auf Grund unserer Generalvoraussetzung $\mathrm{char}(K) = 0$ alle algebraischen Erweiterungen automatisch separabel sind. Aus demselben Grund ist auch $L_i'|L_{i-1}'$ jeweils eine Galois-Erweiterung.

Wir zeigen nun, dass die Galoisgruppe $\mathrm{Gal}(L'|K')$ auflösbar ist. Für $1 \leq i \leq r$ gilt jeweils $L_i' = L_{i-1}'(\gamma_i)$ und $\gamma_i^{n_i} \in L_{i-1}'$, außerdem ist eine geeignete Potenz von ζ eine primitive n_i-te Einheitswurzel in L_{i-1}'. Wir können jetzt Satz 18.2 anwenden und erhalten als Resultat, dass $L_i'|L_{i-1}'$ für $1 \leq i \leq r$ jeweils eine endliche Galois-Erweiterung mit zyklischer Galoisgruppe ist. Sei nun $U_i = \mathrm{Gal}(L'|L_i')$ für $0 \leq i \leq r$. Diese Untergruppen von $\mathrm{Gal}(L'|K')$ bilden eine Kette $\mathrm{Gal}(L'|K') = U_0 \supseteq U_1 \supseteq \ldots \supseteq U_r = \{\mathrm{id}_{L'}\}$. Weil die Erweiterung $L_i'|L_{i-1}'$ normal ist, handelt es sich bei U_i jeweils um einen Normalteiler von U_{i-1}, und nach Satz 16.9 induziert die Einschränkungsabbildung $\sigma \mapsto \sigma|_{L_i'}$ einen Isomorphismus

$$U_{i-1}/U_i \quad = \quad \mathrm{Gal}(L'|L_{i-1}')/\mathrm{Gal}(L'|L_i') \quad \cong \quad \mathrm{Gal}(L_i'|L_{i-1}').$$

Mit $\mathrm{Gal}(L_i'|L_{i-1}')$ sind also auch die Faktorgruppen U_{i-1}/U_i endlich und zyklisch. Wegen Satz 7.14 ist die Gruppe $\mathrm{Gal}(L'|K')$ also tatsächlich auflösbar.

Auf Grund des Verschiebungssatzes der Galoistheorie und wegen $L' = L(\zeta) = L \cdot K'$ gilt $\mathrm{Gal}(L'|K') \cong \mathrm{Gal}(L|L \cap K')$. Also ist auch $\mathrm{Gal}(L|L \cap K')$ eine auflösbare Gruppe. Mit $L|K$ und $K'|K$ ist nach Lemma 19.4 auch $L \cap K'|K$ eine Galois-Erweiterung. Die Galoisgruppe $K'|K$ ist nach Satz 17.4 abelsch (denn jede zu eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ isomorphe Gruppe ist abelsch), also insbesondere auflösbar. Wegen $\mathrm{Gal}(L \cap K'|K) \cong \mathrm{Gal}(K'|K)/\mathrm{Gal}(K'|L \cap K')$ ist $\mathrm{Gal}(L \cap K'|K)$ isomorph zu einer Faktorgruppe von $\mathrm{Gal}(K'|K)$, also ebenfalls auflösbar. Aus der Auflösbarkeit von $\mathrm{Gal}(L|L \cap K')$ und der Auflösbarkeit von $\mathrm{Gal}(L|K)/\mathrm{Gal}(L|L \cap K') \cong \mathrm{Gal}(L \cap K'|K)$ folgt mit Satz 7.15 schließlich die Auflösbarkeit von $\mathrm{Gal}(L|K)$. □

Satz 19.7 Sei $f \in K[x]$ ein nicht-konstantes, durch Radikale auflösbares Polynom. Dann ist $\mathrm{Gal}(f|K)$ eine auflösbare Gruppe.

Beweis: Nach Voraussetzung gibt es eine Radikalerweiterung $L|K$ mit der Eigenschaft, dass f über L in Linearfaktoren zerfällt, und wegen Proposition 19.5 (iii) dürfen wir annehmen, dass $L|K$ eine Galois-Erweiterung ist. Setzen wir $L_1 = K(\alpha_1, \ldots, \alpha_r)$, wobei $\alpha_1, \ldots, \alpha_r$ die verschiedenen Nullstellen von f in L bezeichnen, dann ist $\mathrm{Gal}(f|K)$ isomorph zu

$\mathrm{Gal}(L_1|K)$. Nach Satz 19.6 ist die Gruppe $\mathrm{Gal}(L|K)$ auflösbar. Wegen $\mathrm{Gal}(L|K)/\mathrm{Gal}(L|L_1) \cong \mathrm{Gal}(L_1|K)$ sind $\mathrm{Gal}(L_1|K)$ und $\mathrm{Gal}(f|K)$ isomorph zu einer Faktorgruppe von $\mathrm{Gal}(L|K)$. Nach Satz 7.15 ist somit auch $\mathrm{Gal}(f|K)$ auflösbar. □

Ingesamt ist ein nicht-konstantes Polynom $f \in K[x]$ also genau dann durch Radikale auflösbar, wenn die Gruppe $\mathrm{Gal}(f|K)$ auflösbar ist.

Folgerung 19.8 Sei K ein Körper der Charakteristik 0 und $f \in K[x]$ ein nicht-konstantes Polynom.

(i) Ist f vom Grad ≤ 4, dann ist f durch Radikale auflösbar.

(ii) Ist $\mathrm{Gal}(f|K)$ isomorph zu A_n oder S_n mit $n \geq 5$, dann ist f nicht durch Radikale auflösbar.

Beweis: zu (i) Nach Satz 16.11 ist $\mathrm{Gal}(f|K)$ isomorph zu einer Untergruppe von S_m, wobei m die Anzahl der verschiedenen Nullstellen von f in einem Zerfällungskörper L von f über K bezeichnet. Setzen wir $n = \mathrm{grad}(f)$, dann ist $\mathrm{Gal}(f|K)$ auch isomorph zu einer Untergruppe von S_n (weil S_m isomorph zu einer Untergruppe von S_n ist). Die symmetrische Gruppe S_n ist für $n \leq 4$ auflösbar. Aus Satz 7.15 folgt somit, dass auch $\mathrm{Gal}(f|K)$ eine auflösbare Gruppe ist. Auf Grund von Satz 19.3 ist f also durch Radikale auflösbar.

zu (ii) Die Gruppen A_n und S_n sind für $n \geq 5$ nicht auflösbar, also gilt dasselbe für $\mathrm{Gal}(f|K)$. Aus Satz 19.7 folgt damit, dass f nicht durch Radikale auflösbar ist. □

Man kann zeigen, dass „die meisten“ Polynome $f \in K[x]$ vom Grad n mit eine zu S_n isomorphe Galois-Gruppe besitzen (eine Aussage, die natürlich präzisiert werden muss). Dies bedeutet, dass „die meisten“ Polynome vom Grad ≥ 5 nicht durch Radikale auflösbar sind. Daraus folgt insbesondere, dass es für Polynomgleichungen dieser Grade keine Lösungsformel (ähnlich der p-q-Formel für quadratische Gleichungen) geben kann, die nur aus Wurzelausdrücken besteht. Es ist auch nicht schwer zu zeigen, dass für jedes irreduzible Polynom $f \in K[x]$ vom Grad 5 mit genau drei reellen Nullstellen jeweils $\mathrm{Gal}(f|K) \cong S_5$ gilt. Zum Beispiel $x^5 - 4x + 2 \in \mathbb{Q}[x]$ ein solches Polynom. Folglich lassen sich die Nullstellen dieses Polynoms (weder die reellen noch die beiden nicht-reellen) durch einen verschachtelten Wurzelausdruck darstellen.

Literaturverzeichnis

[Ar] M. Artin, *Algebra*. Birkhäuser Advanced Texts.

[Bö] J. Böhm, *Grundlagen der Algebra und Zahlentheorie*. Springer-Verlag.

[Bo] S. Bosch, *Algebra*. Springer-Verlag.

[Fi] G. Fischer, *Lehrbuch der Algebra*. 4. Auflage, Springer-Verlag.

[Hi] J. Hilgert, *Lesebuch Mathematik für das erste Studienjahr*. Springer-Verlag.

[Lo] F. Lorenz, F. Lemmermeyer, *Algebra 1*. Spektrum Akademischer Verlag.

[Ph] P. Philip, *Linear Algebra*. Vorlesung an der LMU München, WS 18/19.