Algebra

Thomas Kahle

21. 10. 2026

Inhaltsverzeichnis

1 Gruppentheorie 5
1.1 Einleitung 5
1.2 Die Diedergruppe 11
1.3 Die symmetrische Gruppe 17
1.4 Homomorphismen 20
1.5 Gruppenwirkungen 25
1.6 Untergruppen 29
1.7 Spezielle Untergruppen 31
1.8 Zyklische Gruppen 35
1.9 Erzeugte Untergruppen 39
1.10 Der Untergruppenverband 41
1.11 Quotientengruppen 42
1.12 Der Satz von Lagrange 52
1.13 Die Isomorphiesätze 59
1.14 Ausblick: Das Hölderprogramm 65
2 Ringtheorie 66
2.1 Ringe und Grundbegriffe 67
2.2 Polynomringe und Gruppenringe 71
2.3 Ringhomomorphismen, Ideale und Quotienten 74
2.4 Maximale Ideale und Primideale 82
2.5 Teilbarkeit in Integritätsbereichen 85
2.6 Polynomringe über Körpern 88
3 Körpertheorie 94
3.1 Charakteristik und Körpererweiterungen 94
3.2 Algebraische Erweiterungen 102
3.3 Konstruktionen mit Zirkel und Lineal 109
3.4 Zerfällungskörper und algebraischer Abschluss 113
3.5 Endliche Körper und Separabilität 121
3.6 Ausblick: Galoistheorie 124
Stichwortverzeichnis 128

Vorbemerkungen

- Die Vorlesung wurde im Sommersemester 2021 an der OvGU Magdeburg gehalten. Dieses Skript ist eine ausgearbeitete Fassung der handschriftlichen Vorlesungsnotizen.
- Videoaufzeichnungen der Vorlesung von 2021 gibt es hier.
- Als Lehrbuch ist *Abstract Algebra* von Dummit und Foote empfehlenswert.
- Das Dokument ist in Bearbeitung. Es kann auch Änderungen an bereits veröffentlichten Teilen geben.
- Bitte nicht weitergeben und nicht im Internet posten.
- Über Mitteilungen von Fehlern bin ich sehr dankbar.
- Denken Sie immer selbst und glauben Sie nicht blind, bloß weil es schön in typst gesetzt ist.
- Dozent: Thomas Kahle
  - e-mail: `thomas.kahle@ovgu.de`
  - Homepage: thomas.kahle.de
  - Mastodon: @tomkalei@machteburch.social

Goldene Skriptregeln

1. Skript lesen ersetzt nicht den Vorlesungsbesuch.
2. Skript abspeichern ersetzt nicht das Lesen.

Worum geht es?

Die Algebra untersucht Mengen, auf denen Verknüpfungen wie Addition und Multiplikation erklärt sind, und zwar nicht anhand konkreter Zahlen, sondern allein anhand der Rechenregeln, die diese Verknüpfungen erfüllen. Die Vorlesung besteht aus drei Teilen:

- **Gruppentheorie**: eine Verknüpfung, die assoziativ ist, ein neutrales Element hat und bezüglich der jedes Element invertierbar ist.
- **Ringtheorie**: zwei Verknüpfungen, Addition und Multiplikation, die durch das Distributivgesetz verbunden sind. Die ganzen Zahlen und Polynomringe sind die wichtigsten Beispiele.
- **Körpertheorie**: Ringe, in denen man durch jedes Element außer der Null teilen kann. Hier geht es vor allem um Körpererweiterungen und das Lösen von Polynomgleichungen.

Am Ende werden die drei Teile in einem Ausblick auf die Galoistheorie zusammenfinden, die Gruppen benutzt, um Körpererweiterungen zu verstehen.

1 Gruppentheorie

1.1 Einleitung

Der Begriff der Gruppe ist aus mehreren Strömungen der Mathematik entstanden, die zunächst wenig miteinander zu tun hatten. Wir stellen drei davon kurz vor. VL1

Zahlentheorie

In der Zahlentheorie hat man es mit Gruppen wie $\mathbb{Z}$ und daraus abgeleiteten Gruppen zu tun, zum Beispiel mit den Restklassen modulo n.

Beispiel 1.1.1: Euler zeigte 1761, dass a^{40} auf die Ziffern 01 endet, falls a eine ganze Zahl ist, die weder durch 2 noch durch 5 teilbar ist. Zum Beispiel ist

$$7^{40} = 63668057609090279857414351392240 01.$$

In moderner Sprache besagt Eulers Satz, dass $a^{40} \equiv 1 \bmod 100$ für alle zu 10 teilerfremden a gilt. Heutzutage folgt er als Spezialfall des Satzes von Lagrange über Gruppen, den wir in diesem Kapitel beweisen werden: Die zu 100 teilerfremden Restklassen bilden eine Gruppe mit 40 Elementen.

Beispiel 1.1.2: Der *große Satz von Fermat* besagt, dass die Gleichung

$$x^n + y^n = z^n$$

für $n \geq 3$ keine ganzzahligen Lösungen mit $xyz \neq 0$ hat (und damit auch keine rationalen). Fermat notierte die Aussage um 1637, bewiesen wurde sie erst 1994 von Andrew Wiles. Der Beweis benutzt in wesentlicher Weise Gruppen, die aus elliptischen Kurven entstehen.

Beispiel 1.1.3: Eine *elliptische Kurve* ist (für uns) die Lösungsmenge einer Gleichung wie

$$y^2 = x^3 - 2x.$$

Diese Kurve hat unendlich viele rationale Punkte, zum Beispiel $(0,0)$, $(-1,1)$ und $(2,2)$. Schon im 17. Jahrhundert war Folgendes bekannt: Verbindet man zwei rationale Punkte der Kurve durch eine Gerade und schneidet diese mit der Kurve, so erhält man einen dritten Punkt, der wieder rational ist und auf der Kurve liegt. Die Gerade durch $P = (0,0)$ und $Q = (2,2)$ ist zum Beispiel $y = x$. Setzt man sie in die Kurvengleichung ein, erhält man $x^3 - x^2 - 2x = x(x-2)(x+1) = 0$. Neben

thomas.kahle@ovgu.de

$x = 0$ und $x = 2$ ist also $x = -1$ eine Lösung, und der dritte Schnittpunkt ist der rationale Punkt $R = (-1, -1)$.

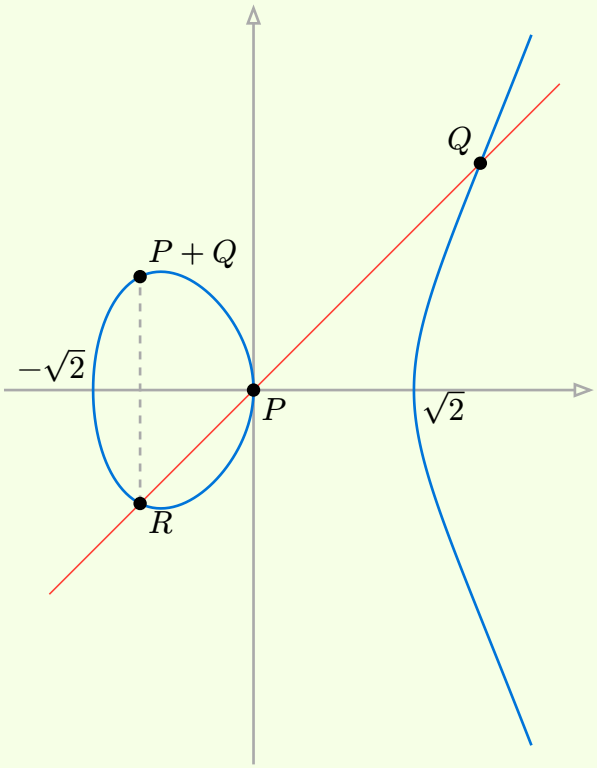


Abbildung 1: Die elliptische Kurve $y^2 = x^3 - 2x$ mit der Sekante durch P und Q.

Die Abbildung, die zwei Punkten den dritten Schnittpunkt zuordnet, kann man als eine Art Multiplikation auffassen. Nach einer kleinen Modifikation (man spiegelt den dritten Schnittpunkt an der x-Achse und nimmt einen Punkt im Unendlichen als neutrales Element hinzu) bilden die rationalen Punkte der Kurve damit tatsächlich eine Gruppe. In Abbildung 1 ist $P + Q = (-1, 1)$.

Lösung von Polynomgleichungen

Sie kennen die p-q-Formel

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

für die Lösungen von $x^2 + px + q = 0$. Analoge Formeln, die die Lösungen durch die Koeffizienten, die Grundrechenarten und Wurzelziehen ausdrücken, sind auch für Gleichungen dritten und vierten Grades

$$x^3 + ax^2 + bx + c = 0 \quad \text{und} \quad x^4 + ax^3 + bx^2 + cx + d = 0$$

bekannt (Cardano und Ferrari, 16. Jahrhundert). 1824 bewies Abel, dass es für Grad 5 und höher keine solchen Formeln geben kann. Dieser Beweis und die darauf aufbauende Theorie von Galois benutzen intensiv Gruppentheorie, denn sie studieren, wie

© 2026 Thomas Kahle

Transformationen (Automorphismen) von Körpern die Nullstellen von Polynomen permutieren. Am Ende der Vorlesung werden wir sehen, wie das funktioniert.

Symmetrie

Gruppen beschreiben Symmetrien: Die Symmetrieoperationen eines geometrischen Objekts kann man hintereinander ausführen und umkehren. Diesen Gesichtspunkt werden wir im nächsten Abschnitt an der Diedergruppe als Erstes vertiefen.

Bemerkenswerterweise stammt die formale Definition einer Gruppe erst aus der Zeit um 1882 (Walther von Dyck), also lange nach den „Anwendungen“ von Gruppen.

Die Definition

Definition 1.1.4: Eine *Gruppe* ist eine Menge G mit einer binären Operation (*Verknüpfung*)

$$*\colon G \times G \to G, \quad (a,b) \mapsto a * b,$$

sodass gilt:

1. $a * (b * c) = (a * b) * c$ für alle $a, b, c \in G$ (*Assoziativität*).
2. Es gibt ein $e \in G$, genannt *Identität*, *Einselement* oder *neutrales Element*, mit $e * a = a * e = a$ für alle $a \in G$.
3. Zu jedem $a \in G$ existiert ein *Inverses* $a^{-1} \in G$ mit $a^{-1} * a = e$ und $a * a^{-1} = e$.

Die Gruppe G heißt *abelsch*, falls $a * b = b * a$ für alle $a, b \in G$ gilt (*Kommutativität*).

Dass $*$ eine Abbildung $G \times G \to G$ ist, beinhaltet, dass das Ergebnis der Verknüpfung zweier Elemente von G wieder in G liegt. Wir schreiben eine Gruppe auch als Paar $(G, *)$, wenn die Verknüpfung betont werden soll.

Beispiel 1.1.5:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Gruppen bezüglich der Addition.
- $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ ist eine Gruppe bezüglich der Multiplikation.
- Allgemeiner ist $K^* := K \setminus \{0\}$ für jeden Körper K eine Gruppe bezüglich der Multiplikation.
- $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$ ist eine Gruppe bezüglich der Multiplikation.

All diese Gruppen sind abelsch.

Etwas weniger triviale Beispiele erhält man aus den Restklassen modulo n.

thomas.kahle@ovgu.de

Beispiel 1.1.6: Sei $n \geq 1$. Die Restklassen modulo n bilden mit der Addition von Restklassen die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Wir schreiben $\overline{a}$ für die Restklasse von $a \in \mathbb{Z}$. Das neutrale Element ist $\overline{0}$, und das Inverse von $\overline{a}$ ist $\overline{-a}$.

Beispiel 1.1.7: Sei $n \geq 2$. Die Restklassen $\overline{a}$ modulo n mit $\mathrm{ggT}(a, n) = 1$ bilden mit der Multiplikation von Restklassen eine Gruppe $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$. Die Multiplikation ist wohldefiniert, und mit $\mathrm{ggT}(a, n) = 1$ und $\mathrm{ggT}(b, n) = 1$ ist auch $\mathrm{ggT}(ab, n) = 1$. Assoziativität und das neutrale Element $\overline{1}$ erbt man von $\mathbb{Z}$. Die Existenz von Inversen folgt aus dem euklidischen Algorithmus: Ist $\mathrm{ggT}(a, n) = 1$, so existieren $x, y \in \mathbb{Z}$ mit

$$1 = ax + ny$$

(Lemma von Bézout). Modulo n bedeutet das

$$\overline{1} = \overline{a} \cdot \overline{x} + \overline{n} \cdot \overline{y} = \overline{a} \cdot \overline{x},$$

denn $\overline{n} = \overline{0}$. Also ist $\overline{x}$ das Inverse von $\overline{a}$ (und es ist $\mathrm{ggT}(x, n) = 1$, wie die Gleichung $1 = ax + ny$ zeigt).

Die Notation $(\mathbb{Z}/n\mathbb{Z})^*$ meint stets diese multiplikative Gruppe. Ist n eine Primzahl, so ist $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$. Mit $\mathbb{Z}/n\mathbb{Z}$ (ohne Stern!) meint man üblicherweise die additive Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Das Beispiel von Euler oben handelt von der Gruppe $(\mathbb{Z}/100\mathbb{Z})^*$.

Aus gegebenen Gruppen kann man neue konstruieren. Die einfachste Konstruktion ist das direkte Produkt.

Definition 1.1.8: Seien $(G, *)$ und $(H, \circ)$ Gruppen. Das *direkte Produkt* $G \times H$ ist die Menge der Paare $\{(g, h) : g \in G, h \in H\}$ mit der komponentenweisen Verknüpfung

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 * g_2, h_1 \circ h_2).$$

Übung. Prüfen Sie nach, dass das direkte Produkt $G \times H$ eine Gruppe ist. Was ist das neutrale Element, was ist das Inverse von (g, h)?

Wir leiten nun ein paar grundlegende Rechenregeln aus den Axiomen ab.

Proposition 1.1.9: Sei $(G, *)$ eine Gruppe.
1. Das neutrale Element von G ist eindeutig.

© 2026 Thomas Kahle

2. Für jedes $a \in G$ ist das Inverse a^{-1} eindeutig.
3. Für alle $a \in G$ gilt $\left(a^{-1}\right)^{-1} = a$.
4. Für alle $a, b \in G$ gilt $(a * b)^{-1} = b^{-1} * a^{-1}$.
5. Für alle $a_1, ..., a_n \in G$ ist der Wert des Produkts $a_1 * ... * a_n$ unabhängig von der Klammerung.

Beweis.

1. Seien e und e' beide neutrale Elemente. Dann gilt $e * e' = e$, weil e' neutral ist, und $e * e' = e'$, weil e neutral ist. Also ist $e = e'$.

2. Seien b und c zwei Inverse von a. Dann gilt $a * b = e = c * a$ und damit

$$c = c * e = c * (a * b) = (c * a) * b = e * b = b.$$

3. Nach 2. hat a^{-1} ein eindeutiges Inverses $\left(a^{-1}\right)^{-1}$, nämlich das eindeutige Element x mit $x * a^{-1} = a^{-1} * x = e$. Da a^{-1} invers zu a ist, gilt $a^{-1} * a = a * a^{-1} = e$. Also erfüllt $x = a$ diese Gleichungen, und es folgt $\left(a^{-1}\right)^{-1} = a$.

4. Sei $c = (a * b)^{-1}$, also $(a * b) * c = e$. Multiplikation von links mit a^{-1} liefert (mit Assoziativität) $b * c = a^{-1}$, und Multiplikation von links mit b^{-1} liefert $c = b^{-1} * a^{-1}$.

5. Wir zeigen per Induktion nach n, dass jede Klammerung von $a_1 * ... * a_n$ denselben Wert hat wie das von links geklammerte Produkt

$$L(a_1, ..., a_n) := (...((a_1 * a_2) * a_3) * ...) * a_n.$$

Für $n \leq 2$ gibt es nichts zu zeigen, und $n = 3$ ist genau das Assoziativgesetz. Sei nun $n \geq 3$ und die Aussage für alle kürzeren Produkte bewiesen. Jede Klammerung des Produkts zerfällt als äußerstes Produkt in

$$X * Y$$

wobei X ein geklammertes Produkt von $a_1, ..., a_k$ und Y ein geklammertes Produkt von $a_{k+1}, ..., a_n$ ist, für ein $1 \leq k < n$. Nach Induktionsvoraussetzung ist $X = L(a_1, ..., a_k)$, und wir dürfen Y beliebig umklammern. Ist $k = n - 1$, so ist $X * Y = L(a_1, ..., a_{n-1}) * a_n = L(a_1, ..., a_n)$ und wir sind fertig. Ist $k < n - 1$, so schreiben wir $Y = a_{k+1} * Y'$ mit einem Produkt Y' von $a_{k+2}, ..., a_n$ und erhalten mit dem Assoziativgesetz

$$X * Y = X * (a_{k+1} * Y') = (X * a_{k+1}) * Y' = L(a_1, ..., a_{k+1}) * Y'.$$

Damit ist das äußere Produkt um eine Stelle nach rechts gewandert, und nach höchstens $n - 1 - k$ Wiederholungen dieses Schritts sind wir im Fall $k = n - 1$. ∎

Ab sofort schreiben wir Gruppen standardmäßig *multiplikativ*, d.h. wir lassen das Symbol $*$ weg und schreiben $ab := a * b$. Das neutrale Element bezeichnen wir mit 1 und das Inverse von a mit a^{-1}. Man beachte, dass im Allgemeinen $ab \neq ba$ ist. Deswegen

thomas.kahle@ovgu.de

ist auch die Bruchschreibweise $\frac{a}{b}$ in Gruppen nicht erlaubt: Es wäre nicht klar, ob ab^{-1} oder $b^{-1}a$ gemeint ist.

Definition 1.1.10: Sei G eine Gruppe und $x \in G$. Für $n \in \mathbb{Z}_{>0}$ definieren wir die *Potenzen*

$$x^n := \underbrace{xx\cdots x}_{n \text{ mal}}, \quad x^{-n} := \underbrace{x^{-1}x^{-1}\cdots x^{-1}}_{n \text{ mal}}, \quad x^0 := 1.$$

Dann gelten die üblichen Potenzgesetze

$$x^n x^m = x^{n+m} \quad \text{und} \quad (x^n)^m = x^{nm} \quad \text{für alle } n, m \in \mathbb{Z}.$$

Insbesondere ist $x^n x^{-n} = x^0 = 1$ eine gültige Gleichung, und es gilt $(x^n)^{-1} = x^{-n}$.

Übung. Beweisen Sie die Potenzgesetze. Unterscheiden Sie dabei die Fälle nach den Vorzeichen von n und m.

Ist G eine *additive Gruppe* wie z.B. $\mathbb{Z}$, so verwenden wir die additive Schreibweise: $+$ für die Verknüpfung, $-x$ für das Inverse und 0 für das neutrale Element. Statt Potenzen schreiben wir dann Vielfache:

$$nx := \underbrace{x + \ldots + x}_{n \text{ mal}}, \quad (-n)x := -(nx), \quad 0x := 0.$$

Die additive Schreibweise verwenden wir nur für abelsche Gruppen.

Achtung! Außer in Beispielen sprechen wir über *abstrakte* Gruppen. Das heißt, wir verwenden nur die Axiome aus Definition 1.1.4 und beweisen damit Aussagen, obwohl die Notation manchmal zu suggestiv ist. Zum Beispiel darf man nicht $ab = ba$ verwenden, auch wenn das bei Zahlen so vertraut ist.

Proposition 1.1.11: Sei G eine Gruppe und $a, b \in G$. Dann sind die Gleichungen

$$ax = b \quad \text{und} \quad ya = b$$

eindeutig lösbar, d.h. es existieren eindeutige $x, y \in G$, für die das gilt.

Beweis. Die Elemente $x = a^{-1}b$ und $y = ba^{-1}$ sind Lösungen. Ist x' eine weitere Lösung von $ax' = b$, so liefert Multiplikation von links mit a^{-1}, dass $x' = a^{-1}b = x$ ist. Analog für y. ∎

Erfüllen $a, b \in G$ eine der beiden Gleichungen $ab = 1$ oder $ba = 1$, so gilt nach Proposition 1.1.11 schon $b = a^{-1}$ und damit auch die jeweils andere Gleichung. Das legt nahe, dass man in Definition 1.1.4 mit weniger Forderungen auskommt.

© 2026 Thomas Kahle

Übung. Sei G eine Menge mit einer assoziativen Verknüpfung, einem Element e mit $ea = a$ für alle $a \in G$, und so, dass zu jedem $a \in G$ ein $b \in G$ mit $ba = e$ existiert. Zeigen Sie, dass G eine Gruppe ist.

Definition 1.1.12: Sei G eine Gruppe und $x \in G$. Die *Ordnung* von x ist die kleinste positive ganze Zahl n mit $x^n = 1$. Man schreibt $|x|$ für die Ordnung. Falls keine solche Zahl existiert, setzt man $|x| = \infty$.

Das Symbol erinnert an die Kardinalität, und das ist Absicht: Die Ordnung von x ist die Anzahl der verschiedenen Potenzen von x in G,

$$|x| = |\{x^n : n \in \mathbb{Z}\}|,$$

wie wir bei den zyklischen Gruppen sehen werden.

Beispiel 1.1.13: In $(\mathbb{Z}/100\mathbb{Z})^*$ hat $\overline{7}$ die Ordnung 4, denn $7^2 = 49$, $7^3 = 343$ und $7^4 = 2401 \equiv 1 \bmod 100$. In $(\mathbb{Z}, +)$ hat jedes Element $x \neq 0$ unendliche Ordnung, während das neutrale Element 0 die Ordnung 1 hat.

1.2 Die Diedergruppe

Eine wichtige Klasse von Gruppen sind Symmetriegruppen von geometrischen Objekten, zum Beispiel von ebenen Figuren. Wir betrachten jetzt das reguläre n-Eck für ein $n \geq 3$.

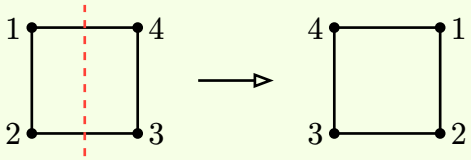
Definition 1.2.1: Sei $n \geq 3$. Die *Diedergruppe* D_{2n} ist die Menge der Symmetrieoperationen des regulären n-Ecks, d.h. der Bewegungen, die man mit einem n-Eck aus Holz im dreidimensionalen Raum ausführen kann, sodass anschließend die Ecken genau wieder auf Ecken zu liegen kommen. Die Verknüpfung ist das Hintereinanderausführen.

Das n-Eck darf also gedreht und umgedreht, aber nicht verbogen oder zerbrochen werden. Hintereinanderausführen von zwei Symmetrieoperationen ergibt wieder eine Symmetrieoperation. Das Hintereinanderausführen von Abbildungen ist assoziativ, das Nichtstun ist das neutrale Element und jede Symmetrieoperation kann man rückgängig machen. Also ist D_{2n} tatsächlich eine Gruppe. In der Literatur wird die Diedergruppe auch mit D_n bezeichnet. Wir schreiben D_{2n}, weil der Index dann, wie wir gleich sehen, die Anzahl der Elemente angibt.

Um die Gruppenstruktur zu verstehen, nummerieren wir die Ecken des n-Ecks gegen den Uhrzeigersinn mit $1, \ldots, n$. Jede Symmetrieoperation bildet Ecken auf Ecken ab und

liefert damit eine Permutation, also eine bijektive Abbildung der Menge $\{1, ..., n\}$ auf sich selbst.

Beispiel 1.2.2: Die Spiegelung des Quadrats an der senkrechten Achse vertauscht die Ecken wie folgt:



Sie liefert die Permutation $1 \mapsto 4$, $2 \mapsto 3$, $3 \mapsto 2$, $4 \mapsto 1$.

Die Anzahl der Symmetrien

Wir zeigen nun $|D_{2n}| = 2n$. Der erste Schritt ist die folgende Beobachtung.

Lemma 1.2.3: Jede Symmetrieoperation des n-Ecks ist durch das Bild der Kante zwischen den Ecken 1 und 2 eindeutig festgelegt.

Beweis. Die Ecken 1 und 2 bleiben benachbart, und der Rest des n-Ecks ist starr mit ihnen verbunden (kein Biegen und Brechen). Kennt man die Bilder von 1 und 2, so liegt auch die Lage des ganzen n-Ecks fest. ■

Worauf kann die Kante 1–2 abgebildet werden? Wir rechnen mit den Eckennummern modulo n, d.h. $n + 1 = 1$ und $1 - 1 = n$.

- Die Ecke 1 kann (zum Beispiel durch Drehen) auf jede Ecke $i \in \{1, ..., n\}$ abgebildet werden.
- Die Ecke 2 ist zu 1 benachbart, landet also auf $i + 1$ oder auf $i - 1$.

Beides ist möglich: Gibt es eine Symmetrie mit $1 \mapsto i$ und $2 \mapsto i + 1$ (eine Drehung), so kann man danach noch an der Geraden durch die Ecke i und den Mittelpunkt spiegeln und erhält eine Symmetrie mit $1 \mapsto i$ und $2 \mapsto i - 1$.

Insgesamt haben wir $2n$ Symmetrien gefunden. Das sind nach Lemma 1.2.3 alle, denn wir haben alle möglichen Bilder der Kante 1–2 ausgeschöpft. Also gilt $|D_{2n}| = 2n$.

Frage 1.2.4: Welches Element von D_8 ist die Punktspiegelung des Quadrats an seinem Mittelpunkt?

© 2026 Thomas Kahle

Rechnen in der Diedergruppe

Jetzt beschreiben wir D_{2n} als abstrakte Gruppe, sodass wir darin rechnen können. Wir fixieren n und ein reguläres n-Eck mit Mittelpunkt im Ursprung des $\mathbb{R}^2$, dessen Ecken gegen den Uhrzeigersinn nummeriert sind. Sei

- r die Drehung um $(2\pi)/n$ gegen den Uhrzeigersinn, also $r(i) = i + 1$, und
- s die Spiegelung an der Achse durch die Ecke 1 und den Ursprung, also $s(i) = 2 - i$ (jeweils modulo n).

Für Symmetrien schreiben wir $sr := s \circ r$. Das ist das Hintereinanderausführen: *erst* r, *dann* s.

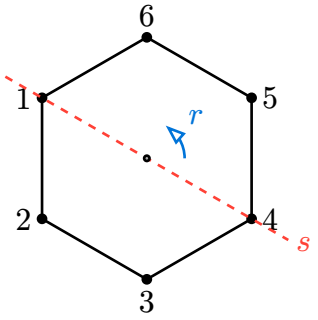


Abbildung 2: Die Erzeuger r und s von D_{12}, also für $n = 6$.

Proposition 1.2.5: In D_{2n} gelten:

1. $1, r, r^2, \ldots, r^{n-1}$ sind paarweise verschieden und $r^n = 1$, d.h. $|r| = n$.
2. $|s| = 2$.
3. $s \neq r^i$ für alle i.
4. $sr^i \neq sr^j$ für $0 \leq i < j \leq n - 1$.
5. $rs = sr^{-1}$.
6. $r^i s = sr^{-i}$ für alle $i \in \mathbb{Z}$.

Beweis.

1. Das ist klar für die Drehung eines n-Ecks: r^i bildet 1 auf $1 + i$ ab, und diese Ecken sind für $i = 0, \ldots, n - 1$ verschieden.
2. Eine Spiegelung zweimal ausgeführt ist die Identität, und $s \neq 1$.
3. Eine Spiegelung kehrt die Reihenfolge der Ecken (den Umlaufsinn) um, eine Drehung nicht.
4. Aus $sr^i = sr^j$ folgt durch Multiplikation von links mit s^{-1}, dass $r^i = r^j$ ist, im Widerspruch zu 1.
5. Wir prüfen die Wirkung beider Seiten auf die Kante 1–2, was nach Lemma 1.2.3 genügt. Es ist $rs(1) = r(1) = 2$ und $rs(2) = r(n) = 1$, sowie $sr^{-1}(1) = s(n) = 2$ und $sr^{-1}(2) = s(1) = 1$.
6. Für $i = 0$ ist nichts zu zeigen. Für $i \geq 0$ folgt die Aussage per Induktion aus 5.:

$$r^{i+1}s = r\big(r^i s\big) = rsr^{-i} = sr^{-1}r^{-i} = sr^{-(i+1)}.$$

thomas.kahle@ovgu.de

Für negative i multipliziert man $r^{-i}s = sr^i$ von links mit r^i und von rechts mit r^{-i}.■

Aus 3. folgt auch $sr^i \neq r^j$ für alle i, j, denn sonst wäre $s = r^{j-i}$. Zusammen mit 1. und 4. haben wir damit $2n$ verschiedene Elemente gefunden, und wegen $|D_{2n}| = 2n$ sind das alle:

$$D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}.$$

Insbesondere ist D_{2n} nicht abelsch, denn nach 5. ist $rs = sr^{-1}$, und $sr^{-1} \neq sr$, weil $r^{-1} \neq r$ für $n \geq 3$ gilt.

Was ist nun ein Produkt wie $r^i s$, bei dem s rechts von r steht? Mit den Regeln 5. und 6. kann jedes Produkt in D_{2n} *sortiert* werden: Man schiebt alle s nach links und vereinfacht mit $s^2 = 1$ und $r^n = 1$. So findet man immer eine Darstellung der Form r^i oder sr^i mit $0 \leq i \leq n-1$.

Beispiel 1.2.6: Sei $n = 12$. Dann ist

$$(sr^9)(sr^6) = s(r^9 s)r^6 = ssr^{-9}r^6 = r^{-3} = r^9.$$

Erzeuger und Relationen

Was ist eine abstrakte Beschreibung einer Gruppe? Für D_{2n} haben wir

- *Erzeuger* r und s angegeben, sodass jedes Element der Gruppe als Produkt der Erzeuger geschrieben werden kann, und
- *Relationen* $r^n = 1$, $s^2 = 1$ und $rs = sr^{-1}$, die angeben, welche dieser Produkte gleich sind.

Achtung! Wir haben nicht alle Gleichungen angegeben, die in D_{2n} gelten (es sind unendlich viele). Aber die angegebenen Relationen reichen aus, um alle gültigen Relationen daraus abzuleiten, denn mit ihnen kann man jedes Produkt in die Normalform r^i bzw. sr^i bringen. Damit kann in D_{2n} effizient gerechnet werden.

Definition 1.2.7: Sei G eine Gruppe und $S \subseteq G$. Man sagt, S *erzeugt* G, und schreibt $G = \langle S \rangle$, wenn sich jedes Element von G als Produkt von Elementen aus S und deren Inversen schreiben lässt. Sind $R_1, ..., R_m$ Relationen zwischen den Erzeugern, sodass jede in G gültige Relation zwischen den Erzeugern daraus abgeleitet werden kann, so schreibt man

$$G = \langle S \mid R_1, ..., R_m \rangle.$$

Dies heißt eine *Präsentation* von G. Ist S endlich (und m endlich), so nennt man dies eine *endliche Präsentation* der Gruppe.

© 2026 Thomas Kahle

Relationen sind Gleichungen zwischen „Wörtern“ in den Buchstaben aus S, zum Beispiel $s_1s_2s_3 = s_4$ für $s_1, s_2, s_3, s_4 \in S$. Man kann alles nach links bringen und erhält $s_1s_2s_3s_4^{-1} = 1$. Rechts steht dann die Identität, und oft lässt man „$= 1$“ einfach weg: $\langle s_1, ..., s_4 \mid s_1s_2s_3s_4^{-1}\rangle$ bedeutet $\langle s_1, ..., s_4 \mid s_1s_2s_3 = s_4\rangle$. Wir haben also

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle.$$

Die hier gegebene Definition ist nicht ganz präzise, denn wir haben nicht gesagt, was „ableiten“ genau bedeutet und warum es zu gegebenen Erzeugern und Relationen überhaupt eine Gruppe gibt. Eine präzise Konstruktion benutzt freie Gruppen, die wir hier nicht behandeln. Für das Rechnen mit Präsentationen reicht die obige Vorstellung.

Frage 1.2.8: Warum ist $\langle S \mid R_1, ..., R_m\rangle$ überhaupt eine Gruppe?

Präsentationen sind sehr nützlich, um in Gruppen zu rechnen. Aber nicht alle Eigenschaften von Gruppen sind offensichtlich, wenn man eine Präsentation hat, zum Beispiel:

- Wie groß ist die Gruppe? Die Anzahl der Elemente $|G|$ einer Gruppe G heißt die *Ordnung* der Gruppe.
- Ist die Gruppe endlich?
- Sind zwei gegebene Elemente (Wörter in den Erzeugern) gleich?

Beispiel 1.2.9: Sei

$$G = \langle x, y \mid x^2 = y^2 = (xy)^2 = 1\rangle.$$

Wegen $x^2 = y^2 = 1$ ist $(yx)(xy) = yx^2y = y^2 = 1$, also $yx = (xy)^{-1}$. Andererseits ist $(xy)^2 = (xy)(xy) = 1$, d.h. xy ist selbst das Inverse von xy. Da Inverse eindeutig sind, folgt $yx = xy$. Insbesondere ist G abelsch, und jedes Element lässt sich sortieren und mit $x^2 = y^2 = 1$ vereinfachen. Damit ist

$$G = \{1, x, y, xy\}$$

und G hat höchstens 4 Elemente. Dass die vier Elemente verschieden sind, folgt aus den Relationen allein nicht. Man sieht es an einem Modell: Die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mit $x = (\overline{1}, \overline{0})$ und $y = (\overline{0}, \overline{1})$ erfüllt die Relationen und hat vier Elemente. Dass daraus $|G| = 4$ folgt, begründen wir mit Satz 1.4.7 in Abschnitt 1.4. Die Gruppe G heißt *Kleinsche Vierergruppe*.

Beispiel 1.2.10: Sei

$$G = \langle x, y \mid x^3 = y^3 = (xy)^3 = 1 \rangle.$$

Wir behaupten, dass diese Gruppe unendlich ist. Eine Idee ist, unendlich viele verschiedene Elemente anzugeben:

$$x, \quad xy, \quad xyx, \quad xyxx, \quad xyxxy, \quad xyxxyx, \quad xyxxyxx, \quad \ldots$$

Diese Elemente scheinen alle verschieden, da zur Anwendung einer Relation x^3, y^3 oder $xyxyxy$ gefunden werden müsste. Das ist allerdings noch kein Beweis, denn man könnte auch Relationen einfügen und dann an anderer Stelle kürzen.

Einen Beweis liefert wieder ein Modell. Sei ABC ein gleichseitiges Dreieck in der Ebene, und seien x und y die Drehungen um 120° um die Ecken A und B (bei geeigneter Orientierung). Dann ist xy eine Drehung um 240° um die dritte Ecke C, und es gilt $x^3 = y^3 = (xy)^3 = 1$. Die Abbildung xy^{-1} ist eine Drehung um $120° - 120° = 0°$, also eine Verschiebung, und zwar keine triviale, da $x \neq y$ ist. Eine nichttriviale Verschiebung hat unendliche Ordnung. Die von x und y erzeugte Gruppe von Bewegungen der Ebene ist also unendlich. Mit Satz 1.4.7 folgt daraus, dass auch G unendlich ist.

Beispiel 1.2.11: Sei $n \geq 1$ und

$$X_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, xy = yx^2 \rangle.$$

Das sieht so ähnlich aus wie D_{2n}, dort hatten wir $rs = sr^{-1}$. Analog zu D_{2n} gibt es hier einen Sortieralgorithmus: Die Relation $xy = yx^2$ erlaubt es, ein y nach links zu bewegen, wenn man dabei das x durch x^2 ersetzt. Also lässt sich jedes Element von X_{2n} schreiben als

$$y^k x^l \quad \text{mit } k \in \{0, 1\} \text{ und } 0 \leq l \leq n - 1.$$

Gilt also $|X_{2n}| = 2n$? Nein! Es gibt eine „versteckte“ Relation:

$$x = xy^2 = (xy)y = yx^2y = yx(xy) = yxyx^2 = y(xy)x^2 = yyx^2x^2 = y^2x^4 = x^4.$$

Also gilt in X_{2n} die Gleichung $x^4 = x$, d.h. $x^3 = 1$. In der Darstellung $y^k x^l$ gilt also sogar $0 \leq l \leq 2$, und damit ist $|X_{2n}| \leq 6$. Ist n nicht durch 3 teilbar, so folgt aus $x^3 = 1$ und $x^n = 1$ sogar $x = 1$ (denn $1 = 3a + nb$ für geeignete $a, b \in \mathbb{Z}$), und dann ist $|X_{2n}| \leq 2$.

Übung. Zeigen Sie, dass für $3 \mid n$ die Elemente $r, s \in D_6$ die Relationen von X_{2n} erfüllen, wenn man $x = r$ und $y = s$ setzt. Was vermuten Sie über $|X_{2n}|$?

© 2026 Thomas Kahle

1.3 Die symmetrische Gruppe

Die Symmetrieoperationen des n-Ecks aus dem letzten Abschnitt permutieren die Ecken. Nimmt man *alle* Permutationen einer Menge, so erhält man die wohl wichtigste Klasse von Gruppen überhaupt.

Definition 1.3.1: Sei Ω eine Menge. Die Menge S_Ω aller Bijektionen $\Omega \to \Omega$ bildet mit der Komposition $\circ$ von Abbildungen eine Gruppe, die *symmetrische Gruppe* auf Ω. Ihre Elemente heißen *Permutationen* von Ω. Für $\Omega = \{1, ..., n\}$ schreibt man S_n.

Dass S_Ω eine Gruppe ist, prüft man leicht nach: Die Komposition von Bijektionen ist wieder eine Bijektion, die Komposition von Abbildungen ist assoziativ, die Identität id_Ω ist das neutrale Element, und das Inverse von σ ist die Umkehrabbildung σ^{-1}.

Die Bedeutung der symmetrischen Gruppen liegt unter anderem darin, dass jede Gruppe G als Gruppe von Permutationen aufgefasst werden kann, nämlich als Teil von S_G. Ist G endlich mit n Elementen, so steckt G also in diesem Sinne in S_n. Wir werden das bei den Gruppenwirkungen präzisieren (Satz 1.5.8).

Proposition 1.3.2: Es gilt $|S_n| = n!$.

Beweis. Um eine Bijektion $\sigma: \{1, ..., n\} \to \{1, ..., n\}$ festzulegen, wählt man zunächst ein Bild $\sigma(1)$, wofür es n Möglichkeiten gibt. Das Bild $\sigma(2)$ muss von $\sigma(1)$ verschieden sein, also gibt es dafür noch $n-1$ Möglichkeiten, usw. Insgesamt erhält man $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ Möglichkeiten. ∎

Zykelschreibweise

Permutationen notiert man meistens nicht als Wertetabelle, sondern in der kompakteren Zykelschreibweise.

Definition 1.3.3: Seien $a_1, ..., a_m \in \{1, ..., n\}$ paarweise verschieden. Der *Zykel* $(a_1 a_2 ... a_m) \in S_n$ ist die Permutation

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto ... \mapsto a_m \mapsto a_1,$$

die alle Elemente von $\{1, ..., n\} \setminus \{a_1, ..., a_m\}$ fest lässt. Zwei Zykel $(a_1 ... a_m)$ und $(b_1 ... b_l)$ heißen *disjunkt*, falls $\{a_1, ..., a_m\} \cap \{b_1, ..., b_l\} = \varnothing$.

thomas.kahle@ovgu.de

Beispiel 1.3.4: In S_4 bezeichnet (123) die Abbildung

$$1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 1, \quad 4 \mapsto 4.$$

Definition 1.3.5: Die *Länge* eines Zykels ist die Anzahl der Elemente darin. Ein *t-Zykel* ist ein Zykel der Länge t. Eine *Transposition* ist ein 2-Zykel.

Ein 1-Zykel (a) ist die Identität. Wir vereinbaren daher, dass 1-Zykel ab sofort weggelassen werden, und bezeichnen die Identität in S_n mit 1. Ein Vorteil der Zykelschreibweise ist, dass sie nicht von n abhängt: (12) bedeutet $1 \mapsto 2$, $2 \mapsto 1$, egal in welcher S_n (mit $n \geq 2$) wir uns befinden.

Für das Produkt in S_n verwenden wir die Komposition von Abbildungen, $\sigma\tau := \sigma \circ \tau$. Produkte werden also **von rechts nach links** ausgewertet: Bei $\sigma\tau$ wird zuerst τ und dann σ angewendet.

Eine beliebige Permutation $\sigma \in S_n$ ist ein Produkt disjunkter Zykel. Diese werden einfach nebeneinander geschrieben:

$$\sigma = \big(a_1 ... a_{m_1}\big)\big(a_{m_1+1} ... a_{m_2}\big) \cdots \big(a_{m_{k-1}+1} ... a_{m_k}\big).$$

Elemente, die σ fest lässt, kommen darin nicht vor (dann ist $m_k < n$). Jedes $i \in \{1, ..., n\}$ kommt höchstens einmal vor und wird auf seinen rechten Nachbarn abgebildet, oder auf das erste Element seines Zykels, falls i am Ende eines Zykels steht.

Beispiel 1.3.6: In S_5 ist $(132)(45)$ die Permutation

$$1 \mapsto 3, \quad 2 \mapsto 1, \quad 3 \mapsto 2, \quad 4 \mapsto 5, \quad 5 \mapsto 4.$$

Achtung! Manchmal schreibt man Permutationen in S_n in *zweizeiliger Notation*, bei der unter jedem i sein Bild steht. Die Permutation aus dem letzten Beispiel ist

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

Dann kommt man auf die Idee, die erste Zeile wegzulassen, und schreibt (31254). **Aber das ist kein Zykel!** Als Zykel gelesen wäre (31254) die Permutation $3 \mapsto 1 \mapsto 2 \mapsto 5 \mapsto 4 \mapsto 3$, also eine ganz andere.

Der folgende einfache Algorithmus übersetzt eine Abbildungsvorschrift in eine Zerlegung in disjunkte Zykel. Sei $\sigma \in S_n$ durch die Werte $\sigma(1), ..., \sigma(n)$ gegeben.

© 2026 Thomas Kahle

1. Finde das kleinste $a \in \{1, ..., n\}$, das noch in keinem Zykel vorkommt (am Anfang ist das $a = 1$). Beginne einen neuen Zykel mit „$(a$“.
2. Sei b das zuletzt geschriebene Element. Bestimme $c = \sigma(b)$. Falls $c = a$ ist, schließe den Zykel mit „$)$“ und gehe zu Schritt 1. Andernfalls schreibe c und wiederhole Schritt 2.
3. Der Prozess endet, wenn alle Zahlen von 1 bis n in einem Zykel vorkommen. Entferne zum Schluss alle 1-Zykel aus dem Ergebnis.

Beispiel 1.3.7: Wir wenden den Algorithmus auf die Permutation mit den Werten $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$, $\sigma(4) = 5$, $\sigma(5) = 4$ an. Wir beginnen mit $(1$, finden $\sigma(1) = 3, \sigma(3) = 2$ und $\sigma(2) = 1$ und schließen den Zykel (132). Das kleinste noch nicht benutzte Element ist 4, und wegen $\sigma(4) = 5, \sigma(5) = 4$ erhalten wir (45). Also ist $\sigma = (132)(45)$, wie oben.

Proposition 1.3.8: Jede Permutation $\sigma \in S_n$ ist ein Produkt disjunkter Zykel. Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Zykel, das zyklische Verschieben innerhalb der Zykel und das Weglassen von 1-Zykeln.

Beweis. Wir müssen begründen, dass der Algorithmus korrekt ist. Beginnt ein Zykel mit a, so schreibt der Algorithmus die Elemente $a, \sigma(a), \sigma^2(a), ...$ Da $\{1, ..., n\}$ endlich ist, gibt es $0 \leq i < j$ mit $\sigma^i(a) = \sigma^j(a)$. Wählt man j minimal, so ist $i = 0$, denn sonst wäre wegen der Injektivität von σ auch $\sigma^{i-1}(a) = \sigma^{j-1}(a)$. Die Folge kehrt also zu a zurück, bevor sich ein anderes Element wiederholt, d.h. der Zykel $(a\, \sigma(a) ... \sigma^{j-1}(a))$ besteht aus paarweise verschiedenen Elementen und wird geschlossen. Die Elemente eines solchen Zykels C kommen in späteren Zykeln nicht mehr vor: σ bildet C bijektiv auf sich ab. Läge $\sigma^k(a')$ für ein später gewähltes $a' \notin C$ in C, so wäre auch $a' = \sigma^{-k}\big(\sigma^k(a')\big) \in C$. Das Produkt der erhaltenen disjunkten Zykel bildet jedes i auf $\sigma(i)$ ab und ist daher gleich σ.

Zur Eindeutigkeit: In jeder Zerlegung in disjunkte Zykel muss der Zykel, der ein gegebenes i enthält, bis auf zyklisches Verschieben gleich $(i\, \sigma(i)\, \sigma^2(i) ...)$ sein, denn i wird auf seinen rechten Nachbarn abgebildet. ■

Beispiel 1.3.9: Die symmetrische Gruppe S_3 hat $3! = 6$ Elemente, nämlich

$$S_3 = \{1, (12), (23), (13), (123), (132)\}.$$

Rechnen in Zykelschreibweise

Die Zykelschreibweise ist nicht eindeutig: Zykel können zyklisch verschoben werden,

$$(a_1 a_2 ... a_m) = (a_2 a_3 ... a_m a_1) = (a_3 a_4 ... a_m a_1 a_2) = ...$$

So ist zum Beispiel $(132) = (321)$. Dafür sind manche Berechnungen in Zykelschreibweise besonders einfach:

- Rückwärtslesen gibt das Inverse: $(a_1 ... a_m)^{-1} = (a_m ... a_1)$.
- Falls Zykel disjunkt sind, spielt die Reihenfolge keine Rolle:

  $$(a_1 ... a_m)(b_1 ... b_l) = (b_1 ... b_l)(a_1 ... a_m), \quad \text{falls } \{a_1, ..., a_m\} \cap \{b_1, ..., b_l\} = \varnothing.$$

  Achtung! Für nicht disjunkte Zykel ist das im Allgemeinen falsch.
- Ist $\sigma = z_1 z_2 z_3$ ein Produkt von Zykeln, so ist nach Proposition 1.1.9 $\sigma^{-1} = z_3^{-1} z_2^{-1} z_1^{-1}$.

Allgemeine Produkte rechnet man von rechts nach links aus. Seien σ und τ in Zykeldarstellung mit jeweils disjunkten Zykeln gegeben,

$$\sigma = (z_1) \cdots (z_k), \quad \tau = (z_1') \cdots (z_{k'}').$$

Dann ist

$$\sigma\tau = \sigma \circ \tau = (z_1) \cdots (z_k)(z_1') \cdots (z_{k'}')$$

ein Produkt von Zykeln, die im Allgemeinen nicht disjunkt sind. Eine disjunkte Zykeldarstellung erhält man mit dem Algorithmus von oben. Dabei verfolgt man die Elemente von $\{1, ..., n\}$ von rechts durch die Zykel.

Beispiel 1.3.10: Wir berechnen $(123)(23)$ in S_3. Das Element 1 wird von (23) fest gelassen und von (123) auf 2 abgebildet. Die 2 geht unter (23) auf 3 und dann unter (123) auf 1. Die 3 geht auf 2 und dann wieder auf 3. Der Algorithmus liefert also $(12)(3)$, und nach Streichen des 1-Zykels

$$(123)(23) = (12).$$

Genauso rechnet man

$$(23)(123) = (13).$$

Insbesondere ist $(123)(23) \neq (23)(123)$, d.h. S_3 ist nicht abelsch. Zur Kontrolle berechnen wir noch das Inverse auf zwei Arten:

$$((123)(23))^{-1} = (23)^{-1}(123)^{-1} = (32)(321) = (12) = (12)^{-1}.$$

Übung. Zeigen Sie, dass S_n für $n \geq 3$ nicht abelsch ist.

1.4 Homomorphismen

Das Wort *homomorph* (griechisch für „gleichgestaltig“) bezeichnet in der Algebra Abbildungen zwischen den Mengen, die algebraischen Objekten zugrunde liegen, und die dabei die Struktur erhalten. Eine Gruppe ist eine Menge mit einer Verknüpfung, also ist ein Homomorphismus von Gruppen eine Abbildung, die die Verknüpfung respektiert.

© 2026 Thomas Kahle

Definition 1.4.1: Seien $(G, *)$ und $(H, \circ)$ Gruppen. Eine Abbildung $\varphi: G \to H$ ist ein *Homomorphismus*, falls für alle $x, y \in G$ gilt:

$$\varphi(x * y) = \varphi(x) \circ \varphi(y).$$

Ein Homomorphismus heißt *Isomorphismus*, falls er bijektiv ist.

Üblicherweise wird in beiden Gruppen die Verknüpfung durch Nebeneinanderschreiben ausgedrückt. Dann lautet die Bedingung

$$\varphi(xy) = \varphi(x)\varphi(y) \quad \text{für alle } x, y \in G.$$

Man beachte, dass hier zwei verschiedene, unsichtbare Verknüpfungen auftreten: links die von G, rechts die von H.

Lemma 1.4.2: Sei $\varphi: G \to H$ ein Homomorphismus von Gruppen. Dann gilt:

1. $\varphi(1) = 1$, d.h. φ bildet das neutrale Element von G auf das neutrale Element von H ab.
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$ für alle $x \in G$.
3. $\varphi(x^n) = \varphi(x)^n$ für alle $x \in G$ und $n \in \mathbb{Z}$.
4. Ist $\psi: H \to K$ ein weiterer Homomorphismus, so ist auch $\psi \circ \varphi: G \to K$ ein Homomorphismus.
5. Ist φ ein Isomorphismus, so ist auch die Umkehrabbildung $\varphi^{-1}: H \to G$ ein Isomorphismus.

Beweis.

1. Es gilt $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$. Das ist eine Gleichung in H. Multipliziert man sie von links mit $\varphi(1)^{-1}$, so erhält man $1 = \varphi(1)$.
2. Nach 1. ist $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1$. Nach Proposition 1.1.11 ist also $\varphi(x^{-1})$ das Inverse von $\varphi(x)$.
3. Für $n > 0$ folgt das per Induktion aus der Homomorphismuseigenschaft, für $n = 0$ ist es 1. und für $n < 0$ folgt es mit 2.
4. $(\psi \circ \varphi)(xy) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y))$.
5. Seien $u, v \in H$ und $x = \varphi^{-1}(u)$, $y = \varphi^{-1}(v)$. Dann ist $\varphi(xy) = \varphi(x)\varphi(y) = uv$, also $\varphi^{-1}(uv) = xy = \varphi^{-1}(u)\varphi^{-1}(v)$.

■

Definition 1.4.3: Existiert ein Isomorphismus $\varphi: G \to H$, so heißen G und H *isomorph*, und man schreibt $G \cong H$.

thomas.kahle@ovgu.de

Für viele Sachverhalte sind isomorphe Gruppen „die gleiche Gruppe“: Jede Eigenschaft, die nur von der Gruppenstruktur abhängt, gilt für G genau dann, wenn sie für H gilt, zum Beispiel, ob die Gruppe abelsch ist. Die Gruppentheorie studiert daher die *Isomorphieklassen* von Gruppen. Nach Lemma 1.4.2 ist Isomorphie eine Äquivalenzrelation: Die Identität ist ein Isomorphismus, Umkehrabbildungen von Isomorphismen sind Isomorphismen, und Kompositionen von Isomorphismen sind Isomorphismen.

Beispiel 1.4.4: Die Exponentialfunktion

$$\exp\colon (\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot), \quad x \mapsto e^x$$

ist ein Isomorphismus. Sie ist bijektiv mit der Umkehrabbildung ln, wie in der Analysis gezeigt wird. Die Homomorphismuseigenschaft $\varphi(xy) = \varphi(x)\varphi(y)$ lautet hier

$$\exp(x+y) = \exp(x)\cdot\exp(y), \quad \text{bzw.} \quad e^{x+y} = e^x \cdot e^y,$$

was ebenfalls aus der Analysis bekannt ist. Also ist $(\mathbb{R},+) \cong (\mathbb{R}_{>0},\cdot)$.

Wir haben in Abschnitt 1.3 die Gruppe S_Ω einer Menge Ω kennengelernt, die Gruppe aller Bijektionen $\Omega \to \Omega$ mit der Komposition als Verknüpfung. Es kommt dabei nur auf die Anzahl der Elemente von Ω an.

Proposition 1.4.5: Seien Δ und Ω Mengen mit $|\Delta| = |\Omega|$. Dann gilt $S_\Delta \cong S_\Omega$.

Beweis. Wegen $|\Delta| = |\Omega|$ gibt es eine Bijektion $\theta\colon \Delta \to \Omega$. Zu jedem $\sigma \in S_\Delta$ brauchen wir ein $\varphi(\sigma) \in S_\Omega$, sodass $\varphi(\sigma\circ\tau) = \varphi(\sigma)\circ\varphi(\tau)$ für alle $\sigma,\tau \in S_\Delta$ gilt. Die Idee ist, σ mit Hilfe von θ nach Ω zu „transportieren“, sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} \Delta & \xrightarrow{\theta} & \Omega \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\varphi(\sigma)} \\ \Delta & \xrightarrow[\theta]{} & \Omega \end{array}$$

Wir setzen also

$$\varphi(\sigma) := \theta\circ\sigma\circ\theta^{-1}.$$

Als Komposition von Bijektionen ist $\varphi(\sigma)$ eine Bijektion $\Omega \to \Omega$, also $\varphi(\sigma) \in S_\Omega$. Die Abbildung φ ist ein Homomorphismus, denn durch Einschieben von $\theta^{-1}\circ\theta = \mathrm{id}_\Delta$ erhält man

$$\varphi(\sigma\circ\tau) = \theta\circ\sigma\circ\tau\circ\theta^{-1} = (\theta\circ\sigma\circ\theta^{-1})\circ(\theta\circ\tau\circ\theta^{-1}) = \varphi(\sigma)\circ\varphi(\tau).$$

© 2026 Thomas Kahle

Schließlich ist φ bijektiv, denn die Abbildung $S_\Omega \to S_\Delta, \rho \mapsto \theta^{-1} \circ \rho \circ \theta$ ist eine Umkehrabbildung von φ. ■

Die Umkehrung gilt auch: Aus $S_\Delta \cong S_\Omega$ folgt $|\Delta| = |\Omega|$. Für endliche, nichtleere Mengen sieht man das so: Isomorphe Gruppen haben gleich viele Elemente, also ist $|\Delta|! = |S_\Delta| = |S_\Omega| = |\Omega|!$, und da die Fakultät auf den positiven ganzen Zahlen injektiv ist, folgt $|\Delta| = |\Omega|$. Die Voraussetzung „nichtleer“ ist nötig: Wegen $0! = 1! = 1$ sind $S_\varnothing$ und $S_{\{1\}}$ beide die triviale Gruppe. Für unendliche Mengen ist die Umkehrung ebenfalls richtig, aber deutlich schwieriger zu beweisen.

Wir werden im Verlauf der Vorlesung sehr viele Isomorphismen sehen, die manchmal nur implizit auftreten. Isomorphismen sind das zentrale Thema bei der Suche nach *Klassifikationen*, d.h. nach Sätzen, die Objekte bis auf Isomorphie eindeutig festlegen. Ein Beispiel ist die folgende Aussage, die wir beim Satz von Lagrange und seinen Folgerungen beweisen werden (Korollar 1.12.16): Jede Gruppe mit 6 Elementen ist entweder isomorph zu $(\mathbb{Z}/6\mathbb{Z}, +)$ oder zu S_3. Insbesondere ist jede nicht-abelsche Gruppe der Ordnung 6 isomorph zu S_3, denn $\mathbb{Z}/6\mathbb{Z}$ ist abelsch.

Umgekehrt beobachtet man oft, dass zwei Gruppen *nicht* isomorph sind, weil sie sich in einer Eigenschaft unterscheiden, die unter Isomorphismen erhalten bleibt.

Übung. Sei $\varphi: G \to H$ ein Isomorphismus. Zeigen Sie:
- $|G| = |H|$.
- G ist genau dann abelsch, wenn H abelsch ist.
- Für alle $x \in G$ gilt $|x| = |\varphi(x)|$.

Beispiel 1.4.6:
- S_3 und $\mathbb{Z}/6\mathbb{Z}$ sind nicht isomorph, denn $\mathbb{Z}/6\mathbb{Z}$ ist abelsch und S_3 nicht.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ und $(\mathbb{R}, +)$ sind nicht isomorph: In $(\mathbb{R} \setminus \{0\}, \cdot)$ hat -1 die Ordnung 2. In $(\mathbb{R}, +)$ gibt es dagegen kein Element der Ordnung 2, denn aus $x + x = 0$ folgt $x = 0$.

Homomorphismen und Präsentationen

Ist eine Gruppe durch Erzeuger und Relationen gegeben, also $G = \langle s_1, ..., s_k \mid R_1, ..., R_l \rangle$ wie bei der Diedergruppe (siehe Definition 1.2.7), so lassen sich Homomorphismen auf G besonders einfach angeben.

Satz 1.4.7: Sei G eine Gruppe, die durch eine endliche Präsentation mit Erzeugern $s_1, ..., s_k$ gegeben ist. Sei H eine Gruppe und seien $t_1, ..., t_k \in H$ beliebig. Angenommen, die t_i erfüllen jede Relation zwischen den s_i, d.h. jede Relation aus G gilt in H, wenn man formal s_i durch t_i ersetzt ($i = 1, ..., k$). Dann gilt:

1. Es existiert ein eindeutiger Homomorphismus $\varphi: G \to H$ mit $\varphi(s_i) = t_i$ für $i = 1, \ldots, k$.
2. Wird H von den t_i erzeugt, so ist φ surjektiv.
3. Ist zusätzlich $|G| = |H| < \infty$, so ist φ ein Isomorphismus.

Beweis (Idee). Ein vollständiger Beweis erfordert eine präzise Definition von Präsentationen (über sogenannte freie Gruppen), die wir hier nicht geben. Die Idee ist aber einfach.

1. Ist $g \in G$ beliebig, so lässt sich g als Produkt $g = s_{i_1}^{\pm 1} \cdots s_{i_m}^{\pm 1}$ der Erzeuger und ihrer Inversen schreiben. Ist φ ein Homomorphismus mit $\varphi(s_i) = t_i$, so ist nach Lemma 1.4.2
$$\varphi(g) = t_{i_1}^{\pm 1} \cdots t_{i_m}^{\pm 1}$$
festgelegt. Das zeigt die Eindeutigkeit, und wir nehmen diese Gleichung als Definition von φ. Gilt in G aber $g = g'$ für zwei verschiedene „Wörter“ in den s_i, so hat man zwei Festlegungen für $\varphi(g) = \varphi(g')$. Die beiden Wörter gehen durch Anwendung der Relationen auseinander hervor. Da alle Relationen zwischen den s_i auch zwischen den t_i gelten, liefern beide Festlegungen dasselbe Element von H, d.h. φ ist wohldefiniert. Nach Konstruktion ist φ ein Homomorphismus.
2. Wird H von den t_i erzeugt, so ist jedes $h \in H$ ein Produkt $t_{i_1}^{\pm 1} \cdots t_{i_m}^{\pm 1}$, und das entsprechende Wort in den s_i ist ein Urbild von h.
3. Eine surjektive Abbildung zwischen endlichen Mengen gleicher Kardinalität ist auch injektiv, also bijektiv. Damit ist φ ein Isomorphismus und $G \cong H$.

■

Das ist ganz analog zur linearen Algebra: Dort zeigt man, dass eine lineare Abbildung $V \to W$ durch die Bilder einer Basis eindeutig festgelegt ist und dass man diese Bilder frei vorgeben darf. Bei Gruppen dürfen die Bilder der Erzeuger nicht frei gewählt werden, sie müssen die Relationen erfüllen.

Beispiel 1.4.8: Wir betrachten die Diedergruppe aus Abschnitt 1.2
$$D_6 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^{-1}s \rangle$$
und die Permutationsgruppe S_3 und wollen einen Homomorphismus $D_6 \to S_3$ konstruieren. Seien $a = (123)$ und $b = (12)$. Dann gilt $a^3 = 1$ und $b^2 = 1$. Außerdem ist $ba = a^{-1}b$, denn
$$ba = (12)(123) = (23) \quad \text{und} \quad a^{-1}b = (321)(12) = (23).$$
Also erfüllen a und b alle Relationen von r und s, und nach Satz 1.4.7 gibt es einen eindeutigen Homomorphismus

$$\varphi\colon D_6 \to S_3 \quad \text{mit} \quad \varphi(r) = a, \quad \varphi(s) = b.$$

Dieser ist surjektiv, denn sein Bild enthält

$$1, \quad a = (123), \quad a^2 = (132), \quad b = (12), \quad ab = (13), \quad a^2b = (23),$$

also alle sechs Elemente von S_3. Da $|D_6| = 6 = |S_3|$ ist, folgt $D_6 \cong S_3$.

1.5 Gruppenwirkungen

Eine wichtige Idee der Mathematik ist es, Objekte durch ihre Symmetrien zu verstehen. Das funktioniert auch für Gruppen selbst: Man kann versuchen, eine Gruppe zu verstehen, indem man beobachtet, wie sie als Symmetrien auf verschiedenen Objekten *wirken* kann. Diese Idee wird in der *Darstellungstheorie* systematisch verfolgt. Die Diedergruppe aus Abschnitt 1.2 ist ein erstes Beispiel: Sie wirkt auf den Ecken des n -Ecks.

Definition 1.5.1: Sei G eine Gruppe und A eine Menge. Eine *Wirkung* von G auf A ist eine Abbildung

$$G \times A \to A, \quad (g, a) \mapsto g \cdot a,$$

sodass gilt:
1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ für alle $g_1, g_2 \in G$ und alle $a \in A$.
2. $1 \cdot a = a$ für alle $a \in A$.

Man sagt dann auch, G *wirkt* oder *operiert* auf A.

Man beachte, dass in der ersten Bedingung links zweimal die Wirkung benutzt wird, rechts dagegen erst die Verknüpfung $g_1 g_2$ in G und dann einmal die Wirkung. Manchmal schreibt man auch ga statt $g \cdot a$, wenn klar ist, was gemeint ist. Probleme können auftreten, wenn $A = G$ ist, denn dann kann ga auch das Produkt in G bezeichnen (siehe die Konjugation weiter unten).

Zu einer Wirkung und einem festen $g \in G$ definieren wir die Abbildung

$$\sigma_g\colon A \to A, \quad \sigma_g(a) := g \cdot a.$$

Proposition 1.5.2: Sei eine Wirkung von G auf A gegeben.
1. Für jedes $g \in G$ ist σ_g bijektiv, also $\sigma_g \in S_A$.
2. Die Abbildung $\varphi\colon G \to S_A$, $g \mapsto \sigma_g$ ist ein Gruppenhomomorphismus.

Beweis.

1. Wir zeigen, dass $\sigma_{g^{-1}}$ eine Umkehrabbildung von σ_g ist. Für $a \in A$ gilt mit beiden Axiomen der Wirkung

$$\big(\sigma_g \circ \sigma_{g^{-1}}\big)(a) = g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = 1 \cdot a = a,$$

   also $\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id}_A$. Analog ist $\sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_A$. Also ist σ_g bijektiv.

2. Zu zeigen ist $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ für alle $g_1, g_2 \in G$. Beide Seiten sind bijektive Abbildungen $A \to A$, und die Verknüpfung in S_A ist die Komposition. Wir prüfen also, wie beide Seiten auf ein beliebiges $a \in A$ wirken:

$$\begin{aligned}\varphi(g_1g_2)(a) = \sigma_{g_1g_2}(a) &= (g_1g_2) \cdot a = g_1 \cdot (g_2 \cdot a)\\ &= g_1 \cdot \sigma_{g_2}(a) = \sigma_{g_1}\big(\sigma_{g_2}(a)\big)\\ &= \big(\sigma_{g_1} \circ \sigma_{g_2}\big)(a) = (\varphi(g_1)\varphi(g_2))(a).\end{aligned}$$

   Da a beliebig war, folgt $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$.

■

Die Abbildung φ heißt manchmal die *Permutationsdarstellung* von G zu der Wirkung. Merke: Eine Gruppenwirkung von G auf A ordnet jedem Gruppenelement eine Permutation von A zu, und zwar so, dass die Verknüpfung in G dem Hintereinanderausführen von Permutationen entspricht („auf homomorphe Weise“).

Umgekehrt liefert jeder Homomorphismus $\varphi\colon G \to S_A$ eine Wirkung von G auf A durch $g \cdot a := \varphi(g)(a)$: Die erste Bedingung ist genau die Homomorphismuseigenschaft, und die zweite folgt aus $\varphi(1) = \mathrm{id}_A$ (Lemma 1.4.2). Wirkungen von G auf A und Homomorphismen $G \to S_A$ sind also zwei Beschreibungen derselben Sache.

Definition 1.5.3: Eine Wirkung von G auf A heißt *treu*, falls die Permutationsdarstellung $\varphi\colon G \to S_A$ injektiv ist, d.h. falls verschiedene Elemente von G auch verschieden auf A wirken.

Eine Wirkung ist genau dann treu, wenn $g = 1$ das einzige Element ist, das als Identität auf A wirkt, d.h. wenn aus $\sigma_g = \mathrm{id}_A$ schon $g = 1$ folgt. Ist nämlich die Wirkung treu, so folgt aus $\sigma_g = \mathrm{id}_A = \sigma_1$, dass $g = 1$ ist. Ist umgekehrt 1 das einzige solche Element und gilt $\sigma_g = \sigma_h$, so ist $\sigma_{h^{-1}g} = \sigma_{h^{-1}} \circ \sigma_g = \sigma_{h^{-1}} \circ \sigma_h = \sigma_1 = \mathrm{id}_A$, also $h^{-1}g = 1$ und damit $g = h$.

Das andere Extrem ist die *triviale Wirkung* $g \cdot a = a$ für alle $g \in G$ und $a \in A$. Ihre Permutationsdarstellung ist der konstante Homomorphismus $\varphi\colon G \to S_A$, $g \mapsto \mathrm{id}_A$.

Beispiel 1.5.4: Ist V ein Vektorraum über einem Körper K, so wirkt die multiplikative Gruppe $K^* = K \setminus \{0\}$ auf V durch Skalarmultiplikation $\lambda \cdot v := \lambda v$. Die

beiden Bedingungen $\lambda(\mu v) = (\lambda\mu)v$ und $1v = v$ sind Vektorraumaxiome. Für $V \neq \{0\}$ ist die Wirkung treu, denn aus $\lambda v = v$ für ein $v \neq 0$ folgt $\lambda = 1$.

Beispiel 1.5.5: Für jede Menge A wirkt S_A auf A durch $\sigma \cdot a := \sigma(a)$. Die Permutationsdarstellung ist die Identität $S_A \to S_A$, $\sigma \mapsto \sigma$, und die Wirkung ist offensichtlich treu.

Beispiel 1.5.6: Die Diedergruppe D_{2n} wirkt auf der Menge $\{1, \ldots, n\}$ der Ecken des n-Ecks. Diese Wirkung ist treu, denn eine Symmetrie, die alle Ecken festhält, ist die Identität (Lemma 1.2.3). Für $n = 3$ ist die Permutationsdarstellung $D_6 \to S_3$ sogar ein Isomorphismus, vergleiche Beispiel 1.4.8. Das bedeutet, dass jede Umordnung der Ecken eines gleichseitigen Dreiecks durch eine Symmetrie realisiert wird. Schon für das Quadrat gilt das nicht: Bei der Wirkung von D_8 bleiben die Ecken 1 und 2 stets benachbart. Die Transposition $(23) \in S_4$ bildet aber die benachbarten Ecken 1 und 2 auf die nicht benachbarten Ecken 1 und 3 ab. Das sieht man auch an $|D_8| = 8 < 24 = |S_4|$.

Beispiel 1.5.7: Sei G eine Gruppe und $A = G$. Die Abbildung

$$G \times G \to G, \quad (g, a) \mapsto ga$$

(*Linksmultiplikation*) ist eine Wirkung: Die erste Bedingung ist das Assoziativgesetz in G, die zweite die Eigenschaft des neutralen Elements. Sie heißt die *reguläre Linkswirkung* von G auf sich selbst. Sie ist treu, denn aus $ga = a$ für alle a folgt mit $a = 1$ schon $g = 1$.

Aus der regulären Wirkung erhalten wir sofort ein berühmtes Ergebnis, das wir in Abschnitt 1.3 angekündigt haben.

Satz 1.5.8 (Satz von Cayley): Jede Gruppe G ist isomorph zu einer Gruppe von Permutationen der Menge G. Genauer ist die Permutationsdarstellung $\varphi: G \to S_G$ der regulären Wirkung ein injektiver Homomorphismus, und G ist isomorph zu ihrem Bild $\varphi(G) \subseteq S_G$. Ist G endlich mit n Elementen, so ist G damit isomorph zu einer Gruppe von Permutationen in S_n.

Beweis. Nach Proposition 1.5.2 und Beispiel 1.5.7 ist φ ein injektiver Homomorphismus. Das Bild $\varphi(G)$ ist mit der Komposition selbst eine Gruppe: Mit $\varphi(g)$ und $\varphi(h)$ liegen auch $\varphi(g) \circ \varphi(h) = \varphi(gh)$ und $\varphi(g)^{-1} = \varphi(g^{-1})$ in $\varphi(G)$, und $\mathrm{id}_G = \varphi(1) \in \varphi(G)$. Als Abbildung $G \to \varphi(G)$ ist φ also ein bijektiver Homomorphismus, d.h. ein Isomorphismus. Für $|G| = n$ ist $S_G \cong S_n$ nach Proposition 1.4.5, und das Bild von $\varphi(G)$ unter einem solchen Isomorphismus ist eine zu G isomorphe Gruppe von Permutationen in S_n. ■

Im Sinne des Satzes von Cayley ist also jede endliche Gruppe „in einer symmetrischen Gruppe enthalten“. Sobald wir Untergruppen kennen, werden wir das so formulieren: G ist isomorph zu einer Untergruppe von S_n (siehe Abschnitt 1.6).

Für die nächste wichtige Wirkung von G auf sich selbst benötigen wir noch einen Begriff.

Definition 1.5.9: Ein Isomorphismus $G \to G$ einer Gruppe auf sich selbst heißt *Automorphismus* von G. Die Menge aller Automorphismen von G wird mit $\mathrm{Aut}(G)$ bezeichnet.

Nach Lemma 1.4.2 sind Kompositionen und Umkehrabbildungen von Automorphismen wieder Automorphismen, und id_G ist ein Automorphismus. Also ist $\mathrm{Aut}(G)$ mit der Komposition eine Gruppe, und jedes Element von $\mathrm{Aut}(G)$ ist insbesondere eine Permutation von G.

Beispiel 1.5.10: Jede Gruppe G wirkt auf sich selbst durch *Konjugation*:

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1}.$$

Das ist eine Wirkung, denn für $g, h, x \in G$ gilt

$$g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} \quad \text{und} \quad 1x1^{-1} = x,$$

wobei wir $(gh)^{-1} = h^{-1}g^{-1}$ aus Proposition 1.1.9 benutzt haben.

Achtung! Hier wäre es verboten, die Wirkung mit „gx“ zu bezeichnen, denn gx ist schon das Produkt von g und x in G, und das ist im Allgemeinen etwas anderes als gxg^{-1}.

Die Permutationen $\sigma_g : x \mapsto gxg^{-1}$ sind sogar Automorphismen von G, denn

$$\sigma_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \sigma_g(x)\sigma_g(y).$$

Die Permutationsdarstellung der Konjugation ist also ein Homomorphismus $G \to \mathrm{Aut}(G)$, $g \mapsto \sigma_g$. Diese Wirkung ist im Allgemeinen nicht treu: Ist G abelsch, so ist $gxg^{-1} = x$ für alle $g, x \in G$, und die Konjugation ist die triviale Wirkung.

© 2026 Thomas Kahle

1.6 Untergruppen

Untergruppen sind eine wichtige „innere“ Struktur von Gruppen: Teilmengen, die mit der eingeschränkten Verknüpfung selbst wieder Gruppen sind. Eine weitere wichtige Konstruktion sind Quotientengruppen, zu denen wir später kommen (siehe Abschnitt 1.11).

Definition 1.6.1: Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ ist eine *Untergruppe* von G, falls sie nicht leer ist und abgeschlossen unter Produkten und Inversenbildung ist, d.h. falls für alle $h_1, h_2 \in H$ gilt:

$$h_1 h_2 \in H \quad \text{und} \quad h_1^{-1} \in H.$$

Wir schreiben dann $H \leq G$.

Äquivalent ist $H \leq G$ genau dann, wenn H mit der von G induzierten Verknüpfung selbst eine Gruppe ist. Wichtig ist dabei, dass die Verknüpfung eine Abbildung $H \times H \to H$ ist, dass also Produkte von Elementen aus H nicht aus H herausfallen. Assoziativität erbt H von G, und das neutrale Element liegt in H, denn mit einem $h \in H$ liegen auch h^{-1} und $hh^{-1} = 1$ in H.

Manchmal schreibt man auch $H < G$ für eine Untergruppe. Andere Autor*innen meinen damit aber $H \leq G$ und $H \neq G$. Wir vermeiden diese Schreibweise.

Beispiel 1.6.2:
- Jede Gruppe G hat die *trivialen* Untergruppen $\{1\}$ und G.
- Die Diedergruppe D_{2n} hat die Untergruppe $H = \{1, r, ..., r^{n-1}\}$ der Rotationen.
- Die geraden Zahlen $2\mathbb{Z}$ bilden eine Untergruppe von $(\mathbb{Z}, +)$.
- Aus $H \leq K$ und $K \leq G$ folgt $H \leq G$.

Definition 1.6.3: Sei $\varphi: G \to H$ ein Homomorphismus von Gruppen. Der *Kern* von φ ist

$$\ker \varphi = \{g \in G : \varphi(g) = 1\}.$$

Dabei ist 1 das neutrale Element von H.

thomas.kahle@ovgu.de

Proposition 1.6.4: Der Kern eines Homomorphismus $\varphi: G \to H$ ist eine Untergruppe von G.

Beweis. Nach Lemma 1.4.2 ist $\varphi(1) = 1$, also $1 \in \ker\varphi$ und der Kern ist nicht leer. Sind $g, h \in \ker\varphi$, so ist $\varphi(gh) = \varphi(g)\varphi(h) = 1 \cdot 1 = 1$ und, wieder nach Lemma 1.4.2, $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$. Also liegen gh und g^{-1} im Kern. ∎

Übung. Zeigen Sie, dass ein Homomorphismus φ genau dann injektiv ist, wenn $\ker\varphi = \{1\}$ gilt.

Nicht jede Gruppe, die irgendwie „in" einer anderen steckt, ist eine Untergruppe. Zum Beispiel ist D_6 keine Untergruppe von D_8, denn D_6 ist nicht einmal eine Teilmenge von D_8: Die Symmetrien eines Dreiecks sind keine Symmetrien eines Quadrats. Andererseits möchte man S_m für $m \leq n$ als Untergruppe von S_n auffassen, indem man eine Permutation von $\{1, ..., m\}$ auf $\{1, ..., n\}$ fortsetzt, sodass sie $m+1, ..., n$ festlässt. Sauber formulieren lässt sich das nur mit einem injektiven Homomorphismus $S_m \to S_n$, dessen Bild dann eine Untergruppe von S_n ist (siehe die Übung unten). Ein solcher injektiver Homomorphismus ist nicht eindeutig: Man könnte S_m genauso gut auf m beliebigen anderen Elementen von $\{1, ..., n\}$ wirken lassen.

Übung. Sei $\varphi: G \to H$ ein Homomorphismus. Zeigen Sie, dass das Bild $\operatorname{im}\varphi = \varphi(G)$ eine Untergruppe von H ist.

Um nachzuweisen, dass eine Teilmenge eine Untergruppe ist, benutzt man meist das folgende Kriterium, das nur eine Bedingung statt zwei verlangt.

Proposition 1.6.5: (*Untergruppenkriterium*) Sei $H \subseteq G$ eine Teilmenge einer Gruppe G. Dann ist H genau dann eine Untergruppe von G, wenn
1. $H \neq \varnothing$ und
2. für alle $x, y \in H$ gilt: $xy^{-1} \in H$.

Ist H endlich, so genügt es, statt 2. die Bedingung

2′. für alle $x, y \in H$ gilt: $xy \in H$

zu prüfen.

Beweis. Ist H eine Untergruppe, so ist H nicht leer, und für $x, y \in H$ liegen y^{-1} und damit auch xy^{-1} in H.

Seien umgekehrt 1. und 2. erfüllt. Da H nicht leer ist, gibt es ein $x \in H$. Mit $y = x$ folgt aus 2., dass $xx^{-1} = 1 \in H$ ist. Wendet man 2. auf 1 und x an, folgt $1 \cdot x^{-1} = x^{-1} \in H$. Also ist H abgeschlossen unter Inversenbildung. Seien nun $x, y \in H$. Dann ist $y^{-1} \in H$, und 2. liefert $x(y^{-1})^{-1} = xy \in H$. Also ist H auch abgeschlossen unter Produkten.

© 2026 Thomas Kahle

Sei nun H endlich und nicht leer, und es gelte 2′. Dann ist H abgeschlossen unter Produkten, und es bleibt die Abgeschlossenheit unter Inversenbildung zu zeigen. Sei dazu $x \in H$ beliebig. Wegen 2′ liegen alle Potenzen $x, x^2, x^3, \ldots$ in H. Da H endlich ist, gibt es $1 \leq a < b$ mit $x^a = x^b$. In G folgt durch Multiplikation mit x^{-a}, dass $x^{b-a} = 1$ ist, und damit

$$x^{-1} = x^{-1}x^{b-a} = x^{b-a-1}.$$

Ist $b - a - 1 \geq 1$, so ist das eine Potenz von x mit positivem Exponenten und liegt in H. Ist $b - a - 1 = 0$, so ist $x^{-1} = x^0 = 1$, also $x = 1$ und $x^{-1} = x \in H$. In jedem Fall ist $x^{-1} \in H$. ∎

Für unendliche Teilmengen reicht die Bedingung 2′ nicht: Die natürlichen Zahlen $\mathbb{N} \subseteq \mathbb{Z}$ sind nicht leer und abgeschlossen unter Addition, aber keine Untergruppe von $(\mathbb{Z}, +)$, denn $-1 \notin \mathbb{N}$.

1.7 Spezielle Untergruppen

In diesem Abschnitt lernen wir einige Untergruppen kennen, die sich in jeder Gruppe in natürlicher Weise definieren lassen. Sei dazu G eine Gruppe und $A \subseteq G$ eine beliebige Teilmenge.

Definition 1.7.1: Der *Zentralisator* von A in G ist

$$C_G(A) = \{g \in G \colon gag^{-1} = a \text{ für alle } a \in A\},$$

die Menge aller $g \in G$, die mit jedem $a \in A$ vertauschen.

Die Formulierung „vertauschen“ ist gerechtfertigt, denn es gilt

$$gag^{-1} = a \quad \Leftrightarrow \quad ga = ag \quad \Leftrightarrow \quad g^{-1}ag = a.$$

Für Teilmengen $A \subseteq B \subseteq G$ gilt

$$C_G(G) \subseteq C_G(B) \subseteq C_G(A),$$

denn ein Element, das mit allen Elementen von B vertauscht, vertauscht insbesondere mit allen Elementen von A.

Proposition 1.7.2: Für jede Teilmenge $A \subseteq G$ ist $C_G(A)$ eine Untergruppe von G.

Beweis. Wir benutzen das Untergruppenkriterium Proposition 1.6.5. Es ist $1 \in C_G(A)$, also ist $C_G(A)$ nicht leer. Seien $x, y \in C_G(A)$ und $a \in A$ beliebig. Wegen $y \in C_G(A)$ ist $y^{-1}ay = a$, und damit

$$(xy^{-1})a(xy^{-1})^{-1} = x(y^{-1}ay)x^{-1} = xax^{-1} = a.$$

thomas.kahle@ovgu.de

Also ist $xy^{-1} \in C_G(A)$. ∎

Beispiel 1.7.3: In einer abelschen Gruppe G ist $C_G(A) = G$ für alle Teilmengen $A \subseteq G$.

Definition 1.7.4: Das *Zentrum* von G ist

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

Das Zentrum besteht also aus den Elementen, die mit allen anderen vertauschen. Nach Proposition 1.7.2 ist es eine Untergruppe, und G ist genau dann abelsch, wenn $Z(G) = G$ ist.

Beispiel 1.7.5: Sei K ein Körper und

$$G = \mathrm{GL}_n(K) = \{A \in K^{n\times n} \colon \det(A) \neq 0\}$$

die Gruppe der invertierbaren $n \times n$-Matrizen mit der Matrixmultiplikation. Dann ist

$$Z(G) = \{\lambda E_n \colon \lambda \in K^*\},$$

wobei E_n die Einheitsmatrix bezeichnet. Die Skalarmatrizen vertauschen offensichtlich mit allen Matrizen; dass es keine weiteren Elemente im Zentrum gibt, ist eine Übung.

Übung. Zeigen Sie die fehlende Inklusion in Beispiel 1.7.5. Tipp: Eine Matrix im Zentrum vertauscht insbesondere mit den Matrizen $E_n + E_{ij}$, wobei E_{ij} die Matrix mit einer 1 an der Stelle (i, j) und sonst Nullen ist.

Für eine Teilmenge $A \subseteq G$ und $g \in G$ schreiben wir

$$gAg^{-1} = \{gag^{-1} \colon a \in A\}$$

und analog $gA = \{ga \colon a \in A\}$ und $Ag = \{ag \colon a \in A\}$.

Definition 1.7.6: Der *Normalisator* von $A \subseteq G$ ist

$$N_G(A) = \{g \in G \colon gAg^{-1} = A\}.$$

© 2026 Thomas Kahle

Achtung! Die Bedingung $gAg^{-1} = A$ bedeutet nicht, dass $gag^{-1} = a$ für alle $a \in A$ gilt, sondern die Gleichheit der *Mengen*. Das Element gag^{-1} muss also nur wieder in A liegen, aber nicht gleich a sein.

- Es gilt $gAg^{-1} = A$ genau dann, wenn $gA = Ag$ ist.
- $N_G(A)$ ist für jede Teilmenge A eine Untergruppe von G. Das kann man direkt mit dem Untergruppenkriterium nachrechnen. Wir geben unten einen anderen Beweis.
- Es gilt $C_G(A) \leq N_G(A)$, denn aus $gag^{-1} = a$ für alle $a \in A$ folgt $gAg^{-1} = A$.

Beispiel 1.7.7: Sei

$$G = D_8 = \langle r, s \mid r^4 = 1, s^2 = 1, rs = sr^{-1} \rangle$$

die Diedergruppe des Quadrats. Die Relation $rs = sr^{-1}$ ist äquivalent zu $sr = r^{-1}s$, und nach Proposition 1.2.5 gilt allgemeiner $sr^i s^{-1} = r^{-i}$ für alle $i \in \mathbb{Z}$. Sei $A = \{1, r, r^2, r^3\}$ die Untergruppe der Rotationen. Wir bestimmen Zentralisator und Normalisator von A sowie das Zentrum von D_8.

Zentralisator. Da A abelsch ist, gilt $A \subseteq C_{D_8}(A)$. Es ist $s \notin C_{D_8}(A)$, denn $sr = r^{-1}s = r^3 s \neq rs$. Auch $sr^i \notin C_{D_8}(A)$ für $i = 0, ..., 3$: Wäre $sr^i \in C_{D_8}(A)$, so wäre, da $C_{D_8}(A)$ eine Untergruppe ist und $r^{-i} \in A$ enthält, auch $sr^i r^{-i} = s \in C_{D_8}(A)$, ein Widerspruch. Da $D_8 = A \cup \{s, sr, sr^2, sr^3\}$ ist, folgt

$$C_{D_8}(A) = A.$$

Normalisator. Es gilt $N_{D_8}(A) \supseteq C_{D_8}(A) = A$. Weiter ist

$$sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A,$$

also $s \in N_{D_8}(A)$. Da $N_{D_8}(A)$ eine Untergruppe ist, die die Erzeuger r und s enthält, enthält sie alle Produkte von ihnen, und es folgt

$$N_{D_8}(A) = D_8.$$

Zentrum. Wegen $A \subseteq D_8$ ist $Z(D_8) = C_{D_8}(D_8) \subseteq C_{D_8}(A) = A$. Die Elemente r und r^3 liegen nicht im Zentrum, denn

$$sr = r^{-1}s = r^3 s \neq rs \quad \text{und} \quad sr^3 = r^{-3}s = rs \neq r^3 s.$$

Die Konjugation mit s vertauscht also r und r^3: $srs^{-1} = r^3$ und $sr^3s^{-1} = r$. Dagegen vertauscht r^2 mit beiden Erzeugern, denn $sr^2 = r^{-2}s = r^2 s$. Der Zentralisator $C_{D_8}(\{r^2\})$ ist also eine Untergruppe, die r und s enthält, und damit ganz D_8. Somit ist $r^2 \in Z(D_8)$, und insgesamt

$$Z(D_8) = \{1, r^2\}.$$

thomas.kahle@ovgu.de

Wie man an diesem Beispiel sieht, ist es bei Rechnungen sehr nützlich zu wissen, dass $C_G(A)$, $N_G(A)$ und $Z(G)$ Untergruppen sind: Man muss dann nur für Erzeuger nachprüfen, ob sie dazugehören.

Die drei gerade gesehenen Konstruktionen sind Spezialfälle von allgemeinen Konstruktionen für Wirkungen. Sei dazu G eine Gruppe, die auf einer Menge A wirkt, und $\varphi\colon G \to S_A$ der zugehörige Homomorphismus (siehe Abschnitt 1.5).

Definition 1.7.8: Sei G eine Gruppe, die auf einer Menge A wirkt, und $\varphi\colon G \to S_A$ der zugehörige Homomorphismus.

- Sei $a \in A$. Der *Stabilisator* von a ist
$$G_a = \{g \in G\colon ga = a\}.$$
- Der *Kern der Wirkung* ist der Kern von φ, d.h.
$$\ker\varphi = \{g \in G\colon ga = a \text{ für alle } a \in A\}.$$

Proposition 1.7.9: Der Kern einer Wirkung und die Stabilisatoren G_a, $a \in A$, sind Untergruppen von G.

Beweis. Der Kern ist als Kern eines Homomorphismus nach Proposition 1.6.4 eine Untergruppe. Für den Stabilisator benutzen wir das Untergruppenkriterium. Es ist $1a = a$, also $1 \in G_a$. Seien $x, y \in G_a$. Aus $ya = a$ folgt durch Anwenden von y^{-1}
$$y^{-1}a = y^{-1}(ya) = (y^{-1}y)a = 1a = a,$$
d.h. $y^{-1} \in G_a$. (Anders gesagt: y^{-1} wirkt durch die Umkehrabbildung der Abbildung, durch die y wirkt.) Damit ist
$$(xy^{-1})a = x(y^{-1}a) = xa = a,$$
also $xy^{-1} \in G_a$. ∎

Normalisator, Zentralisator und Zentrum sind Untergruppen, weil sie Spezialfälle dieser Konstruktionen sind:

- Sei $\mathcal{S} = 2^G$ die Potenzmenge von G. Die Gruppe G wirkt auf $\mathcal{S}$ durch Konjugation:
$$G \times \mathcal{S} \to \mathcal{S}, \quad (g, A) \mapsto gAg^{-1}.$$
Der Normalisator $N_G(A)$ ist genau der Stabilisator von $A \in \mathcal{S}$ unter dieser Wirkung, denn beide sind die Menge $\{g \in G\colon gAg^{-1} = A\}$.
- Nach Definition wirkt $N_G(A)$ auf A durch Konjugation:
$$N_G(A) \times A \to A, \quad (g, a) \mapsto gag^{-1}.$$

© 2026 Thomas Kahle

Der Zentralisator $C_G(A)$ ist offensichtlich der Kern dieser Wirkung und damit eine Untergruppe von $N_G(A)$, also per Transitivität auch von G.
- Das Zentrum $Z(G)$ ist der Kern der Wirkung von G auf sich selbst durch Konjugation,

$$G \times G \to G, \quad (g, a) \mapsto gag^{-1}.$$

Übung. Prüfen Sie nach, dass die Konjugation $(g, A) \mapsto gAg^{-1}$ tatsächlich eine Wirkung von G auf der Potenzmenge 2^G ist, und dass $N_G(A)$ durch Konjugation auf A wirkt.

1.8 Zyklische Gruppen

Die einfachsten Untergruppen einer Gruppe entstehen aus einem einzigen Element. Sei G eine Gruppe und $x \in G$. Dann ist

$$\langle x \rangle := \{x^n : n \in \mathbb{Z}\} = \{1, x^{\pm 1}, x^{\pm 2}, \ldots\}$$

eine Untergruppe von G, denn sie enthält $1 = x^0$, und für $x^a, x^b \in \langle x \rangle$ ist nach den Potenzgesetzen $x^a \left(x^b\right)^{-1} = x^{a-b} \in \langle x \rangle$ (siehe Abschnitt 1.6).

Definition 1.8.1: Eine Gruppe G heißt *zyklisch*, falls sie von einem Element $x \in G$ erzeugt wird, d.h. falls

$$G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}.$$

In diesem Fall heißt x ein *Erzeuger* von G.

Ein paar Bemerkungen zur Definition:
- Es wird nichts über Relationen gesagt, also zum Beispiel darüber, ob $x^n = 1$ für manche n gilt. In der Notation für Präsentationen aus Definition 1.2.7 wäre $G = \langle x \mid R \rangle$ für gewisse Relationen R.
- Erzeuger sind nicht eindeutig: Ist x ein Erzeuger von G, so auch x^{-1}, denn $x^n = \left(x^{-1}\right)^{-n}$.
- Zyklische Gruppen sind abelsch, denn $x^a x^b = x^{a+b} = x^b x^a$.

Beispiel 1.8.2:
1. In D_{2n} haben wir zum Beispiel die zyklischen Untergruppen

$$\langle r \rangle = \{1, r, \ldots, r^{n-1}\}, \quad \langle s \rangle = \{1, s\}, \quad \langle sr \rangle = \{1, sr\},$$

   letzteres, da $(sr)^2 = s(rs)r = s(sr^{-1})r = 1$ nach Proposition 1.2.5 gilt. Allgemein erzeugt jedes Element einer Gruppe eine zyklische Untergruppe. Die Diedergruppe selbst ist für $n \geq 3$ nicht zyklisch, da sie nicht abelsch ist.
2. $(\mathbb{Z}, +)$ ist unendlich und zyklisch:

$$\mathbb{Z} = \langle 1 \rangle = \{0, \pm 1, \pm 2, ...\}.$$

In additiver Schreibweise sind die „Potenzen“ von 1 die Vielfachen $n \cdot 1 = n$; man vergleiche mit $1, x^{\pm 1}, x^{\pm 2}, ...$ in multiplikativer Schreibweise. Hier sind alle Vielfachen des Erzeugers verschieden.

3. $(\mathbb{Z}/n\mathbb{Z}, +)$ ist zyklisch mit Erzeuger $\overline{1}$, denn $\overline{a} = a \cdot \overline{1}$.

Übung. Zeigen Sie: Eine Gruppe G ist genau dann zyklisch, wenn es einen surjektiven Homomorphismus $(\mathbb{Z}, +) \to G$ gibt.

Der folgende Satz klassifiziert alle zyklischen Gruppen.

Satz 1.8.3: Sei $G = \langle x \rangle$ zyklisch. Dann gilt

$$G \cong \begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) & \text{falls } G \text{ endlich ist mit } |G| = n \\ (\mathbb{Z}, +) & \text{falls } G \text{ unendlich ist.} \end{cases}$$

Genauer ist im endlichen Fall $|x| = |G| = n$ und $G = \{1, x, ..., x^{n-1}\}$, und im unendlichen Fall ist $|x| = \infty$ und die Potenzen x^k, $k \in \mathbb{Z}$, sind paarweise verschieden.

Beweis. Sei zunächst G endlich. Da $G = \{x^k : k \in \mathbb{Z}\}$ endlich ist, existieren $a, b \in \mathbb{Z}$ mit $a > b$ und $x^a = x^b$. Dann ist $x^{a-b} = 1$, also ist die Ordnung $n := |x| \leq a - b$ endlich. Die Elemente $1, x, ..., x^{n-1}$ sind paarweise verschieden: Aus $x^i = x^j$ mit $0 \leq i < j \leq n - 1$ würde $x^{j-i} = 1$ mit $0 < j - i < n$ folgen, im Widerspruch zur Minimalität von n. Also ist $|G| \geq n$.

Sei nun $x^t \in G$ beliebig. Division mit Rest liefert $t = qn + k$ mit $k \in \{0, ..., n - 1\}$, also

$$x^t = (x^n)^q x^k = x^k \in \{1, x, ..., x^{n-1}\}.$$

Damit ist $|G| \leq n$, also $G = \{1, x, ..., x^{n-1}\}$ und $|G| = n$. Ein Isomorphismus ist

$$\mathbb{Z}/n\mathbb{Z} \to G, \quad \overline{k} \mapsto x^k.$$

Diese Abbildung ist wohldefiniert, denn aus $\overline{k} = \overline{l}$ folgt $k - l = mn$ für ein $m \in \mathbb{Z}$ und damit $x^k = x^l (x^n)^m = x^l$. Sie ist ein Homomorphismus, da $\overline{k} + \overline{l} = \overline{k + l} \mapsto x^{k+l} = x^k x^l$, sie ist surjektiv nach dem eben Gezeigten, und als surjektive Abbildung zwischen zwei Mengen mit n Elementen ist sie bijektiv.

Sei nun G unendlich. Nach dem ersten Teil kann $|x|$ nicht endlich sein, denn sonst hätte G höchstens $|x|$ Elemente. Also ist $|x| = \infty$, und die Potenzen x^k sind paarweise verschieden, denn aus $x^a = x^b$ mit $a > b$ folgte $x^{a-b} = 1$. Daher ist

$$\mathbb{Z} \to G, \quad k \mapsto x^k$$

© 2026 Thomas Kahle

injektiv. Sie ist ein Homomorphismus wegen $x^{k+l} = x^k x^l$ und surjektiv, da $G = \langle x \rangle$ ist. Also ist sie ein Isomorphismus. ■

Wendet man den Satz auf die zyklische Untergruppe $\langle x \rangle$ eines beliebigen Elements x einer Gruppe an, erhält man die in Definition 1.1.12 angekündigte Interpretation der Ordnung eines Elements.

Korollar 1.8.4: Sei G eine Gruppe und $x \in G$. Dann ist $|x| = |\langle x \rangle|$.

Klassifikationen sind toll! Der Satz besagt insbesondere, dass je zwei zyklische Gruppen gleicher Ordnung isomorph sind. Man bezeichnet daher oft mit $\mathbb{Z}_n$ die (Isomorphieklasse der) zyklische(n) Gruppe der Ordnung n.

Es folgen ein paar nützliche Fakten in diesem Zusammenhang.

Proposition 1.8.5: Sei G eine Gruppe, $x \in G$ und $m, n \in \mathbb{Z}$.
1. Gilt $x^n = 1$ und $x^m = 1$, so ist auch $x^{\mathrm{ggT}(m,n)} = 1$.
2. Gilt $x^m = 1$ für ein $m \neq 0$, so ist $|x|$ endlich und $|x|$ teilt m.

Beweis.
1. Nach dem Lemma von Bézout gibt es $a, b \in \mathbb{Z}$ mit $d := \mathrm{ggT}(m, n) = am + bn$. Damit ist
$$x^d = (x^m)^a (x^n)^b = 1.$$
2. Sei $x^m = 1$ mit $m \neq 0$. Dann ist auch $x^{|m|} = 1$ mit $|m| > 0$, also ist $n := |x|$ endlich und $n \leq |m|$. Sei $d = \mathrm{ggT}(m, n)$. Nach 1. ist $x^d = 1$, und es gilt $1 \leq d \leq n$. Da n minimal mit $x^n = 1$ und $n > 0$ ist, folgt $d = n$. Wegen $d \mid m$ folgt $n \mid m$.

■

Umgekehrt folgt aus $|x| = n < \infty$ und $n \mid m$ natürlich $x^m = (x^n)^{m/n} = 1$.

Proposition 1.8.6: Sei G eine Gruppe, $x \in G$ und $a \in \mathbb{Z} \setminus \{0\}$.
1. Ist $|x| = \infty$, so ist $|x^a| = \infty$.
2. Ist $|x| = n < \infty$, so ist $|x^a| = \frac{n}{\mathrm{ggT}(a,n)}$.
3. Ist $|x| = n < \infty$ und $a > 0$ ein Teiler von n, so ist $|x^a| = \frac{n}{a}$.

Beweis.
1. Angenommen, $|x^a| = m < \infty$. Dann ist $x^{am} = (x^a)^m = 1$ mit $am \neq 0$, nach Proposition 1.8.5 also $|x| < \infty$, ein Widerspruch.
2. Sei $y = x^a$ und $d = \mathrm{ggT}(a, n)$. Wir schreiben $n = db$ und $a = dc$ mit $b > 0$ und $\mathrm{ggT}(b, c) = 1$. Zu zeigen ist $|y| = b$. Es gilt

$$y^b = x^{ab} = x^{dcb} = (x^n)^c = 1,$$

nach Proposition 1.8.5 ist also $k := |y|$ ein Teiler von b. Andererseits ist $x^{ak} = y^k = 1$, also $n \mid ak$, d.h. $db \mid dck$ und damit $b \mid ck$. Da b und c teilerfremd sind, folgt $b \mid k$. Da b und k positiv sind und sich gegenseitig teilen, ist $k = b = \frac{n}{\mathrm{ggT}(a,n)}$.

3. Das ist der Spezialfall von 2. mit $\mathrm{ggT}(a, n) = a$.

■

Damit kann man alle Erzeuger einer zyklischen Gruppe $G = \langle x \rangle$ bestimmen. Nach Korollar 1.8.4 ist $\langle x^a \rangle = G$ genau dann, wenn $|x^a| = |G|$ gilt (im endlichen Fall, da $\langle x^a \rangle \subseteq G$ ist).

- Ist $|x| = \infty$, so gilt $G = \langle x^a \rangle$ genau dann, wenn $a = \pm 1$ ist. Ist nämlich $G = \langle x^a \rangle$, so ist $x = (x^a)^k$ für ein $k \in \mathbb{Z}$, also $x^{ak-1} = 1$. Da $|x| = \infty$ ist, folgt $ak = 1$, also $a = \pm 1$.
- Ist $|x| = n < \infty$, so gilt $G = \langle x^a \rangle$ genau dann, wenn $\mathrm{ggT}(a, n) = 1$ ist. Für $a \neq 0$ folgt das aus Proposition 1.8.6, und $x^0 = 1$ erzeugt G nur für $n = 1 = \mathrm{ggT}(0, 1)$.

Zum Beispiel sind die Erzeuger von $\mathbb{Z}/8\mathbb{Z}$ genau $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

Der nächste Satz beschreibt alle Untergruppen einer zyklischen Gruppe.

Satz 1.8.7: Sei $G = \langle x \rangle$ zyklisch.

1. Jede Untergruppe $H \leq G$ ist zyklisch. Genauer ist $H = \{1\}$ oder $H = \langle x^d \rangle$, wobei d die kleinste positive ganze Zahl mit $x^d \in H$ ist.
2. Ist $|G| = \infty$, so gilt $\langle x^a \rangle \neq \langle x^b \rangle$ für $a \neq b$ in $\mathbb{N}_0$, aber $\langle x^m \rangle = \langle x^{-m} \rangle$ für alle $m \in \mathbb{Z}$. Die Untergruppen von G stehen also in Bijektion mit $\mathbb{N}_0$ via $a \mapsto \langle x^a \rangle$.
3. Ist $|G| = n < \infty$, so gibt es für jeden positiven Teiler a von n genau eine Untergruppe der Ordnung a, nämlich $\langle x^{n/a} \rangle$. Außerdem gilt $\langle x^m \rangle = \langle x^{\mathrm{ggT}(m,n)} \rangle$ für alle $m \in \mathbb{Z}$. Die Untergruppen von G stehen also in Bijektion mit den positiven Teilern von n.

Beweis.

1. Ist $H = \{1\}$, so ist nichts zu zeigen. Sei also $H \neq \{1\}$. Dann gibt es ein $a \neq 0$ mit $x^a \in H$, und mit x^a ist auch $x^{-a} \in H$. Also ist die Menge

$$P = \{a \in \mathbb{N} \colon a > 0, x^a \in H\}$$

nicht leer. Nach der Wohlordnung der natürlichen Zahlen hat P ein kleinstes Element d. Da H eine Untergruppe ist, ist $\langle x^d \rangle \leq H$. Wir zeigen Gleichheit. Sei $x^a \in H$ beliebig. Wir schreiben $a = qd + r$ mit $r \in \{0, \ldots, d-1\}$. Dann ist

$$x^r = x^a (x^d)^{-q} \in H,$$

da beide Faktoren in H liegen. Da d minimal mit $d > 0$ und $x^d \in H$ ist, folgt $r = 0$. Also ist $a = qd$ und $x^a \in \langle x^d \rangle$. Damit ist $H = \langle x^d \rangle$. Wir halten fest, was wir dabei gezeigt haben: **Ist $x^a \in H$, so ist a ein Vielfaches von d.**

© 2026 Thomas Kahle

2. Für $m \in \mathbb{Z}$ ist $\langle x^m \rangle = \langle x^{-m} \rangle$, da $x^{-m} = (x^m)^{-1}$ ist und eine Untergruppe mit jedem Element auch dessen Inverses enthält. Seien nun $a, b \in \mathbb{N}_0$. Ist $a = 0$, so ist $\langle x^a \rangle = \{1\}$, während für $b > 0$ die Untergruppe $\langle x^b \rangle$ das Element $x^b \neq 1$ enthält. Sind $a, b > 0$, so sind die Elemente von $\langle x^a \rangle$ die Potenzen x^{ak}, $k \in \mathbb{Z}$, und da nach Satz 1.8.3 alle Potenzen von x verschieden sind, ist a die kleinste positive Zahl e mit $x^e \in \langle x^a \rangle$. Also ist a durch die Untergruppe $\langle x^a \rangle$ eindeutig bestimmt. Die Abbildung $a \mapsto \langle x^a \rangle$ ist also injektiv, und nach 1. ist sie surjektiv, denn $\{1\} = \langle x^0 \rangle$.
3. Nach Satz 1.8.3 ist $|x| = n$. Sei $a > 0$ ein Teiler von n. Nach Proposition 1.8.6 ist $\left|x^{n/a}\right| = n/(n/a) = a$, also hat $\langle x^{n/a} \rangle$ nach Korollar 1.8.4 die Ordnung a. Sei umgekehrt H eine Untergruppe der Ordnung a. Ist $H = \{1\}$, so ist $a = 1$ und $H = \langle x^n \rangle$. Andernfalls ist $H = \langle x^d \rangle$ wie in 1. Wegen $x^n = 1 \in H$ ist n ein Vielfaches von d, also ist $\left|x^d\right| = n/d$ nach Proposition 1.8.6. Aus $a = |H| = n/d$ folgt $d = n/a$, also $H = \langle x^{n/a} \rangle$. Dieses Argument zeigt auch, dass die Ordnung jeder Untergruppe ein Teiler von n ist. Für die zweite Aussage sei $m \in \mathbb{Z}$ und $g = \mathrm{ggT}(m, n)$. Für $m \neq 0$ haben $\langle x^m \rangle$ und $\langle x^g \rangle$ nach Proposition 1.8.6 beide die Ordnung n/g, wegen $g \mid n$ ist dies ein Teiler von n, und nach der Eindeutigkeit sind die beiden Untergruppen gleich. Für $m = 0$ ist $g = n$ und $\langle x^0 \rangle = \{1\} = \langle x^n \rangle$.

■

Beispiel 1.8.8: Die Untergruppen von $\mathbb{Z}/12\mathbb{Z}$ entsprechen den Teilern $1, 2, 3, 4, 6, 12$ von 12. Zum Beispiel ist die Untergruppe der Ordnung 4 gleich $\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, und es ist $\langle \overline{9} \rangle = \langle \overline{\mathrm{ggT}(9, 12)} \rangle = \langle \overline{3} \rangle$.

1.9 Erzeugte Untergruppen

Wir verallgemeinern nun die von einem Element erzeugte (zyklische) Untergruppe $\langle x \rangle$ auf mehrere Elemente.

Definition 1.9.1: Sei $A \subseteq G$ eine beliebige Teilmenge einer Gruppe G. Die *von A erzeugte Untergruppe* ist

$$\langle A \rangle := \bigcap_{\substack{H \leq G \\ A \subseteq H}} H,$$

der Schnitt über alle Untergruppen H von G, die A enthalten.

Dazu ein paar Bemerkungen:

- Der Schnitt ist wohldefiniert, denn er läuft über eine nichtleere Familie von Mengen: Wegen $A \subseteq G$ und $G \leq G$ kommt zumindest G selbst im Schnitt vor.
- Der Schnitt beliebig vieler Untergruppen ist wieder eine Untergruppe. Er ist nicht leer, da $1 \in H$ für alle $H \leq G$ gilt. Sind $x, y \in \bigcap H$, so liegen x und y in jeder der

geschnittenen Untergruppen H, also auch xy^{-1}, und damit ist $xy^{-1} \in \bigcap H$ (siehe Abschnitt 1.6).
- Es gilt $A \subseteq \langle A \rangle$.
- $\langle A \rangle$ ist die kleinste Untergruppe von G, die A enthält: Ist $H \leq G$ mit $A \subseteq H$, so kommt H im Schnitt vor, also ist $\langle A \rangle \subseteq H$.
- Ist $A = \{a_1, ..., a_n\}$ endlich, so schreibt man $\langle a_1, ..., a_n \rangle$ statt $\langle \{a_1, ..., a_n\} \rangle$. Manchmal schreibt man auch $\langle A, B \rangle := \langle A \cup B \rangle$ für $A, B \subseteq G$.

Die Definition als Schnitt ist elegant, aber nicht konstruktiv. Die folgende Proposition beschreibt die Elemente von $\langle A \rangle$ explizit.

Proposition 1.9.2: Sei G eine Gruppe und $A \subseteq G$. Dann ist

$$\langle A \rangle = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_m^{\varepsilon_m} : m \in \mathbb{N}_0,\ a_i \in A,\ \varepsilon_i \in \{1, -1\} \text{ für } i = 1, ..., m\},$$

wobei das Produkt für $m = 0$ (das „leere Produkt“) das neutrale Element $1 \in G$ bedeuten soll.

Beweis. Sei W die Menge auf der rechten Seite. W ist eine Untergruppe von G: Es ist $1 \in W$ (mit $m = 0$), das Produkt zweier solcher Ausdrücke ist wieder einer, und nach Proposition 1.1.9 ist

$$\left(a_1^{\varepsilon_1} \cdots a_m^{\varepsilon_m}\right)^{-1} = a_m^{-\varepsilon_m} \cdots a_1^{-\varepsilon_1} \in W.$$

Außerdem enthält W die Menge A (mit $m = 1, \varepsilon_1 = 1$). Da $\langle A \rangle$ die kleinste Untergruppe ist, die A enthält, folgt $\langle A \rangle \subseteq W$. Umgekehrt enthält jede Untergruppe H mit $A \subseteq H$ alle Elemente von A, deren Inverse und alle Produkte davon, also $W \subseteq H$. Damit ist W im Schnitt $\langle A \rangle$ enthalten. ∎

Insbesondere passt die Definition zu den früheren Begriffen: Für $A = \{x\}$ erhält man $\langle x \rangle = \{1, x^{\pm 1}, x^{\pm 2}, ...\}$ wie in Abschnitt 1.8, und $G = \langle S \rangle$ im Sinne von Definition 1.9.1 bedeutet genau, dass S die Gruppe G im Sinne von Definition 1.2.7 erzeugt.

Ist G abelsch und $A = \{a_1, ..., a_n\}$, so kann man die Faktoren in jedem Produkt sortieren und erhält

$$\langle A \rangle = \{a_1^{u_1} a_2^{u_2} \cdots a_n^{u_n} : u_i \in \mathbb{Z} \text{ für } i = 1, ..., n\}.$$

Zum Beispiel ist $a_1 a_2 a_1 a_2 = a_1 a_1 a_2 a_2 = a_1^2 a_2^2$. Falls G nicht abelsch ist, ist Vorsicht geboten. In D_{2n} haben wir zwar Sortierrelationen, und jedes Element lässt sich als r^k oder sr^k schreiben (siehe Abschnitt 1.2). Das liegt aber daran, dass dort die Erzeuger klug gewählt wurden. Auf diese Weise können viele Untergruppen erzeugt werden, aber im Allgemeinen ist $\langle A \rangle$ schwer zu handhaben, falls $|A| \geq 2$ ist.

Manchmal ist $\langle x, y \rangle$ trotzdem einfach. Liegt y im Zentralisator $C_G(x) = \{g \in G : gxg^{-1} = x\}$ von x (siehe Abschnitt 1.7), d.h. gilt $xy = yx$, so kann man wie im abelschen Fall sortieren und erhält $\langle x, y \rangle = \{x^a y^b : a, b \in \mathbb{Z}\}$.

© 2026 Thomas Kahle

1.10 Der Untergruppenverband

Die Untergruppen einer Gruppe G sind durch die Relation $\leq$ partiell geordnet; diese stimmt mit der Inklusion $\subseteq$ überein. Bezüglich dieser partiellen Ordnung gibt es zu je zwei Untergruppen $H, K \leq G$ ein größtes gemeinsames unteres und ein kleinstes gemeinsames oberes Element:

- $H \cap K \leq G$ ist die größte Untergruppe von G, die in H und in K enthalten ist (das *Meet* von H und K).
- $\langle H, K\rangle \leq G$ ist die kleinste Untergruppe von G, die H und K enthält (das *Join* von H und K). Im Allgemeinen ist $\langle H, K\rangle$ echt größer als $H \cup K$, denn die Vereinigung zweier Untergruppen ist meist keine Untergruppe.

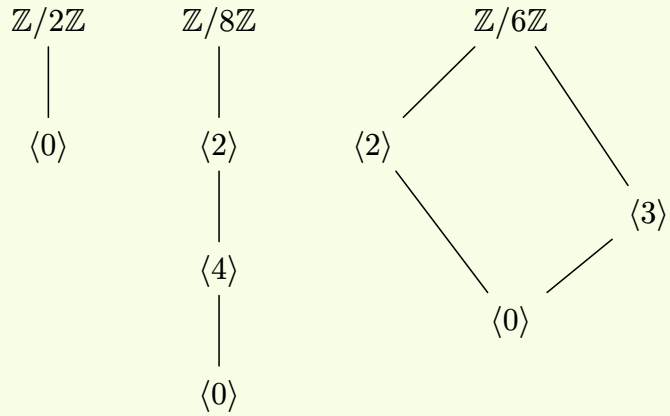
Außerdem gibt es unter den Untergruppen ein kleinstes Element, nämlich $\langle 1\rangle = \{1\}$, und ein größtes Element, nämlich $G = \langle G\rangle$.

In der Ordnungstheorie heißt eine solche Struktur ein *Verband*.

Definition 1.10.1: Die Menge der Untergruppen von G, partiell geordnet durch Inklusion, heißt der *Untergruppenverband* von G.

Ist G endlich, so kann man den Untergruppenverband mit Hilfe eines *Hasse-Diagramms* zeichnen. Dabei steht G oben, $\{1\}$ unten, und Linien kennzeichnen direkte Inklusionen, d.h. Inklusionen $K \subsetneq H$, zwischen denen keine weitere Untergruppe liegt. Die größere Untergruppe steht dabei weiter oben.

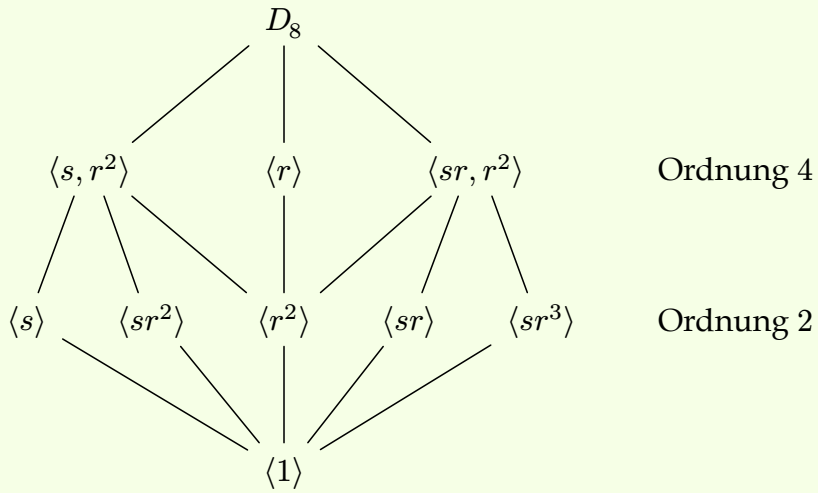
Beispiel 1.10.2: Wir zeichnen die Untergruppenverbände von $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ und schreiben dabei kurz $\langle a\rangle$ statt $\langle \overline{a}\rangle$. Nach Satz 1.8.7 entsprechen die Untergruppen den Teilern von 2, 8 bzw. 6.



In $\mathbb{Z}/6\mathbb{Z}$ hat $\langle \overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}\}$ die Ordnung 3 und $\langle \overline{3}\rangle = \{\overline{0}, \overline{3}\}$ die Ordnung 2. Die Höhe im Diagramm deutet die Ordnung an.

thomas.kahle@ovgu.de

Beispiel 1.10.3: Der Untergruppenverband der Diedergruppe D_8 (die Symmetrien des Quadrats) sieht so aus:



Dabei ist $\langle s, r^2\rangle = \{1, r^2, s, sr^2\}$ und $\langle sr, r^2\rangle = \{1, r^2, sr, sr^3\}$. Die fünf Untergruppen der Ordnung 2 werden von den fünf Elementen der Ordnung 2 erzeugt, nämlich von r^2 und den vier Spiegelungen s, sr, sr^2, sr^3. Dass dies alle Untergruppen von D_8 sind, kann man mit dem Satz von Lagrange einsehen, den wir später beweisen (siehe Abschnitt 1.12).

Noch ein paar Bemerkungen zu Untergruppenverbänden:

- Für unendliche Gruppen sind manchmal Teildiagramme nützlich. Dann kann eine Kante aber eine andere Bedeutung haben, denn zwischen zwei eingezeichneten Untergruppen können weitere liegen, die nicht eingezeichnet sind.
- Isomorphe Gruppen haben isomorphe Untergruppenverbände. Ist nämlich $\varphi\colon G \to H$ ein Isomorphismus und $K \leq G$, so ist $\varphi(K) \leq H$, denn $1 = \varphi(1) \in \varphi(K)$ und $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(K)$ für $a, b \in K$ nach Lemma 1.4.2. Die Abbildung $K \mapsto \varphi(K)$ erhält Inklusionen, und ihre Umkehrung ist $L \mapsto \varphi^{-1}(L)$.
- Nicht-isomorphe Gruppen können isomorphe Untergruppenverbände haben. Zum Beispiel haben $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ beide nur die zwei Untergruppen $\{0\}$ und sich selbst. Ebenso haben $\mathbb{Z}/6\mathbb{Z}$ und $\mathbb{Z}/10\mathbb{Z}$ nach Satz 1.8.7 isomorphe Verbände, denn 6 und 10 haben gleich viele Teiler, die auf die gleiche Weise angeordnet sind.

1.11 Quotientengruppen

Quotientengruppen sind neben den Untergruppen die zweite wichtige Möglichkeit, aus einer Gruppe kleinere, einfachere Gruppen zu gewinnen. Quotienten und Untergruppen sind dabei in einem präzisen Sinn *komplementär*: Untergruppen gehören zu Homomorphismen *in* die Gruppe G hinein, Quotienten gehören zu Homomorphismen *aus* G heraus.

© 2026 Thomas Kahle

Lemma 1.11.1: Sei $\varphi\colon H \to G$ ein Homomorphismus von Gruppen. Dann ist das Bild $\varphi(H)$ eine Untergruppe von G. Umgekehrt ist jede Untergruppe $H \leq G$ das Bild eines Homomorphismus, nämlich der Inklusion $H \to G$, $h \mapsto h$.

Beweis. Wir benutzen das Untergruppenkriterium (siehe Abschnitt 1.6). Es ist $\varphi(1) \in \varphi(H)$, also $\varphi(H) \neq \varnothing$. Seien $x, y \in \varphi(H)$, etwa $x = \varphi(a)$ und $y = \varphi(b)$ mit $a, b \in H$. Nach Lemma 1.4.2 ist dann $xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(H)$. Also ist $\varphi(H) \leq G$. Die zweite Aussage ist klar. ∎

Quotienten dagegen gehören zu Homomorphismen $G \to K$ in beliebige Gruppen K. Um das zu verstehen, sehen wir uns an, wie ein Homomorphismus die Gruppe G zerlegt.

Fasern

Definition 1.11.2: Sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen und $a \in H$. Die *Faser* von φ über a ist die Menge der Urbilder

$$X_a := \varphi^{-1}(a) = \{g \in G\colon \varphi(g) = a\}.$$

Nach der Definition von Abbildungen liegt jedes $g \in G$ in genau einer Faser, nämlich in $X_{\varphi(g)}$. Also ist G die disjunkte Vereinigung der nichtleeren Fasern, und das sind genau die Fasern X_a mit $a \in \varphi(G)$. Das ist ein Spezialfall einer allgemeinen Beobachtung: Für jede Abbildung $f\colon X \to Y$ ist durch $x_1 \sim x_2 :\Leftrightarrow f(x_1) = f(x_2)$ eine Äquivalenzrelation auf X definiert, und ihre Äquivalenzklassen sind die nichtleeren Fasern von f. Man stellt sich die Situation wie in Abbildung 3 vor.

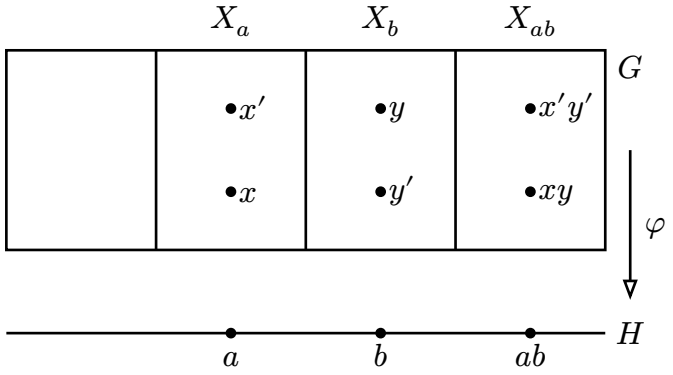


Abbildung 3: Die Fasern eines Homomorphismus $\varphi\colon G \to H$. Liegen x, x' in X_a und y, y' in X_b, so liegen xy und $x'y'$ beide in X_{ab}.

thomas.kahle@ovgu.de

Proposition 1.11.3: Sei $\varphi: G \to H$ ein Homomorphismus. Die Menge der nichtleeren Fasern $\{X_a : a \in \varphi(G)\}$ ist mit der Multiplikation

$$X_a \cdot X_b := X_{ab}$$

eine Gruppe. Die Abbildung $\varphi(G) \to \{X_a : a \in \varphi(G)\}$, $a \mapsto X_a$, ist ein Isomorphismus.

Beweis. Sind $a, b \in \varphi(G)$, so ist auch $ab \in \varphi(G)$, denn $\varphi(G)$ ist nach Lemma 1.11.1 eine Untergruppe. Also ist X_{ab} wieder eine nichtleere Faser, und da verschiedene a verschiedene (disjunkte) Fasern liefern, ist die Multiplikation wohldefiniert. Die Gruppenaxiome erbt man von $\varphi(G)$:

$$X_a(X_bX_c) = X_{a(bc)} = X_{(ab)c} = (X_aX_b)X_c,$$

das neutrale Element ist X_1, und das Inverse von X_a ist $X_{a^{-1}}$. Die Abbildung $a \mapsto X_a$ ist nach Definition der Multiplikation ein Homomorphismus, und sie ist bijektiv, weil die nichtleeren Fasern genau den Elementen von $\varphi(G)$ entsprechen. ∎

Die Multiplikation der Fasern ist übrigens auch die Multiplikation von Teilmengen: Für $a, b \in \varphi(G)$ gilt $X_aX_b = \{xy : x \in X_a, y \in X_b\} = X_{ab}$. Die Inklusion „$\subseteq$“ ist genau die Beobachtung aus Abbildung 3, und ist umgekehrt $z \in X_{ab}$ und $x \in X_a$ beliebig, so ist $x^{-1}z \in X_b$ und $z = x(x^{-1}z)$.

Beispiel 1.11.4: Sei $G = \mathbb{Z}$ (additiv) und $H = \mathbb{Z}_n = \langle x \rangle$ die zyklische Gruppe der Ordnung n, also $H = \{1, x, x^2, ..., x^{n-1}\}$ mit $x^n = 1$ (siehe Abschnitt 1.8). Die Abbildung

$$\varphi: \mathbb{Z} \to \mathbb{Z}_n, \quad a \mapsto x^a$$

ist nach den Potenzgesetzen ein Homomorphismus, und sie ist surjektiv. Ihre Fasern sind

$$\begin{aligned} X_{x^a} = \varphi^{-1}(x^a) &= \{m \in \mathbb{Z} : x^m = x^a\} = \{m \in \mathbb{Z} : x^{m-a} = 1\} \\ &= \{m \in \mathbb{Z} : n \mid m - a\} = \{m \in \mathbb{Z} : m \equiv a \bmod n\}, \end{aligned}$$

wobei wir benutzt haben, dass $x^k = 1$ genau dann gilt, wenn die Ordnung n von x die Zahl k teilt (siehe Abschnitt 1.8). Die Fasern sind also genau die Restklassen modulo n, und der Kern ist $\ker \varphi = X_1 = n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$.

© 2026 Thomas Kahle

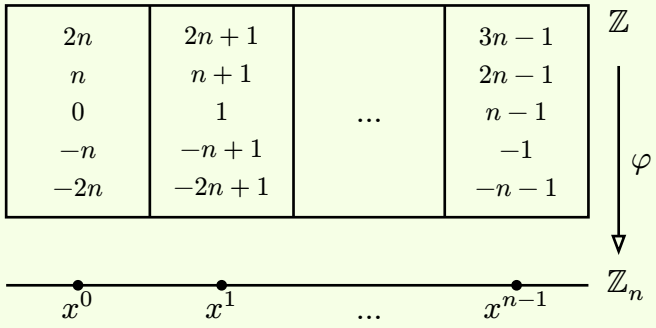


Abbildung 4: Die Fasern von $\mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto x^a$, sind die Restklassen modulo n.

Die Quotientengruppe nach einem Kern

Die Gruppe der Fasern bekommt einen eigenen Namen. Dabei rückt der Kern in den Mittelpunkt. Wir erinnern daran, dass der Kern $\ker \varphi = \{g \in G : \varphi(g) = 1\}$ eines Homomorphismus $\varphi: G \to H$ eine Untergruppe von G ist (siehe Abschnitt 1.6).

Definition 1.11.5: Sei $\varphi: G \to H$ ein Homomorphismus von Gruppen mit Kern $K = \ker \varphi$. Die *Quotientengruppe* G/K (gesprochen „G modulo K“) ist die Gruppe der nichtleeren Fasern von φ mit dem Produkt

$$\varphi^{-1}(a) \cdot \varphi^{-1}(b) := \varphi^{-1}(ab).$$

- Der Kern $K = \varphi^{-1}(1)$ ist selbst eine der Fasern, nämlich das neutrale Element von G/K.
- Die Notation G/K erinnert an die Notation für Äquivalenzrelationen: Ist $\sim$ eine Äquivalenzrelation auf einer Menge M, so schreibt man $M/\sim$ für die Menge der Äquivalenzklassen. Hier ist G/K die Menge der Äquivalenzklassen bezüglich

$$u \sim v :\Leftrightarrow uv^{-1} \in K \Leftrightarrow \varphi(uv^{-1}) = 1 \Leftrightarrow \varphi(u)\varphi(v)^{-1} = 1 \Leftrightarrow \varphi(u) = \varphi(v).$$

- In der Notation G/K verschwindet φ. Es bleibt aber in Gestalt der *kanonischen Abbildung* $G \to G/K$ erhalten, die $g \in G$ auf seine Äquivalenzklasse, also die Faser $\varphi^{-1}(\varphi(g))$, abbildet.

Die Fasern lassen sich direkt durch den Kern beschreiben.

Proposition 1.11.6: Sei $\varphi: G \to H$ ein Homomorphismus mit Kern K, und sei $X \in G/K$ eine Faser, d.h. $X = \varphi^{-1}(a)$ für ein $a \in \varphi(G)$. Dann gilt für alle $u \in X$:

$$X = \{uk : k \in K\} =: uK \quad \text{und} \quad X = \{ku : k \in K\} =: Ku.$$

Beweis. Wir zeigen nur die erste Gleichung, die zweite folgt analog. Sei $u \in X$, also $\varphi(u) = a$.

„$\supseteq$“: Sei $k \in K$ beliebig. Dann ist $\varphi(uk) = \varphi(u)\varphi(k) = a \cdot 1 = a$, also $uk \in X$. Damit ist $uK \subseteq X$.

„$\subseteq$“: Sei $g \in X$ und setze $k := u^{-1}g \in G$. Dann ist $uk = g$, und es bleibt $k \in K$ zu zeigen. Es gilt $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1$. Also ist $k \in K$ und $g = uk \in uK$. Damit ist $X \subseteq uK$. ∎

Im Beispiel 1.11.4 ist jede Faser von der Form $a + n\mathbb{Z}$ für jedes Element a der Faser, in additiver Schreibweise also genau $a + \ker\varphi$.

Der Kern eines Homomorphismus ist also eine Untergruppe mit besonderen Eigenschaften. Wir werden gleich sehen, dass nicht jede Untergruppe der Kern eines Homomorphismus ist. Zunächst machen wir die Konstruktion aus Proposition 1.11.6 für beliebige Untergruppen.

Nebenklassen

Definition 1.11.7: Sei $H \leq G$ eine Untergruppe und $g \in G$.
- Die Menge $gH := \{gh : h \in H\}$ heißt *Linksnebenklasse* von H bezüglich g (oder nach g).
- Die Menge $Hg := \{hg : h \in H\}$ heißt *Rechtsnebenklasse* von H bezüglich g.

- Wird G additiv geschrieben, so schreibt man die Nebenklassen als $g + H$.
- Ist G abelsch, so gilt $gH = Hg$ für alle $g \in G$.
- Proposition 1.11.6 besagt, dass die Fasern $\varphi^{-1}(a)$ eines Homomorphismus sowohl die Links- als auch die Rechtsnebenklassen des Kerns $K = \ker\varphi$ sind. Insbesondere gilt hier $uK = Ku = \varphi^{-1}(a)$ für alle $u \in \varphi^{-1}(a)$. Wir werden bald sehen, dass eine Untergruppe K genau dann ein Kern ist, wenn $uK = Ku$ für alle $u \in G$ gilt.

Die Elemente von G/K können wir also als Linksnebenklassen auffassen. Wie multipliziert man sie? Seien xK und yK zwei Elemente von G/K mit $x, y \in G$. Die naheliegende Idee ist, die Multiplikation in G/K über Repräsentanten zu berechnen:

$$xK \cdot yK := xyK. \tag{1}$$

Hier gibt es ein Problem: Jedes Element von xK kann als Repräsentant gewählt werden. Ist $x' \in xK$ und $y' \in yK$, so ist zwar $xK = x'K$ und $yK = y'K$, aber es ist nicht klar, ob auch $xyK = x'y'K$ gilt. Die Festlegung (1) hängt also unter Umständen von der Wahl der Repräsentanten x, y ab. Für Kerne geht aber alles gut.

Satz 1.11.8: Sei $\varphi : G \to H$ ein Homomorphismus mit Kern K. Die Menge G/K der Linksnebenklassen von K ist mit

$$(xK)(yK) := (xy)K$$

eine Gruppe, und diese Gruppe ist die Quotientengruppe aus Definition 1.11.5. Dasselbe gilt für die Rechtsnebenklassen.

Beweis. Nach Proposition 1.11.6 sind die Linksnebenklassen genau die Fasern, d.h. $xK = \varphi^{-1}(a)$ und $yK = \varphi^{-1}(b)$ mit $a = \varphi(x)$ und $b = \varphi(y)$. In welcher Faser liegt xy? Es ist $\varphi(xy) = \varphi(x)\varphi(y) = ab$, also $xy \in \varphi^{-1}(ab)$ und damit $xyK = \varphi^{-1}(ab)$. Die Multiplikation (1) ist also genau die Multiplikation $\varphi^{-1}(a) \cdot \varphi^{-1}(b) = \varphi^{-1}(ab)$ der Quotientengruppe. Da die Wahl der Repräsentanten x, y beliebig war, erhält man stets dieselbe Faser $\varphi^{-1}(ab)$, vergleiche Abbildung 3. Für Rechtsnebenklassen argumentiert man genauso. ∎

Ist klar, um welche Untergruppe K es geht, so verwendet man auch die kurze Notation $\overline{x} := xK$ für Nebenklassen. In dieser Notation gilt $\overline{x} \cdot \overline{y} = \overline{xy}$. Das kennen wir von den Restklassen $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, und das ist kein Zufall: $\mathbb{Z}/n\mathbb{Z}$ ist der Quotient von $\mathbb{Z}$ nach $n\mathbb{Z}$, dem Kern des Homomorphismus aus Beispiel 1.11.4.

Beispiel 1.11.9:
- Ist $\varphi: G \to H$ ein Isomorphismus, so ist $K = \{1\}$, alle Fasern $\varphi^{-1}(a)$ sind einelementig, und $G/\{1\} \cong G$ via $g \mapsto \{g\}$.
- Seien G, H beliebig und $\varphi: G \to H$, $g \mapsto 1$, der triviale Homomorphismus. Dann ist $K = \ker\varphi = G$ und $G/G \cong \{1\}$.
- Ist V ein Vektorraum und $U \subseteq V$ ein Untervektorraum, so ist der Quotientenvektorraum $V/U = \{v + U : v \in V\}$ insbesondere eine Quotientengruppe der abelschen Gruppe $(V, +)$.

Achtung! In der Gruppentheorie können wir (vorerst) nur Quotienten bezüglich Kernen bilden. Wer die lineare Algebra mag, sollte hier vorsichtig sein:
- Jeder Untervektorraum ist der Kern einer linearen Abbildung. Bei Gruppen ist nicht jede Untergruppe ein Kern (siehe Beispiel 1.11.14 unten).
- Jeder Quotient V/U ist isomorph zu einem Untervektorraum, genauer gilt $V \cong U \oplus V/U$. Für Gruppen ist das falsch: Zum Beispiel ist $\mathbb{Z}/2\mathbb{Z}$ ein Quotient von $\mathbb{Z}$, aber nicht isomorph zu einer Untergruppe von $\mathbb{Z}$, denn in $\mathbb{Z}$ hat kein Element außer 0 endliche Ordnung.

Diese Analogien sind also falsch! Insbesondere sind Quotienten und Untergruppen wirklich komplementär und nicht heimlich das Gleiche.

Quotienten nach Untergruppen

Wir wollen nun G/H für beliebige Untergruppen $H \leq G$ betrachten und dabei ohne einen Homomorphismus auskommen. Als Menge soll G/H aus den Linksnebenklas-

sen bestehen, inspiriert von Proposition 1.11.6, wonach eine Faser eine Nebenklasse $X = uK = Ku$ des Kerns ist.

Praktischerweise sind Nebenklassen bezüglich einer beliebigen Untergruppe $H \leq G$ immer Äquivalenzklassen. Für $u, u' \in G$ gilt nämlich

$$u^{-1}u' \in H \Leftrightarrow uH = u'H.$$

Ist $u^{-1}u' = h_1 \in H$, so ist $u' = uh_1$ und damit $u'H = uh_1H = uH$, denn $h_1H = H$. Ist umgekehrt $uH = u'H$, so ist insbesondere $u' = u' \cdot 1 \in uH$, also $u' = uh_1$ für ein $h_1 \in H$ und $u^{-1}u' = h_1 \in H$. Damit ist

$$u \sim u' :\Leftrightarrow u^{-1}u' \in H$$

eine Äquivalenzrelation, denn sie ist von der Form $uH = u'H$. Ihre Äquivalenzklassen sind die Linksnebenklassen. Daraus folgt: G ist die disjunkte Vereinigung der Linksnebenklassen von H, und man hat eine *kanonische Abbildung*

$$\pi\colon G \to G/H := \{gH\colon g \in G\}, \quad g \mapsto gH.$$

Die entscheidende Frage ist: Ist G/H mit der Multiplikation (1) eine Gruppe und π ein Homomorphismus? In diesem Fall ist $H = \ker\pi$ ein Kern, und G/H ist ein Quotient wie oben. Dass dabei nur die Multiplikation (1) in Frage kommt, liegt daran, dass π ein Homomorphismus sein soll: Dann muss $\pi(g)\pi(g') = \pi(gg')$ gelten, also $gH \cdot g'H = gg'H$.

Proposition 1.11.10: Sei $H \leq G$ eine Untergruppe.

1. Die Multiplikation von Linksnebenklassen
$$gH \cdot g'H := gg'H$$
ist genau dann wohldefiniert, wenn für alle $g \in G$ und $h \in H$ gilt: $ghg^{-1} \in H$ (bzw. $gHg^{-1} \subseteq H$, wobei $gHg^{-1} := \{ghg^{-1}\colon h \in H\}$).
2. In diesem Fall bilden die Linksnebenklassen mit dieser Multiplikation eine Gruppe.

Beweis.

1. Angenommen, die Multiplikation ist wohldefiniert. Seien $g \in G$ und $h \in H$. Wegen $h \in H$ ist $hH = H = 1H$. Wir berechnen das Produkt $(1H)(g^{-1}H)$ mit zwei verschiedenen Repräsentanten des ersten Faktors:
$$g^{-1}H = (1H)(g^{-1}H) = (hH)(g^{-1}H) = hg^{-1}H.$$
Multipliziert man diese Gleichung von links mit gH (wieder wohldefiniert), so folgt $ghg^{-1}H = gg^{-1}H = H$, also $ghg^{-1} \in H$.

© 2026 Thomas Kahle

Sei nun umgekehrt $ghg^{-1} \in H$ für alle $g \in G$, $h \in H$. Wir zeigen die Wohldefiniertheit. Seien $u, u', v, v' \in G$ mit $uH = u'H$ und $vH = v'H$, d.h. $u' = uh_1$ und $v' = vh_2$ mit $h_1, h_2 \in H$. Zu zeigen ist $uvH = u'v'H$. Es gilt

$$u'v' = uh_1vh_2 = uv\underbrace{(v^{-1}h_1v)}_{\in H}h_2 = uvh_3$$

mit $h_3 := (v^{-1}h_1v)h_2 \in H$; dabei haben wir die Voraussetzung mit $g = v^{-1}$ benutzt. Also ist $u'v'H = uvh_3H = uvH$.

2. Die Assoziativität erbt man von G: $(gH)(g'Hg''H) = g(g'g'')H = (gg')g''H = (gHg'H)(g''H)$. Das neutrale Element ist $1H = H$, und das Inverse von gH ist $g^{-1}H$. ■

Die Bedingung aus Proposition 1.11.10 verdient einen Namen.

Definition 1.11.11: Sei G eine Gruppe, $H \leq G$ eine Untergruppe und $g \in G$.
- Für $h \in H$ heißt ghg^{-1} das mit g *konjugierte* Element von h.
- Die Menge $gHg^{-1} = \{ghg^{-1} : h \in H\}$ heißt *Konjugation* oder *konjugierte Untergruppe* zu H.
- g *normalisiert* H, falls $gHg^{-1} = H$ gilt.
- H heißt *normal* oder *Normalteiler*, falls jedes $g \in G$ die Untergruppe H normalisiert, d.h. falls $gHg^{-1} = H$ für alle $g \in G$ gilt. Mit dem Normalisator $N_G(H) = \{g \in G : gHg^{-1} = H\}$ heißt das $N_G(H) = G$ (siehe Abschnitt 1.7). In diesem Fall schreibt man $H \trianglelefteq G$.

Die konjugierte Untergruppe gHg^{-1} ist tatsächlich eine Untergruppe von G: Sie ist das Bild von H unter dem Homomorphismus $G \to G$, $x \mapsto gxg^{-1}$, denn $gxyg^{-1} = (gxg^{-1})(gyg^{-1})$. Nach Lemma 1.11.1 ist sie also eine Untergruppe.

Satz 1.11.12: Sei $H \leq G$ eine Untergruppe. Dann sind äquivalent:
1. $H \trianglelefteq G$.
2. $N_G(H) = G$.
3. $gH = Hg$ für alle $g \in G$.
4. Die Multiplikation $gH \cdot g'H := gg'H$ der Linksnebenklassen ist wohldefiniert und macht G/H zu einer Gruppe.
5. Die Multiplikation $Hg \cdot Hg' := Hgg'$ der Rechtsnebenklassen ist wohldefiniert und macht die Menge der Rechtsnebenklassen zu einer Gruppe.
6. Es gibt eine Gruppenstruktur auf G/H, sodass die kanonische Abbildung $\pi : G \to G/H$, $g \mapsto gH$, ein Homomorphismus ist.
7. $gHg^{-1} \subseteq H$ für alle $g \in G$.

Beweis. (1) $\Leftrightarrow$ (2) ist die Definition.

thomas.kahle@ovgu.de

(1) $\Rightarrow$ (7) ist klar. Für (7) $\Rightarrow$ (1) sei $g \in G$. Nach Voraussetzung, angewendet auf g^{-1}, ist $g^{-1}Hg \subseteq H$. Konjugiert man diese Inklusion mit g, so folgt $H \subseteq gHg^{-1}$, also zusammen mit (7) die Gleichheit $gHg^{-1} = H$.

(1) $\Rightarrow$ (3): Aus $gHg^{-1} = H$ folgt durch Multiplikation von rechts mit g, dass $gH = Hg$ ist. (3) $\Rightarrow$ (1): Aus $gH = Hg$ folgt durch Multiplikation von rechts mit g^{-1}, dass $gHg^{-1} = H$ ist.

(7) $\Leftrightarrow$ (4) ist Proposition 1.11.10.

(7) $\Leftrightarrow$ (5): Wie in Proposition 1.11.10 zeigt man, dass die Multiplikation der Rechtsnebenklassen genau dann wohldefiniert ist, wenn $g^{-1}Hg \subseteq H$ für alle $g \in G$ gilt. Da mit g auch g^{-1} ganz G durchläuft, ist das äquivalent zu (7).

(4) $\Rightarrow$ (6): Mit der Multiplikation aus (4) gilt $\pi(g)\pi(g') = gHg'H = gg'H = \pi(gg')$.

(6) $\Rightarrow$ (4): Ist π ein Homomorphismus, so gilt $gH \cdot g'H = \pi(g)\pi(g') = \pi(gg') = gg'H$ für alle $g, g' \in G$. Die Gruppenstruktur ist also durch die Multiplikation aus (4) gegeben, und diese ist insbesondere wohldefiniert. ■

Im Fall $H \trianglelefteq G$ heißt die Gruppe G/H der *Quotient* von G nach H (auch *Faktorgruppe*). Er stimmt mit der Quotientengruppe $G/\ker\pi$ im Sinne von Definition 1.11.5 überein, denn $\ker\pi = \{g \in G : gH = H\} = H$.

Beachte: Ist H ein Normalteiler, so ist $H = \ker\pi$ für die kanonische Abbildung $\pi : G \to G/H$ ein Kern. Ist umgekehrt H ein Kern, so ist H ein Normalteiler, denn die Fasern erfüllen nach Proposition 1.11.6 $uH = Hu$ für alle $u \in G$. Also gilt:

Korollar 1.11.13: Eine Untergruppe $H \leq G$ ist genau dann ein Normalteiler, wenn sie der Kern eines Homomorphismus ist.

Beispiel 1.11.14: Sei $H = \langle(12)\rangle = \{1, (12)\} \leq S_3$. Dann ist

$$(13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin H.$$

Also ist H kein Normalteiler von S_3 und damit nach Korollar 1.11.13 auch nicht der Kern eines Homomorphismus. Insbesondere ist nicht jede Untergruppe ein Kern.

Normalteiler nachprüfen

Das Prüfen der Normalteilereigenschaft sieht mühsam aus, denn man muss $ghg^{-1} \in H$ für alle $g \in G$ und alle $h \in H$ zeigen. Es lässt sich aber oft vereinfachen.

- Elemente von H müssen nicht als g geprüft werden, denn für $g \in H$ ist $ghg^{-1} \in H$ klar.

© 2026 Thomas Kahle

- Inverse von Konjugierten sind Konjugierte von Inversen: $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. Das ist wieder ein konjugiertes Element, und zwar mit dem *gleichen* g, was wichtig ist!
- Produkte: Sei g fest. Dann ist $(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1}$ wieder ein mit g konjugiertes Element.

Ist H durch Erzeuger gegeben, so genügt es also, $ghg^{-1} \in H$ für alle $g \in G$ und alle Erzeuger h von H zu prüfen. Ist auch G durch Erzeuger gegeben, so reicht noch weniger.

Proposition 1.11.15: Sei $G = \langle T \rangle$ und $H = \langle S \rangle \leq G$. Gilt $tst^{-1} \in H$ für alle $s \in S$ und alle $t \in T \cup T^{-1}$ (wobei $T^{-1} = \{t^{-1} : t \in T\}$), so ist $H \trianglelefteq G$.

Beweis. Sei $h \in H$ und $g \in G$. Wir schreiben

$$h = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}, \quad g = t_1^{\varepsilon_1'} \cdots t_l^{\varepsilon_l'}$$

mit $s_i \in S$, $t_j \in T$ und $\varepsilon_i, \varepsilon_j' \in \{\pm 1\}$. Dann ist

$$ghg^{-1} = t_1^{\varepsilon_1'} \cdots t_l^{\varepsilon_l'} \cdot h \cdot \left(t_l^{\varepsilon_l'}\right)^{-1} \cdots \left(t_1^{\varepsilon_1'}\right)^{-1}.$$

Per Induktion nach l (von innen nach außen) genügt es zu zeigen, dass $tht^{-1} \in H$ für alle $h \in H$ und alle $t \in T \cup T^{-1}$ gilt. Schiebt man zwischen je zwei Faktoren von h das Produkt $t^{-1}t = 1$ ein, so wird

$$tht^{-1} = \left(ts_1^{\varepsilon_1}t^{-1}\right) \cdots \left(ts_k^{\varepsilon_k}t^{-1}\right) = \left(ts_1t^{-1}\right)^{\varepsilon_1} \cdots \left(ts_kt^{-1}\right)^{\varepsilon_k}.$$

Es genügt also $ts_it^{-1} \in H$, und das gilt nach Voraussetzung. Damit ist $ghg^{-1} \in H$, und nach Satz 1.11.12 ist $H \trianglelefteq G$. ∎

Ist H endlich, so sind noch weitere Vereinfachungen möglich. Im Wesentlichen liegt das daran, dass $gHg^{-1} \subseteq H$ für ein einzelnes g dann schon $gHg^{-1} = H$ für dieses g liefert: Die Abbildung $H \to H$, $h \mapsto ghg^{-1}$, ist injektiv (aus $gh_1g^{-1} = gh_2g^{-1}$ folgt durch Kürzen $h_1 = h_2$), und eine injektive Abbildung einer endlichen Menge in sich selbst ist bijektiv. Im Beweis von Satz 1.11.12 haben wir dagegen nur benutzt, dass aus $gHg^{-1} \subseteq H$ für *alle* g die Gleichheit für alle g folgt. Für unendliche H und ein einzelnes g ist das falsch.

Beispiel 1.11.16: Sei $G = \mathrm{GL}_2(\mathbb{Q})$, $H = \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}$ und $g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. Dann ist

$$g\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}g^{-1} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix},$$

also ist $gHg^{-1} = \left\{\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in 2\mathbb{Z}\right\}$ eine echte Teilmenge von H.

thomas.kahle@ovgu.de

Bemerkungen zur Faktorabbildung
Sei $N \trianglelefteq G$ ein Normalteiler. Die kanonische Abbildung

$$\pi\colon G \to G/N, \quad g \mapsto gN,$$

heißt auch *kanonische Projektion* oder *Faktorabbildung*.

- Ist $\overline{H} \leq G/N$ eine Untergruppe, so heißt das Urbild $\pi^{-1}\left(\overline{H}\right)$ das *vollständige* oder *natürliche Urbild* von $\overline{H}$ in G. Es ist eine Untergruppe von G (das Urbild einer Untergruppe unter einem Homomorphismus ist eine Untergruppe, wie man mit dem Untergruppenkriterium nachrechnet), und es enthält $N = \ker \pi = \pi^{-1}(1)$. Wir werden später zeigen, dass dies eine Bijektion zwischen den Untergruppen von G, die N enthalten, und den Untergruppen von G/N liefert (siehe Abschnitt 1.13).
- Mit Normalisatoren kann man intern in einer Gruppe „messen“, wie normal eine Untergruppe ist. Zum Beispiel ist N genau dann normal, wenn $N_G(N) = \{g \in G\colon gNg^{-1} = N\} = G$ ist.
- Normalität ist keine intrinsische Eigenschaft einer Gruppe, sondern hängt von der Einbettung in eine umgebende Gruppe ab. Es kann $N \leq G_1 \leq G_2$ gelten mit $N \trianglelefteq G_1$, aber N nicht normal in G_2. Ein Beispiel in D_8 sehen wir in Beispiel 1.12.8.
- Quotienten von G entsprechen eins zu eins den Bildern von G unter Homomorphismen: Ist $\varphi\colon G \to H$ ein Homomorphismus, so ist $G/\ker\varphi \cong \varphi(G)$, denn beide sind die Gruppe der Fasern (Proposition 1.11.3). Und für jeden Normalteiler $N \trianglelefteq G$ hat man eine surjektive Abbildung $G \to G/N$. Das ist ein erster Blick auf den ersten Isomorphiesatz (siehe Abschnitt 1.13).
- Ist G abelsch, so ist jede Untergruppe normal, denn $gNg^{-1} = \{gng^{-1}\colon n \in N\} = \{n\colon n \in N\} = N$.
- Quotienten von zyklischen Gruppen sind zyklisch: Ist $G = \langle x\rangle$ und $N \trianglelefteq G$, so ist $G/N = \langle xN\rangle$, denn jedes Element von G/N hat die Form $x^kN = (xN)^k$.

1.12 Der Satz von Lagrange

Wir kommen nun zum ersten wirklich starken Satz über endliche Gruppen. Er setzt die Ordnung einer Gruppe mit den Ordnungen ihrer Untergruppen in Beziehung und hat eine Fülle von Folgerungen. Wir benutzen dabei, dass die Linksnebenklassen gH einer Untergruppe $H \leq G$ die Äquivalenzklassen einer Äquivalenzrelation sind und G daher disjunkt in Nebenklassen zerfällt (siehe Abschnitt 1.11).

Satz 1.12.1 (Lagrange): Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann teilt die Ordnung $|H|$ die Ordnung $|G|$, und $|G|/|H|$ ist die Anzahl der Linksnebenklassen von H in G.

Die Idee des Beweises ist, dass jede Nebenklasse genau $|H|$ Elemente hat.

Beweis. Sei $|H| = n$ und k die Anzahl der Linksnebenklassen von H in G. Sei $g \in G$ fest. Wir betrachten die Abbildung

$$H \to gH, \quad h \mapsto gh.$$

Sie ist surjektiv nach Definition der Nebenklasse $gH = \{gh : h \in H\}$. Sie ist injektiv, denn aus $gh_1 = gh_2$ folgt durch Multiplikation von links mit g^{-1}, dass $h_1 = h_2$. Also ist sie bijektiv, und es gilt $|gH| = |H| = n$ für jedes $g \in G$. Da G die disjunkte Vereinigung seiner k Linksnebenklassen ist, folgt $|G| = n \cdot k$. ■

Die Anzahl der Nebenklassen ist so wichtig, dass sie einen eigenen Namen bekommt.

Definition 1.12.2: Sei G eine Gruppe und $H \leq G$. Die Anzahl der Linksnebenklassen von H in G heißt der *Index* von H in G und wird mit $|G : H|$ bezeichnet.

Ist G endlich, so gilt nach dem Satz von Lagrange also

$$|G : H| = \frac{|G|}{|H|}.$$

Der Index ergibt aber auch für unendliche Gruppen Sinn. Zum Beispiel hat $2\mathbb{Z} \leq \mathbb{Z}$ endlichen Index: Es gibt genau zwei Nebenklassen, nämlich $0 + 2\mathbb{Z}$ (die geraden Zahlen) und $1 + 2\mathbb{Z}$ (die ungeraden Zahlen). Also ist $|\mathbb{Z} : 2\mathbb{Z}| = 2$.

Statt der Links- könnte man auch die Rechtsnebenklassen Hg zählen. Das ergibt dieselbe Zahl, denn die Abbildung $gH \mapsto Hg^{-1}$ ist eine Bijektion zwischen der Menge der Linksnebenklassen und der Menge der Rechtsnebenklassen.

Übung. Zeigen Sie, dass $gH \mapsto Hg^{-1}$ wohldefiniert und bijektiv ist. Warum funktioniert $gH \mapsto Hg$ im Allgemeinen nicht?

Korollar 1.12.3: Ist G endlich und $x \in G$, so teilt die Ordnung von x die Ordnung von G. Insbesondere gilt $x^{|G|} = 1$ für alle $x \in G$.

Beweis. Die Ordnung von x ist die Ordnung der von x erzeugten Untergruppe, $|x| = |\langle x \rangle|$ (siehe Abschnitt 1.8). Nach dem Satz von Lagrange ist also $|G| = m \cdot |x|$ für ein $m \in \mathbb{N}$, und damit $x^{|G|} = \left(x^{|x|}\right)^m = 1^m = 1$. ■

Damit können wir das Versprechen aus der Einleitung (Abschnitt 1.1) einlösen. Für $n \geq 2$ sei

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| = |\{k \in \{1, \ldots, n\} : \mathrm{ggT}(k, n) = 1\}|$$

die Anzahl der zu n teilerfremden Restklassen.

Korollar 1.12.4: Sei $n \geq 2$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Dann gilt $a^{\varphi(n)} \equiv 1 \bmod n$. Insbesondere gilt für jede Primzahl p und jedes nicht durch p teilbare a, dass $a^{p-1} \equiv 1 \bmod p$.

Beweis. Wende Korollar 1.12.3 auf $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ an. Für eine Primzahl p ist $\varphi(p) = p - 1$. ∎

Der zweite Teil heißt *kleiner Satz von Fermat*. Für $n = 100$ sind genau die Zahlen teilerfremd zu n, die weder durch 2 noch durch 5 teilbar sind. Davon gibt es zwischen 1 und 100 genau $100 - 50 - 20 + 10 = 40$ Stück. Also ist $\varphi(100) = 40$, und das ist der Satz von Euler aus der Einleitung.

Korollar 1.12.5: Sei G eine Gruppe mit Primzahlordnung $|G| = p$. Dann ist G zyklisch und $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$.

Beweis. Sei $x \in G$ mit $x \neq 1$. Dann gilt $|x| > 1$ und nach Korollar 1.12.3 teilt $|x|$ die Primzahl p. Also ist $|x| = p$ und damit $\langle x \rangle = G$. Nach der Klassifikation der zyklischen Gruppen ist $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$ (siehe Abschnitt 1.8). ∎

Bis auf Isomorphie gibt es also für jede Primzahl p genau eine Gruppe der Ordnung p.

Lagrange und Normalität

Der Satz von Lagrange hilft oft auch dabei, Normalteiler zu erkennen. Wir erinnern daran, dass $H \leq G$ genau dann normal ist, wenn der Normalisator $N_G(H) = \{g \in G : gHg^{-1} = H\}$ ganz G ist (siehe Abschnitt 1.7).

Beispiel 1.12.6: Wir wollen zeigen, dass $H = \langle (123) \rangle = \{1, (123), (132)\}$ ein Normalteiler in S_3 ist. Da H eine Untergruppe ist, gilt

$$H \leq N_{S_3}(H) \leq S_3.$$

Nach dem Satz von Lagrange teilt $|H| = 3$ die Ordnung $\left|N_{S_3}(H)\right|$, und diese teilt $|S_3| = 6$. Also ist $N_{S_3}(H) = H$ oder $N_{S_3}(H) = S_3$. Nun ist

$$(12)(123)(12)^{-1} = (132) = (123)^{-1} \in H.$$

Da (123) die Gruppe H erzeugt, folgt daraus $(12)(123)^k(12)^{-1} = ((12)(123)(12)^{-1})^k \in H$ für alle k, also $(12)H(12)^{-1} \subseteq H$, und da beide Seiten drei Elemente haben, gilt Gleichheit. Also ist $(12) \in N_{S_3}(H)$. Wegen $(12) \notin H$ ist $\left|N_{S_3}(H)\right| > 3$ und damit $N_{S_3}(H) = S_3$, d.h. $H \trianglelefteq S_3$.

Eine Verallgemeinerung dieses Beispiels ist die folgende Aussage.

© 2026 Thomas Kahle

Proposition 1.12.7: Sei $H \leq G$ mit $|G\colon H| = 2$. Dann ist $H \trianglelefteq G$.

Beweis. Für $g \in H$ ist $gH = H = Hg$. Sei nun $g \in G \setminus H$. Da es genau zwei Linksnebenklassen gibt und $g \notin H$, ist

$$G = H \cup gH$$

die Zerlegung in Nebenklassen von H, also $gH = G \setminus H$. Da es auch genau zwei Rechtsnebenklassen gibt, liefert dasselbe Argument $G \setminus H = Hg$. Also gilt $gH = Hg$ und damit $gHg^{-1} = H$ für alle $g \in G$, d.h. $H \trianglelefteq G$. ∎

Zum Beispiel ist die Untergruppe $\langle r \rangle$ der Drehungen in der Diedergruppe D_{2n} ein Normalteiler, denn sie hat n Elemente und damit Index 2.

Achtung! Normalität ist nicht transitiv: Aus $K \trianglelefteq H$ und $H \trianglelefteq G$ folgt im Allgemeinen nicht $K \trianglelefteq G$.

Beispiel 1.12.8: In $D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \rangle$ betrachten wir

$$\langle s \rangle = \{1, s\} \quad \text{und} \quad \langle s, r^2 \rangle = \{1, r^2, s, sr^2\}.$$

Die zweite Untergruppe hat vier Elemente, denn r^2 und s vertauschen ($sr^2 = r^{-2}s = r^2 s$). Es gilt

$$\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8,$$

da beide Inklusionen Index 2 haben (Proposition 1.12.7). Aber

$$rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} = sr^2 \notin \langle s \rangle,$$

also ist $r \notin N_{D_8}(\langle s \rangle)$, und $\langle s \rangle$ ist kein Normalteiler von D_8.

Normalteiler können selten sein. Die Gruppe S_3 hat zum Beispiel sechs Untergruppen, nämlich $\{1\}$, die drei Untergruppen $\langle (12) \rangle$, $\langle (13) \rangle$, $\langle (23) \rangle$ der Ordnung 2, die Untergruppe $\langle (123) \rangle$ und S_3 selbst. Davon sind nur drei normal: $\{1\}$, $\langle (123) \rangle$ und S_3.

Beispiel 1.12.9: Sei $n \geq 3$. Die Untergruppe $H = \langle (12) \rangle = \{1, (12)\} \leq S_n$ ist nicht normal. Das sieht man an der Multiplikation von Nebenklassen, die für Normalteiler durch $(xH)(yH) = xyH$ wohldefiniert ist (siehe Abschnitt 1.11). Einerseits ist $(1H) \cdot ((13)H) = (13)H$. Andererseits ist (12) ebenfalls ein Repräsentant von H, also $H = (12)H$, aber

$$((12)H) \cdot ((13)H) = (12)(13)H = (132)H \neq (13)H,$$

thomas.kahle@ovgu.de

denn $(13)^{-1}(132) = (13)(132) = (23) \notin H$. Für $n = 3$ haben wir das in Beispiel 1.11.14 schon direkt mit Konjugation gesehen.

Umkehrungen des Satzes von Lagrange

Ist $H \leq G$ und G endlich, so gilt nach Lagrange $|H| \mid |G|$. Umgekehrt kann man fragen: Wenn a ein Teiler von $|G|$ ist, gibt es dann eine Untergruppe der Ordnung a in G? Im Allgemeinen ist die Antwort nein. Die Gruppe der zwölf Drehsymmetrien eines regulären Tetraeders hat zum Beispiel keine Untergruppe der Ordnung 6. Für Primzahlen und Primzahlpotenzen gibt es aber positive Antworten.

Satz 1.12.10 (Cauchy): Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Dann existiert ein Element $x \in G$ mit $|x| = p$. Insbesondere ist $\langle x \rangle \leq G$ eine Untergruppe der Ordnung p.

Man kann ihn per Induktion nach $|G|$ beweisen. Wir geben stattdessen einen kurzen Abzählbeweis (nach McKay).

Beweis. Sei X die Menge der p-Tupel $(x_1, ..., x_p) \in G^p$ mit $x_1 x_2 \cdots x_p = 1$. Die Elemente $x_1, ..., x_{p-1}$ kann man beliebig wählen, und dann ist $x_p = (x_1 \cdots x_{p-1})^{-1}$ eindeutig festgelegt. Also ist $|X| = |G|^{p-1}$, und diese Zahl ist durch p teilbar.

Ist $(x_1, ..., x_p) \in X$, so ist auch das zyklisch verschobene Tupel $(x_2, ..., x_p, x_1)$ in X, denn $x_2 \cdots x_p x_1 = x_1^{-1}(x_1 x_2 \cdots x_p) x_1 = x_1^{-1} x_1 = 1$. Sei $\sigma \colon X \to X$ diese Verschiebung. Es gilt $\sigma^p = \mathrm{id}$. Wir nennen zwei Tupel äquivalent, wenn sie durch mehrfaches Verschieben auseinander hervorgehen. Das ist eine Äquivalenzrelation, und die Klasse von $t \in X$ ist $\{t, \sigma(t), ..., \sigma^{p-1}(t)\}$. Gilt $\sigma^k(t) = t$ für ein $0 < k < p$, so gibt es wegen $\mathrm{ggT}(k, p) = 1$ ganze Zahlen a, b mit $ak + bp = 1$, und es folgt $\sigma(t) = \sigma^{ak+bp}(t) = t$. Dann sind alle Einträge von t gleich. Ist t also nicht konstant, so sind $t, \sigma(t), ..., \sigma^{p-1}(t)$ paarweise verschieden, und die Klasse hat genau p Elemente. Ist t konstant, so hat die Klasse ein Element.

Da X disjunkt in diese Klassen zerfällt, gilt

$$|X| = c + p \cdot \ell,$$

wobei c die Anzahl der konstanten Tupel in X und ℓ die Anzahl der Klassen mit p Elementen ist. Die konstanten Tupel in X sind genau die $(x, ..., x)$ mit $x^p = 1$. Da p sowohl $|X|$ als auch $p\ell$ teilt, teilt p auch c. Wegen $(1, ..., 1) \in X$ ist $c \geq 1$, also $c \geq p \geq 2$. Es gibt also ein $x \neq 1$ mit $x^p = 1$.

Es bleibt $|x| = p$ zu zeigen. Teilt man p mit Rest durch $|x|$, also $p = q|x| + r$ mit $0 \leq r < |x|$, so ist $x^r = x^p (x^{|x|})^{-q} = 1$, also $r = 0$ wegen der Minimalität von $|x|$. Somit teilt $|x|$ die Primzahl p, und wegen $x \neq 1$ folgt $|x| = p$. ∎

© 2026 Thomas Kahle

Definition 1.12.11: Sei p eine Primzahl.
- Eine *p-Gruppe* ist eine Gruppe der Ordnung p^α für ein $\alpha \geq 0$.
- Eine *p-Untergruppe* einer Gruppe G ist eine Untergruppe, die eine p-Gruppe ist.
- Sei G endlich mit $|G| = p^\alpha m$ und $p \nmid m$. Eine *p-Sylowgruppe* von G ist eine p-Untergruppe der Ordnung p^α.

Eine p-Sylowgruppe ist also eine p-Untergruppe von größtmöglicher Ordnung, denn nach Lagrange kann es keine Untergruppe der Ordnung p^β mit $\beta > \alpha$ geben. Ist $P \leq G$ eine p-Sylowgruppe und $g \in G$, so ist auch gPg^{-1} eine p-Sylowgruppe, denn die Konjugation $x \mapsto gxg^{-1}$ ist ein Isomorphismus $G \to G$ und bildet P bijektiv auf die Untergruppe gPg^{-1} ab.

Satz 1.12.12 (Sylow): Sei G eine endliche Gruppe mit $|G| = p^\alpha m$, wobei p eine Primzahl ist und $p \nmid m$.
1. Es gibt eine p-Sylowgruppe in G.
2. Ist P eine p-Sylowgruppe und $Q \leq G$ eine p-Untergruppe, so existiert ein $g \in G$ mit $Q \leq gPg^{-1}$. Insbesondere sind je zwei p-Sylowgruppen zueinander konjugiert, d.h. sind P, P' zwei p-Sylowgruppen, so gibt es ein $g \in G$ mit $gPg^{-1} = P'$.
3. Die Anzahl n_p der p-Sylowgruppen von G erfüllt
$$n_p \equiv 1 \bmod p \quad \text{und} \quad n_p \mid m.$$

Das sind die *Sätze von Sylow*. Sie sind ein typisches Ergebnis der Strukturtheorie von Gruppen und sehr nützlich, um „kleine“ Gruppen zu verstehen. Wir beweisen sie in dieser Vorlesung nicht. Für $\alpha \geq 1$ folgt der Satz von Cauchy aus dem ersten Teil: Ist $y \neq 1$ in einer p-Sylowgruppe P, so ist $|y| = p^\beta$ mit $\beta \geq 1$ nach Korollar 1.12.3, und $x = y^{p^{\beta-1}}$ hat die Ordnung p.

Eine wichtige Folgerung aus dem zweiten Teil ist: Eine p-Sylowgruppe P ist genau dann ein Normalteiler, wenn $n_p = 1$ ist. Ist nämlich $n_p = 1$, so ist $gPg^{-1} = P$ für alle $g \in G$, da gPg^{-1} wieder eine p-Sylowgruppe ist. Ist umgekehrt $P \trianglelefteq G$, so ist jede p-Sylowgruppe von der Form $gPg^{-1} = P$.

Gruppen der Ordnung pq

Als Anwendung bestimmen wir alle Gruppen, deren Ordnung das Produkt zweier verschiedener Primzahlen ist. Wir brauchen dazu ein Lemma.

Lemma 1.12.13: Seien $P, Q \trianglelefteq G$ Normalteiler mit $P \cap Q = \{1\}$. Dann gilt $xy = yx$ für alle $x \in P$ und $y \in Q$.

Beweis. Wir betrachten $z = xyx^{-1}y^{-1}$. Einerseits ist $z = (xyx^{-1})y^{-1} \in Q$, da Q normal ist. Andererseits ist $z = x(yx^{-1}y^{-1}) \in P$, da P normal ist. Also ist $z \in P \cap Q = \{1\}$, d.h. $xyx^{-1}y^{-1} = 1$ und damit $xy = yx$. ∎

Satz 1.12.14: Seien $p < q$ Primzahlen und G eine Gruppe der Ordnung pq.
1. Ist $p \nmid q - 1$, so ist G zyklisch, also $G \cong (\mathbb{Z}/pq\mathbb{Z}, +)$.
2. Ist $p = 2$, so ist $G \cong (\mathbb{Z}/2q\mathbb{Z}, +)$ oder $G \cong D_{2q}$.

Beweis. Nach dem ersten Sylowsatz gibt es Untergruppen $P, Q \leq G$ mit $|P| = p$ und $|Q| = q$. Nach Korollar 1.12.5 sind beide zyklisch, etwa $P = \langle x \rangle$ und $Q = \langle y \rangle$. Außerdem ist $P \cap Q = \{1\}$, denn $P \cap Q$ ist eine Untergruppe von P und von Q, ihre Ordnung teilt also p und q und ist daher 1.

Für die Anzahl der q-Sylowgruppen gilt nach dem dritten Sylowsatz $n_q \equiv 1 \bmod q$ und $n_q \mid p$. Wegen $n_q \leq p < q$ folgt $n_q = 1$, d.h. Q ist die einzige q-Sylowgruppe und $Q \trianglelefteq G$. Für die p-Sylowgruppen gilt $n_p \mid q$, also $n_p = 1$ oder $n_p = q$, und außerdem $n_p \equiv 1 \bmod p$.

Wir betrachten zunächst den Fall $P \trianglelefteq G$, also $n_p = 1$. Dann gilt nach Lemma 1.12.13 $xy = yx$. Damit ist $(xy)^n = x^n y^n$ für alle n. Ist $(xy)^n = 1$, so ist $x^n = y^{-n} \in P \cap Q = \{1\}$, also $x^n = 1$ und $y^n = 1$. Dann teilen p und q die Zahl n, also auch pq. Somit hat xy die Ordnung pq, und $G = \langle xy \rangle$ ist zyklisch.

1. Ist $p \nmid q - 1$, so ist $q \not\equiv 1 \bmod p$. Also kann n_p nicht q sein, und es folgt $n_p = 1$. Nach dem eben behandelten Fall ist G zyklisch.
2. Sei $p = 2$. Da Q normal ist, liegt xyx^{-1} in Q, also $xyx^{-1} = y^k$ für ein $k \in \{0, \ldots, q-1\}$. Wegen $x^2 = 1$ folgt
$$y = x^2 y x^{-2} = x y^k x^{-1} = \left(xyx^{-1}\right)^k = y^{k^2},$$
also $y^{k^2-1} = 1$ und $q \mid k^2 - 1 = (k-1)(k+1)$. Da q prim ist, gilt $k \equiv 1$ oder $k \equiv -1 \bmod q$. Ist $k \equiv 1$, so vertauschen x und y, und wie oben hat xy die Ordnung $2q$, also ist G zyklisch. Ist $k \equiv -1$, so gilt $xyx^{-1} = y^{-1}$, also $xy = y^{-1}x$. Die Elemente y und x erfüllen damit die Relationen $r^q = 1$, $s^2 = 1$ und $sr = r^{-1}s$ der Diedergruppe D_{2q} (Definition 1.2.1). Außerdem erzeugen sie G: Die Ordnung von $\langle x, y \rangle$ ist nach Lagrange durch 2 und q teilbar, also gleich $2q$. Nach Satz 1.4.7 gibt es einen surjektiven Homomorphismus $D_{2q} \to G$ mit $r \mapsto y$ und $s \mapsto x$, und wegen $\left|D_{2q}\right| = 2q = |G|$ ist er ein Isomorphismus. ∎

© 2026 Thomas Kahle

Beispiel 1.12.15: Für $p = 3$ und $q = 5$ ist $3 \nmid 4$. Also ist $(\mathbb{Z}/15\mathbb{Z}, +)$ bis auf Isomorphie die einzige Gruppe der Ordnung 15.

Für $p = 2$ und $q = 3$ erhalten wir die in Abschnitt 1.4 angekündigte Klassifikation der Gruppen der Ordnung 6.

Korollar 1.12.16: Jede Gruppe der Ordnung 6 ist isomorph zu $(\mathbb{Z}/6\mathbb{Z}, +)$ oder zu S_3. Insbesondere ist jede nicht-abelsche Gruppe der Ordnung 6 isomorph zu S_3.

Beweis. Nach Satz 1.12.14 ist $G \cong \mathbb{Z}/6\mathbb{Z}$ oder $G \cong D_6$, und nach Beispiel 1.4.8 ist $D_6 \cong S_3$. Da $\mathbb{Z}/6\mathbb{Z}$ abelsch ist und S_3 nicht, sind diese beiden Gruppen nicht isomorph. ∎

Allgemein gilt: Ist $p \mid q - 1$, so gibt es bis auf Isomorphie genau eine nicht-abelsche Gruppe der Ordnung pq; zusammen mit $\mathbb{Z}/pq\mathbb{Z}$ sind das alle Gruppen der Ordnung pq. Für $p = 2$ ist diese nicht-abelsche Gruppe die Diedergruppe D_{2q}. Man kann zeigen, dass jede Gruppe der Ordnung pq aus ihren Untergruppen P und Q als sogenanntes *semidirektes Produkt* entsteht. Das ist eine sehr starke Einschränkung an die möglichen Gruppenstrukturen. Diese Aussagen beweisen wir hier nicht.

1.13 Die Isomorphiesätze

Die Isomorphiesätze sind Werkzeuge, um Quotienten von Gruppen mit anderen Gruppen zu identifizieren. Der erste fasst zusammen, was wir bei der Konstruktion von Quotienten schon gesehen haben (siehe Abschnitt 1.11).

Satz 1.13.1 (Erster Isomorphiesatz): Sei $\varphi: G \to H$ ein Homomorphismus von Gruppen. Dann ist $\ker \varphi$ ein Normalteiler von G, und es gilt

$$G/\ker \varphi \cong \operatorname{im}(\varphi) = \varphi(G).$$

Insbesondere ist φ genau dann injektiv, wenn $\ker \varphi = \{1\}$ ist, und es gilt $|G : \ker \varphi| = |\varphi(G)|$.

Beweis. Im Wesentlichen haben wir das schon gesehen: Die Quotientengruppe $G/\ker \varphi$ ist gerade die Gruppe der Fasern von φ, und die Fasern stehen in Bijektion mit den Elementen des Bildes. Wir führen das Argument der Vollständigkeit halber noch einmal aus. Sei $K := \ker \varphi$.

Für $g \in G$ und $k \in K$ gilt $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$, also $gKg^{-1} \subseteq K$ für alle $g \in G$. Damit ist K ein Normalteiler.

Für $g, g' \in G$ gilt

$$\varphi(g) = \varphi(g') \iff \varphi(g^{-1}g') = 1 \iff g^{-1}g' \in K \iff gK = g'K.$$

Von links nach rechts gelesen zeigt das, dass die Abbildung

$$\overline{\varphi}\colon G/K \to \varphi(G), \quad gK \mapsto \varphi(g)$$

wohldefiniert ist, und von rechts nach links, dass sie injektiv ist. Sie ist offensichtlich surjektiv, und wegen $\overline{\varphi}(gK \cdot g'K) = \overline{\varphi}(gg'K) = \varphi(gg') = \varphi(g)\varphi(g')$ ist sie ein Homomorphismus, also ein Isomorphismus.

Ist $K = \{1\}$, so liefert die Äquivalenz oben $\varphi(g) = \varphi(g') \Rightarrow g^{-1}g' = 1 \Rightarrow g = g'$, d.h. φ ist injektiv. Ist umgekehrt φ injektiv, so ist 1 das einzige Element mit Bild $\varphi(1) = 1$. Schließlich ist $|G\colon K|$ die Anzahl der Nebenklassen von K, also $|G\colon K| = |G/K| = |\varphi(G)|$. ∎

In der linearen Algebra kann man die Dimensionsformel

$$\dim V = \dim \ker f + \dim \operatorname{im} f$$

für eine lineare Abbildung $f\colon V \to W$ mit Hilfe des Isomorphismus $V/\ker f \cong \operatorname{im} f$ beweisen, denn $\dim(V/\ker f) = \dim V - \dim \ker f$. Der erste Isomorphiesatz ist das gruppentheoretische Gegenstück dazu. Für endliche Gruppen liefert er zusammen mit dem Satz von Lagrange (siehe Satz 1.12.1) die Formel $|G| = |\ker \varphi| \cdot |\varphi(G)|$.

Produkte von Untergruppen

Für den zweiten Isomorphiesatz brauchen wir eine Technik, um aus zwei Untergruppen eine neue zu bilden. Seien $H, K \leq G$ Untergruppen einer Gruppe G. Wir betrachten die Menge der Produkte

$$HK := \{hk\colon h \in H, k \in K\}.$$

Wann ist HK eine Untergruppe von G? Im Allgemeinen ist das nicht der Fall.

Übung. Zeigen Sie, dass für $H = \langle(12)\rangle$ und $K = \langle(13)\rangle$ in S_3 die Menge HK vier Elemente hat und daher keine Untergruppe von S_3 ist.

Für endliche Untergruppen kann man die Größe von HK immer bestimmen.

Lemma 1.13.2: Seien $H, K \leq G$ endliche Untergruppen. Dann gilt

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Beweis. Die Menge HK ist die Vereinigung der Linksnebenklassen hK mit $h \in H$. Jede dieser Nebenklassen hat $|K|$ Elemente, und verschiedene Nebenklassen sind disjunkt. Es bleibt zu zählen, wie viele der Nebenklassen hK, $h \in H$, verschieden sind. Für $h, h' \in H$ gilt

$$hK = h'K \iff h^{-1}h' \in K \iff h^{-1}h' \in H \cap K \iff h(H \cap K) = h'(H \cap K),$$

© 2026 Thomas Kahle

wobei wir im mittleren Schritt $h^{-1}h' \in H$ benutzt haben. Also gibt es genau so viele verschiedene Nebenklassen hK wie Nebenklassen von $H \cap K$ in H, nach dem Satz von Lagrange (siehe Satz 1.12.1) also $|H|/|H \cap K|$ viele. Damit folgt die Formel. ■

Proposition 1.13.3: Seien $H, K \leq G$. Dann gilt

$$HK \leq G \iff HK = KH.$$

Achtung! Die Gleichung $HK = KH$ bezieht sich auf Mengen. Sie bedeutet *nicht*, dass $hk = kh$ für alle $h \in H$ und $k \in K$ gilt, sondern nur, dass sich jedes Produkt hk auch als ein Produkt $k'h'$ mit $k' \in K$, $h' \in H$ schreiben lässt und umgekehrt.

Beweis. „$\Longleftarrow$“: Es ist $1 = 1 \cdot 1 \in HK$, also $HK \neq \varnothing$. Nach dem Untergruppenkriterium (siehe Abschnitt 1.6) genügt es, für $a, b \in HK$ zu zeigen, dass $ab^{-1} \in HK$ ist. Sei $a = h_1k_1$ und $b = h_2k_2$ mit $h_i \in H$, $k_i \in K$. Dann ist $b^{-1} = k_2^{-1}h_2^{-1}$ und

$$ab^{-1} = h_1 \underbrace{(k_1k_2^{-1})}_{\in K} \underbrace{h_2^{-1}}_{\in H}.$$

Das Produkt $(k_1k_2^{-1})h_2^{-1}$ liegt in $KH = HK$, lässt sich also als h_3k_3 mit $h_3 \in H$, $k_3 \in K$ schreiben. Damit ist $ab^{-1} = (h_1h_3)k_3 \in HK$.

„$\Longrightarrow$“: Sei $HK \leq G$. Wegen $H, K \subseteq HK$ und da HK unter Produkten abgeschlossen ist, gilt $KH \subseteq HK$. Sei umgekehrt $hk \in HK$. Da HK eine Untergruppe ist, liegt auch $a := (hk)^{-1}$ in HK, also $a = h'k'$ für gewisse $h' \in H$, $k' \in K$. Dann ist $hk = a^{-1} = k'^{-1}h'^{-1} \in KH$. Also gilt $HK \subseteq KH$. ■

Eine wichtige hinreichende Bedingung liefert der Normalisator. Zur Erinnerung: $N_G(K) = \{g \in G : gKg^{-1} = K\}$ (siehe Abschnitt 1.7).

Korollar 1.13.4: Seien $H, K \leq G$ mit $H \leq N_G(K)$. Dann ist $HK \leq G$. Insbesondere ist $HK \leq G$ für alle $H \leq G$, falls $K \trianglelefteq G$ ist (d.h. falls $N_G(K) = G$ ist).

Beweis. Wir zeigen $HK = KH$ und wenden Proposition 1.13.3 an. Seien $h \in H$ und $k \in K$. Wegen $h \in N_G(K)$ ist $hkh^{-1} \in K$, also

$$hk = \underbrace{hkh^{-1}}_{\in K} h \in KH.$$

Das zeigt $HK \subseteq KH$. Da $N_G(K)$ eine Untergruppe ist, ist auch $h^{-1} \in N_G(K)$, und analog folgt aus $kh = h(h^{-1}kh)$ die Inklusion $KH \subseteq HK$. ■

Der zweite Isomorphiesatz

Satz 1.13.5 (Zweiter Isomorphiesatz, Diamantensatz): Sei G eine Gruppe und seien $A, B \leq G$ mit $A \leq N_G(B)$. Dann ist $AB \leq G$, und es gilt
- $B \trianglelefteq AB$,
- $A \cap B \trianglelefteq A$,

und

$$AB/B \cong A/(A \cap B).$$

Die Idee dahinter ist folgende: Wir würden gerne „A/B“ bilden, obwohl das für zwei beliebige Untergruppen $A, B \leq G$ gar nicht definiert ist (B muss weder in A liegen noch normal sein). Es gibt zwei Arten, das zu reparieren:
1. Man vergrößert A zu AB, bis B darin ein Normalteiler ist, und bildet AB/B.
2. Man verkleinert B zu $A \cap B$, bis es ein Normalteiler in A ist, und bildet $A/(A \cap B)$.

Der Satz sagt, dass beide Möglichkeiten isomorphe Ergebnisse liefern.

Beweis. Nach Korollar 1.13.4 ist AB eine Untergruppe von G. Nach Voraussetzung ist $A \leq N_G(B)$, und trivialerweise ist $B \leq N_G(B)$. Da $N_G(B)$ eine Untergruppe ist, folgt $AB \leq N_G(B)$, d.h. jedes Element von AB normalisiert B. Also ist $B \trianglelefteq AB$, und der Quotient AB/B kann gebildet werden.

Wir betrachten

$$\varphi\colon A \to AB/B, \quad a \mapsto aB.$$

(Man denke an $aB = (a \cdot 1)B$ mit $1 \in B$, d.h. $a \in AB$.) Die Abbildung φ ist ein Homomorphismus, denn sie ist die Einschränkung der kanonischen Projektion $AB \to AB/B$ auf A. Ausgeschrieben: $\varphi(a_1a_2) = (a_1a_2)B = a_1B \cdot a_2B = \varphi(a_1)\varphi(a_2)$, wobei wir benutzt haben, dass B normal in AB ist.

Die Abbildung φ ist surjektiv: Jedes Element von AB/B hat die Form abB mit $a \in A$, $b \in B$, und es ist $abB = aB = \varphi(a)$. Für den Kern gilt

$$\ker\varphi = \{a \in A\colon aB = 1B\} = \{a \in A\colon a \in B\} = A \cap B.$$

Nach dem ersten Isomorphiesatz (Satz 1.13.1) ist daher $A \cap B$ ein Normalteiler in A und $A/(A \cap B) \cong AB/B$. ∎

Wo ist der Diamant? Zeichnet man die beteiligten Untergruppen im Untergruppenverband (siehe Abschnitt 1.10) von G auf, so bilden AB, A, B und $A \cap B$ eine Raute. Der Satz sagt, dass die Quotienten zu den beiden gegenüberliegenden, hervorgehobenen Kanten isomorph sind.

© 2026 Thomas Kahle

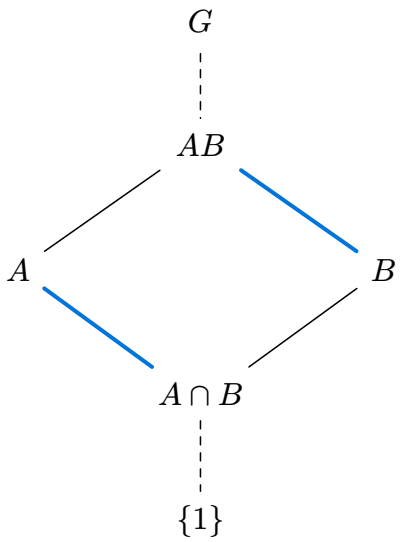


Abbildung 5: Der Diamant des zweiten Isomorphiesatzes. Die Quotienten AB/B und $A/(A \cap B)$ zu den blauen Kanten sind isomorph.

Der dritte und vierte Isomorphiesatz

Satz 1.13.6 (Dritter Isomorphiesatz): Sei G eine Gruppe und seien $H, K \trianglelefteq G$ Normalteiler mit $H \leq K$. Dann gilt $H \trianglelefteq K$, $K/H \trianglelefteq G/H$ und

$$(G/H)/(K/H) \cong G/K.$$

Man kann sich den Satz als „Kürzen“ von Brüchen merken.

Beweis. Dass $H \trianglelefteq K$ ist, ist klar, denn es gilt $kHk^{-1} = H$ sogar für alle $k \in G$. Wir betrachten

$$\varphi\colon G/H \to G/K, \quad gH \mapsto gK.$$

Diese Abbildung ist auf Repräsentanten definiert, wir müssen also prüfen, dass sie wohldefiniert ist. Ist $g' \in gH$ ein anderer Repräsentant, so existiert ein $h \in H$ mit $g' = gh$. Wegen $H \leq K$ ist $h \in K$ und damit $g'K = ghK = gK$, also $\varphi(g'H) = \varphi(gH)$. Die Abbildung φ ist ein Homomorphismus, denn

$$\varphi(gH \cdot g'H) = \varphi(gg'H) = gg'K = gK \cdot g'K = \varphi(gH)\varphi(g'H),$$

und sie ist surjektiv, da jedes $g \in G$ als Repräsentant gewählt werden kann. Für den Kern gilt

$$\ker\varphi = \{gH \in G/H\colon gK = 1K\} = \{gH \in G/H\colon g \in K\} = K/H.$$

Als Kern eines Homomorphismus ist K/H ein Normalteiler von G/H, und der erste Isomorphiesatz (Satz 1.13.1) liefert $(G/H)/(K/H) \cong G/K$. ∎

Der vierte Isomorphiesatz beschreibt die Untergruppen eines Quotienten G/N. Sei dazu $\pi\colon G \to G/N$, $g \mapsto gN$ die kanonische Projektion.

Satz 1.13.7 (Vierter Isomorphiesatz, Korrespondenzsatz): Sei $N \trianglelefteq G$ ein Normalteiler einer Gruppe G. Dann ist

$$\{A \leq G \colon N \leq A\} \to \left\{\overline{A} \leq G/N\right\}, \quad A \mapsto A/N = \pi(A)$$

eine Bijektion zwischen den Untergruppen von G, die N enthalten, und den Untergruppen von G/N. Die Umkehrabbildung ist $\overline{A} \mapsto \pi^{-1}\left(\overline{A}\right)$. Für $N \leq A, B \leq G$ schreiben wir $\overline{A} = A/N$ und $\overline{B} = B/N$. Dann gilt:

1. $A \leq B \iff \overline{A} \leq \overline{B}$.
2. Ist $A \leq B$, so gilt $|B \colon A| = \left|\overline{B} \colon \overline{A}\right|$.
3. $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$.
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$.
5. $A \trianglelefteq G \iff \overline{A} \trianglelefteq \overline{G} = G/N$.

Man nennt $A = \pi^{-1}\left(\overline{A}\right)$ auch das *vollständige Urbild* von $\overline{A}$.

Beweis. Für $N \leq A \leq G$ ist $\pi(A) = \{aN \colon a \in A\} = A/N$ als Bild eines Homomorphismus eine Untergruppe von G/N. Für $\overline{A} \leq G/N$ ist das Urbild $\pi^{-1}\left(\overline{A}\right)$ eine Untergruppe von G (prüfen Sie das nach), und es enthält $N = \pi^{-1}(\{1\})$. Die beiden Abbildungen sind invers zueinander: Da π surjektiv ist, gilt $\pi\left(\pi^{-1}\left(\overline{A}\right)\right) = \overline{A}$. Umgekehrt ist $A \subseteq \pi^{-1}(\pi(A))$, und ist $g \in \pi^{-1}(\pi(A))$, so ist $gN = aN$ für ein $a \in A$, also $g \in aN \subseteq A$ wegen $N \leq A$. Damit ist auch $\pi^{-1}(\pi(A)) = A$.

1. Bilder und Urbilder erhalten Inklusionen, also erhalten beide Abbildungen der Bijektion die Inklusion.
2. Die Abbildung $bA \mapsto \pi(b)\overline{A}$ von den Nebenklassen von A in B auf die Nebenklassen von $\overline{A}$ in $\overline{B}$ ist wohldefiniert und surjektiv. Sie ist injektiv, denn aus $\pi(b)\overline{A} = \pi(b')\overline{A}$ folgt $\pi(b^{-1}b') \in \overline{A}$, also $b^{-1}b' \in \pi^{-1}\left(\overline{A}\right) = A$ und damit $bA = b'A$.
3. und 4. Nach 1. ist die Bijektion mit ihrer Umkehrung verträglich mit der Inklusion. Die Untergruppe $\langle A, B\rangle$ ist die kleinste Untergruppe, die A und B enthält (sie enthält auch N), und $A \cap B$ ist die größte Untergruppe, die in A und B enthalten ist. Solche Eigenschaften, die nur von der Inklusion abhängen, bleiben unter einer inklusionserhaltenden Bijektion erhalten.
5. Für $g \in G$ gilt $\pi(gAg^{-1}) = \pi(g)\overline{A}\pi(g)^{-1}$. Mit der Bijektivität folgt $gAg^{-1} = A \iff \pi(g)\overline{A}\pi(g)^{-1} = \overline{A}$, und da π surjektiv ist, durchläuft $\pi(g)$ dabei ganz G/N. ∎

Der Korrespondenzsatz sagt also, dass der Untergruppenverband von G/N genau der Teil des Untergruppenverbands von G oberhalb von N ist (siehe Abschnitt 1.10). Solche Bijektionen zwischen partiell geordneten Mengen, die die Ordnung in beiden Richtungen erhalten, sind sehr starke Beziehungen. Verwandte, etwas schwächere Beziehungen zwischen partiell geordneten Mengen, die die Ordnung *umkehren*, heißen *Galoisverbindungen*. Eine solche werden wir am Ende der Vorlesung im Hauptsatz der Galoistheorie kennenlernen.

© 2026 Thomas Kahle

Als Faustregel kann man sich merken: Wenn man Quotienten sieht, denkt man an die Isomorphiesätze.

1.14 Ausblick: Das Hölderprogramm

Die wichtigste zentrale Frage der Gruppentheorie lautet: Was sind alle Gruppen? Kann man alle Gruppen klassifizieren, bzw. auflisten? In voller Allgemeinheit ist das hoffnungslos, aber es gibt Teilergebnisse in diese Richtung.

- Eine endliche Gruppe von Primzahlordnung ist zyklisch. Das haben wir als Folgerung aus dem Satz von Lagrange gesehen (siehe Abschnitt 1.12).
- Endlich erzeugte abelsche Gruppen sind klassifiziert: Jede solche Gruppe ist isomorph zu

$$\mathbb{Z}^n \times \mathbb{Z}_{q_1} \times \ldots \times \mathbb{Z}_{q_s},$$

wobei $\mathbb{Z}^n = (\mathbb{Z}, +)^n$ ist und die $\mathbb{Z}_{q_i}$ zyklische Gruppen von Primzahlpotenzordnung sind. Dabei sind n und die q_i (bis auf Reihenfolge) eindeutig bestimmt.

Definition 1.14.1: Eine Gruppe $G \neq \{1\}$ heißt *einfach*, falls $\{1\}$ und G ihre einzigen Normalteiler sind.

Einfache Gruppen sind die Bausteine der Gruppentheorie. Ist nämlich $N \trianglelefteq G$ ein Normalteiler mit $\{1\} \neq N \neq G$, so kann man G aus den „kleineren“ Gruppen N und G/N zusammengesetzt denken. Umgekehrt kann man fragen: Gegeben zwei Gruppen A und B, finde eine Gruppe G mit $B \trianglelefteq G$ und $A \cong G/B$. Dann ist G aus A und B zusammengesetzt. Allerdings gibt es dafür oft viele Möglichkeiten. Zum Beispiel erhält man für $A = B = \mathbb{Z}_2$ sowohl $G = \mathbb{Z}_4$ als auch $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Setzt man auf diese Weise n Kopien von $\mathbb{Z}_2$ zusammen, so erhält man sehr schnell sehr viele nicht-isomorphe Gruppen der Ordnung 2^n.

Wenigstens könnte man versuchen, die Bausteine zu klassifizieren, also die endlichen einfachen Gruppen. Dies ist in einer gewaltigen Gemeinschaftsleistung von ca. 1955 bis 2004 gelungen, in Hunderten von Arbeiten mit insgesamt zehntausenden Seiten. Das Ergebnis ist die Klassifikation der endlichen einfachen Gruppen: Jede endliche einfache Gruppe gehört zu einer von 18 unendlichen Familien oder ist eine von 26 (oder 27, je nach Zählweise) *sporadischen* Gruppen. Das ist eine der größten Errungenschaften der Mathematik, und der Satz ist extrem nützlich.

Beispiel 1.14.2: Beispiele endlicher einfacher Gruppen sind:
- die zyklischen Gruppen $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p,
- die alternierenden Gruppen A_n für $n \geq 5$, d.h. die Untergruppen der geraden Permutationen in S_n,

thomas.kahle@ovgu.de

- die Gruppen

$$\mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/Z(\mathrm{SL}_n(\mathbb{F}_q))$$

für $n \geq 2$ und endliche Körper $\mathbb{F}_q$, mit Ausnahme der beiden Fälle $n = 2$, $q \in \{2, 3\}$. Dabei ist $\mathrm{SL}_n(\mathbb{F}_q)$ die Gruppe der $n \times n$-Matrizen mit Determinante 1 über $\mathbb{F}_q$ und $Z(\cdot)$ ihr Zentrum (siehe Abschnitt 1.7).

Wie setzt sich eine endliche Gruppe aus einfachen Gruppen zusammen? Dazu studiert man *Kompositionsreihen*, d.h. Ketten von Untergruppen

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G,$$

in denen jede Gruppe ein Normalteiler in der nächsten ist und alle Faktoren G_i/G_{i-1} einfach sind. Jede endliche Gruppe besitzt eine Kompositionsreihe.

Satz 1.14.3 (Jordan–Hölder): Sei G eine endliche Gruppe. Die Faktoren G_i/G_{i-1} einer Kompositionsreihe von G sind bis auf Isomorphie und Reihenfolge eindeutig durch G bestimmt.

Den Beweis führen wir hier nicht. Der „Plan“, alle endlichen Gruppen zu klassifizieren, indem man erst die einfachen Gruppen klassifiziert und dann versteht, wie sie sich zusammensetzen lassen, heißt *Hölderprogramm*. Der erste Teil ist mit der Klassifikation der endlichen einfachen Gruppen erledigt, der zweite ist weit offen.

Es gibt noch viele weitere Themen der Gruppentheorie, zum Beispiel:
- *Lie-Gruppen*, d.h. Gruppen, die auch Mannigfaltigkeiten sind, auf denen also Differentialgeometrie funktioniert. Sie sind unter anderem in der theoretischen Physik wichtig.
- Gruppenwirkungen und *Darstellungstheorie*.
- *Kombinatorische Gruppentheorie*, zum Beispiel Coxetergruppen.
- *Geometrische Gruppentheorie*, die Gruppen selbst als geometrische Räume auffasst.
- und vieles mehr.

2 Ringtheorie

Ringe haben zwei Verknüpfungen, eine Addition und eine Multiplikation, die durch das Distributivgesetz miteinander verbunden sind. Das Vorbild sind die ganzen Zahlen. Wir nutzen die Ringtheorie unter anderem, um Begriffe wie *Primzahl* und *Faktorisierung* auf viel größere Klassen von Objekten als nur Zahlen auszudehnen. Die Ringtheorie ist außerdem die Grundlage der algebraischen Geometrie. Diese beschäftigt sich mit Lösungsmengen von Polynomgleichungen, und Polynome bilden Ringe.

2.1 Ringe und Grundbegriffe

Definition 2.1.1: Ein *Ring* ist eine Menge R mit zwei Verknüpfungen

$$+\colon R \times R \to R \quad \text{(Addition)} \quad \text{und} \quad \cdot\colon R \times R \to R \quad \text{(Multiplikation)},$$

sodass gilt:

1. $(R, +)$ ist eine abelsche Gruppe.
2. Die Multiplikation ist assoziativ: $(ab)c = a(bc)$ für alle $a, b, c \in R$.
3. Es gelten die Distributivgesetze
$$(a+b)c = ac + bc \quad \text{und} \quad a(b+c) = ab + ac \quad \text{für alle } a, b, c \in R.$$
4. Es gibt ein Element $1 \in R$ mit $1a = a1 = a$ für alle $a \in R$, die *Eins* von R.

Der Ring heißt *kommutativ*, falls die Multiplikation kommutativ ist.

Wir verwenden die folgenden Konventionen: Das Produkt schreiben wir als $ab := a \cdot b$, und es gilt Punktrechnung vor Strichrechnung, also $a + bc := a + (bc)$. Das neutrale Element der Addition heißt $0 \in R$ und das additive Inverse von a heißt $-a$. Wir schreiben $a - b := a + (-b)$.

Achtung! In der Literatur wird die Existenz einer Eins nicht immer gefordert. Ringe im Sinne von Definition 2.1.1 heißen dann *Ringe mit Eins* oder *unitäre Ringe*, und Ringe ohne die Forderung 4. werden manchmal *Rng* genannt (das „i“ fehlt, wie die Identität). In diesem Skript haben Ringe immer eine Eins.

Inverse bezüglich der Multiplikation werden nicht vorausgesetzt. Die Kommutativität der Addition ist in Definition 2.1.1 sogar überflüssig, wie die folgende Übung zeigt.

Übung. Sei R eine Menge mit Verknüpfungen $+$ und $\cdot$, die alle Axiome eines Rings erfüllt, außer dass $(R, +)$ nur als Gruppe (nicht als abelsche Gruppe) vorausgesetzt wird. Zeigen Sie, dass $(R, +)$ abelsch ist. *Hinweis:* Berechnen Sie $(1+1)(a+b)$ auf zwei Weisen.

Definition 2.1.2: Ein *Divisionsring* (oder *Schiefkörper*) ist ein Ring mit $1 \neq 0$, in dem jedes $a \in R \setminus \{0\}$ ein multiplikatives Inverses hat. Ein *Körper* ist ein kommutativer Divisionsring.

Beispiel 2.1.3:

- Der *Nullring* $R = \{0\}$ ist ein kommutativer Ring, in dem $1 = 0$ gilt. Umgekehrt folgt aus $1 = 0$ schon $a = 1a = 0a = 0$ für alle a (siehe Proposition 2.1.4), also $R = \{0\}$.

thomas.kahle@ovgu.de

- Die ganzen Zahlen $\mathbb{Z}$ bilden einen kommutativen Ring.
- Bekannte Körper sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p (siehe Beispiel 2.1.7).
- Die *Quaternionen* $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ mit den Rechenregeln $i^2 = j^2 = k^2 = ijk = -1$ bilden einen Divisionsring, der kein Körper ist, denn es gilt $ij = k = -ji$.
- *Ringe aus Abbildungen:* Sei $X \neq \varnothing$ eine Menge und A ein Ring. Dann ist
$$R = \{f : X \to A\}$$
die Menge aller Abbildungen von X nach A ein Ring mit den punktweisen Verknüpfungen
$$(f + g)(x) := f(x) + g(x), \quad (fg)(x) := f(x)g(x),$$
wobei rechts in A gerechnet wird. Die Eins ist die konstante Abbildung $x \mapsto 1$. Es ist R genau dann kommutativ, wenn A kommutativ ist.
- Sei V ein K-Vektorraum der Dimension n. Die linearen Abbildungen
$$\mathrm{End}(V) = \{f : V \to V \text{ linear}\} \cong K^{n \times n}$$
bilden mit der Addition und der Komposition (bzw. dem Matrixprodukt) einen Ring. Für $n \geq 2$ ist er nicht kommutativ.
- Stetige Funktionen bilden Ringe, z.B. die stetigen Funktionen $[0, 1] \to \mathbb{R}$ mit punktweiser Addition und Multiplikation. Dass Summen und Produkte stetiger Funktionen stetig sind, folgt aus den Grenzwertsätzen der Analysis.

Die geraden ganzen Zahlen $2\mathbb{Z}$ erfüllen alle Ringaxiome bis auf die Existenz einer Eins. Sie sind also nach unserer Konvention kein Ring. Ebenso ist jede abelsche Gruppe $R \neq \{0\}$ mit der trivialen Multiplikation $ab := 0$ ein Beispiel für einen „Ring ohne Eins“.

Proposition 2.1.4: Sei R ein Ring und $a, b \in R$. Dann gilt:
1. $0a = a0 = 0$.
2. $(-a)b = a(-b) = -(ab)$.
3. $(-a)(-b) = ab$.
4. Die Eins von R ist eindeutig.

Beweis.
1. Es ist $0a = (0 + 0)a = 0a + 0a$. Addition von $-(0a)$ liefert $0 = 0a$. Analog ist $a0 = 0$.
2. Es gilt $ab + (-a)b = (a + (-a))b = 0b = 0$ nach 1. Also ist $(-a)b$ das additive Inverse von ab. Analog für $a(-b)$.
3. Nach 2. ist $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

© 2026 Thomas Kahle

4. Das ist das gleiche Argument wie für das neutrale Element einer Gruppe (Proposition 1.1.9): Sind 1 und $1'$ Einsen, so ist $1 = 1 \cdot 1' = 1'$.

■

Abelsche Gruppen sind für sich genommen nicht so spannend. In der Ringtheorie geht es hauptsächlich um die Multiplikation, und hier gibt es zwei neue Phänomene: Manche Elemente sind multiplikativ invertierbar, manche nicht. Und aus $ab = 0$ folgt im Allgemeinen *nicht*, dass $a = 0$ oder $b = 0$ ist.

Definition 2.1.5: Sei R ein Ring.
1. Ein Element $a \in R$ heißt *Nullteiler*, falls ein $b \in R$ mit $b \neq 0$ existiert, sodass $ab = 0$ oder $ba = 0$ gilt.
2. Ein Element $u \in R$ heißt *Einheit*, falls ein $v \in R$ existiert mit $uv = vu = 1$. Die Menge aller Einheiten von R bildet mit der Multiplikation die *Einheitengruppe* von R, die mit R^* bezeichnet wird.

Ein paar Bemerkungen zu dieser Definition:
- Ist $R \neq \{0\}$, so ist 0 nach dieser Definition ein Nullteiler, denn $0 \cdot 1 = 0$ und $1 \neq 0$. Manche Autor*innen nennen nur $a \neq 0$ Nullteiler.
- Aus $ab = 0$ folgt im Allgemeinen nicht $ba = 0$. Man könnte also *Linksnullteiler* und *Rechtsnullteiler* unterscheiden. In kommutativen Ringen fällt das zusammen.
- Dass R^* eine Gruppe ist, prüft man leicht nach: Mit u und u' ist auch uu' eine Einheit, denn $(uu')(v'v) = 1 = (v'v)(uu')$, wenn v, v' die Inversen von u, u' sind. Assoziativität erbt man von R, das neutrale Element ist 1, und das Inverse v einer Einheit u ist selbst eine Einheit.
- Ein Nullteiler ist nie eine Einheit: Sei $ab = 0$ mit $b \neq 0$ und $a \in R^*$. Dann existiert a^{-1}, und es folgt
$$b = a^{-1}ab = a^{-1}0 = 0,$$
ein Widerspruch. Analog argumentiert man im Fall $ba = 0$.
- Insbesondere enthalten Körper keine Nullteiler außer 0. Ist K ein Körper, so ist $K^* = K \setminus \{0\}$.

Beispiel 2.1.6: Es ist $\mathbb{Z}^* = \{\pm 1\}$, und $\mathbb{Z}$ hat keine Nullteiler außer 0. Es gibt also Elemente, die weder Einheiten noch Nullteiler sind, zum Beispiel $2 \in \mathbb{Z}$.

Beispiel 2.1.7: Sei $n \geq 2$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ mit der Addition und Multiplikation von Restklassen ein kommutativer Ring. Seine Einheitengruppe ist

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \colon \mathrm{ggT}(a,n) = 1\},$$

und jede Nichteinheit ist ein Nullteiler. Dass die Restklassen $\overline{a}$ mit $\mathrm{ggT}(a,n) = 1$ invertierbar sind, haben wir in Abschnitt 1.1 mit dem Lemma von Bézout gesehen. Ist umgekehrt $\mathrm{ggT}(a,n) = d > 1$, so setzen wir $b := n/d$. Dann ist $0 < b < n$, also $\overline{b} \neq \overline{0}$, und

$$ab = n \cdot \frac{a}{d}$$

ist ein Vielfaches von n, also $\overline{a} \cdot \overline{b} = \overline{0}$. Damit ist $\overline{a}$ ein Nullteiler und nach obiger Bemerkung keine Einheit.

Ist p eine Primzahl, so ist $\mathrm{ggT}(a,p) = 1$ für alle $\overline{a} \neq \overline{0}$. Also ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, den man auch mit $\mathbb{F}_p$ bezeichnet.

Beispiel 2.1.8: Sei $D \in \mathbb{Q}$ keine Quadratzahl in $\mathbb{Q}$, d.h. $\sqrt{D} \notin \mathbb{Q}$. Wir betrachten

$$\mathbb{Q}\big(\sqrt{D}\big) = \big\{a + b\sqrt{D} \colon a, b \in \mathbb{Q}\big\} \subseteq \mathbb{C}.$$

- $\big(\mathbb{Q}\big(\sqrt{D}\big), +\big)$ ist eine abelsche Gruppe, sogar ein $\mathbb{Q}$-Vektorraum.
- $\mathbb{Q}\big(\sqrt{D}\big)$ ist abgeschlossen unter der Multiplikation, denn $\big(a + b\sqrt{D}\big)\big(c + d\sqrt{D}\big) = (ac + bdD) + (ad + bc)\sqrt{D}$.
- $\mathbb{Q}\big(\sqrt{D}\big) \setminus \{0\}$ ist eine multiplikative Gruppe, wie man durch Rationalmachen des Nenners sieht: Für $(a,b) \neq (0,0)$ ist

$$\frac{1}{a + b\sqrt{D}} = \frac{a - b\sqrt{D}}{\big(a + b\sqrt{D}\big)\big(a - b\sqrt{D}\big)} = \frac{a}{a^2 - b^2 D} - \frac{b}{a^2 - b^2 D}\sqrt{D}.$$

  Der Nenner $a^2 - b^2 D$ ist dabei nicht 0: Für $b = 0$ ist $a \neq 0$, und für $b \neq 0$ würde aus $a^2 = b^2 D$ folgen, dass $\sqrt{D} = \pm a/b \in \mathbb{Q}$ ist.

Also ist $\mathbb{Q}\big(\sqrt{D}\big)$ ein Körper, eine sogenannte *quadratische Erweiterung* von $\mathbb{Q}$. Man spricht „$\mathbb{Q}$ adjungiert Wurzel D“. Es ist der kleinste Teilkörper von $\mathbb{C}$, der $\mathbb{Q}$ und eine Nullstelle des Polynoms $x^2 - D$ enthält.

Definition 2.1.9: Ein kommutativer Ring R mit $1 \neq 0$, der keine Nullteiler außer 0 hat, heißt *Integritätsbereich*.

Zum Beispiel sind $\mathbb{Z}$ und jeder Körper Integritätsbereiche, und $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Integritätsbereich, wenn n eine Primzahl ist.

© 2026 Thomas Kahle

Proposition 2.1.10: Sei R ein Ring und seien $a, b, c \in R$, wobei a kein Nullteiler ist. Dann gilt

$$ab = ac \Longrightarrow b = c \quad \text{und} \quad ba = ca \Longrightarrow b = c.$$

Das heißt, man kann a kürzen, auch wenn a nicht invertierbar ist. Anders gesagt: Die Multiplikation mit a ist injektiv.

Beweis. Aus $ab = ac$ folgt $a(b - c) = 0$. Da a kein Nullteiler ist, folgt $b - c = 0$. Der zweite Teil geht genauso. ■

Die Proposition gilt insbesondere in Integritätsbereichen für alle $a \neq 0$, zum Beispiel in $\mathbb{Z}$: Ist $ab = ac$ für ganze Zahlen a, b, c mit $a \neq 0$, so gilt $b = c$.

Proposition 2.1.11: Jeder endliche Integritätsbereich ist ein Körper.

Beweis. Sei $a \in R$ mit $a \neq 0$. Die Abbildung $R \to R$, $x \mapsto ax$ ist nach Proposition 2.1.10 injektiv. Da R endlich ist, ist sie damit auch surjektiv. Also existiert ein $x \in R$ mit $ax = 1$, und da R kommutativ ist, ist x das Inverse von a. ■

Definition 2.1.12: Ein *Teilring* oder *Unterring* eines Rings R ist eine additive Untergruppe $S \subseteq R$, die unter der Multiplikation abgeschlossen ist und die 1 von R enthält.

Beispiel 2.1.13:

- $\mathbb{Z} \subseteq \mathbb{Q}$ ist ein Teilring.
- Für $n \neq \pm 1$ ist $n\mathbb{Z} \subseteq \mathbb{Z}$ kein Teilring, denn $1 \notin n\mathbb{Z}$. Es ist aber eine additive Untergruppe, die unter Multiplikation abgeschlossen ist. Wir werden sehen, dass $n\mathbb{Z}$ ein *Ideal* ist.
- **Achtung!** $\mathbb{Z}/n\mathbb{Z}$ ist kein Teilring von $\mathbb{Z}$ (es ist nicht einmal eine Teilmenge), sondern ein *Quotient*.
- Die stetigen Funktionen $[0, 1] \to \mathbb{R}$ bilden einen Teilring des Rings aller Funktionen $[0, 1] \to \mathbb{R}$. Ebenso bilden die differenzierbaren Funktionen einen Teilring der stetigen Funktionen, usw.

2.2 Polynomringe und Gruppenringe

Den Polynomring kennen Sie mit reellen oder komplexen Koeffizienten. Er kann auch mit Koeffizienten aus einem beliebigen Ring definiert werden.

Definition 2.2.1: Sei R ein kommutativer Ring und x eine Unbestimmte. Ein *Polynom* mit Koeffizienten in R ist eine formale Linearkombination

$$p = a_n x^n + \ldots + a_1 x + a_0$$

mit $n \geq 0$ und $a_i \in R$. Zwei Polynome sind gleich, wenn ihre Koeffizienten übereinstimmen (wobei fehlende Koeffizienten als 0 gelten). Ist $a_n \neq 0$, so heißt n der *Grad* $\deg(p)$ von p, $a_n x^n$ der *Leitterm* und a_n der *Leitkoeffizient*. Sind alle $a_i = 0$, so ist p das *Nullpolynom* und hat den Grad $-\infty$.

Die Menge dieser Polynome wird mit $R[x]$ bezeichnet. Mit der üblichen Addition und Multiplikation

$$\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i, \quad \left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k$$

bildet $R[x]$ einen kommutativen Ring, den *Polynomring* über R.

Die Ringaxiome für $R[x]$ rechnet man direkt nach. Die Eins ist das konstante Polynom 1. Die *konstanten Polynome* a_0 bilden einen Teilring von $R[x]$, den wir mit R identifizieren. In diesem Sinne ist $R \subseteq R[x]$.

Beispiel 2.2.2: Wir rechnen in $(\mathbb{Z}/4\mathbb{Z})[x]$. Seien $p = x^2 + \overline{2}x + \overline{1}$ und $q = x^3 + \overline{2}$. Dann ist

$$\begin{aligned} p + q &= x^3 + x^2 + \overline{2}x + \overline{3}, \\ pq &= x^5 + \overline{2}x^4 + x^3 + \overline{2}x^2 + \overline{0}x + \overline{2} = x^5 + \overline{2}x^4 + x^3 + \overline{2}x^2 + \overline{2}. \end{aligned}$$

In $(\mathbb{Z}/4\mathbb{Z})[x]$ passieren aber auch merkwürdige Dinge. Zum Beispiel ist

$$\left(\overline{2}x + \overline{1}\right)^2 = \overline{4}x^2 + \overline{4}x + \overline{1} = \overline{1}.$$

Das Polynom $\overline{2}x + \overline{1}$ vom Grad 1 ist also eine Einheit, und der Grad eines Produkts ist nicht die Summe der Grade.

Für viele algebraische Fragen, z.B. die Faktorisierung, machen die Koeffizienten einen Unterschied. So ist $x^2 + 1$ in $\mathbb{Z}[x]$ nicht als Produkt zweier Polynome vom Grad 1 darstellbar (es hat ja keine reelle Nullstelle). In $(\mathbb{Z}/2\mathbb{Z})[x]$ dagegen ist

$$\left(x + \overline{1}\right)^2 = x^2 + \overline{2}x + \overline{1} = x^2 + \overline{1},$$

denn $\overline{2} = \overline{0}$.

© 2026 Thomas Kahle

Proposition 2.2.3: Sei R ein Integritätsbereich und $p, q \in R[x] \setminus \{0\}$. Dann gilt:
1. $\deg(pq) = \deg(p) + \deg(q)$.
2. Die Einheiten von $R[x]$ sind die Einheiten von R, d.h. $(R[x])^* = R^*$.
3. $R[x]$ ist ein Integritätsbereich.

Beweis. Seien $a_n x^n$ und $b_m x^m$ die Leitterme von p und q. Dann ist $a_n b_m \neq 0$, da R keine Nullteiler außer 0 hat, und $a_n b_m x^{n+m}$ ist der Leitterm von pq. Daraus folgen 1. und 3.

Sei nun $p \in (R[x])^*$ und p^{-1} sein Inverses. Nach 1. gilt

$$0 = \deg(1) = \deg(pp^{-1}) = \deg(p) + \deg(p^{-1}).$$

Da beide Grade ≥ 0 sind, folgt $\deg(p) = \deg(p^{-1}) = 0$. Also sind p und p^{-1} Konstanten, d.h. Elemente von R, und damit ist $p \in R^*$. Umgekehrt ist jede Einheit von R auch eine Einheit von $R[x]$. ■

Beispiel 2.2.2 zeigt, dass die Voraussetzung, dass R ein Integritätsbereich ist, nicht weggelassen werden kann. Allgemein gilt:
- Hat R einen Nullteiler $a \neq 0$, so auch $R[x]$, denn die Konstante a ist auch in $R[x]$ ein Nullteiler.
- Ist $S \subseteq R$ ein Teilring, so ist $S[x] \subseteq R[x]$ ein Teilring. Zum Beispiel ist $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$.

Gruppenringe erweitern diese Idee noch. Sei G eine Gruppe und R ein kommutativer Ring. Wir wollen einen Ring konstruieren, der R als Teilring enthält und die Multiplikation von G in seiner Multiplikation enthält.

Definition 2.2.4: Sei G eine Gruppe und R ein kommutativer Ring. Sei $R[G]$ die Menge der formalen Linearkombinationen

$$r_1 g_1 + \ldots + r_n g_n \quad \text{mit } n \geq 0, r_i \in R, g_i \in G.$$

Die Addition ist die von Linearkombinationen, und die Multiplikation ist durch

$$(rg)(r'g') := (rr')(gg')$$

definiert und mit dem Distributivgesetz linear fortgesetzt. Hierbei wird rr' in R und gg' in G berechnet. Dann ist $R[G]$ ein Ring mit Eins $1_R 1_G$, der *Gruppenring* von G mit Koeffizienten in R.

Der Ring $R[G]$ ist genau dann kommutativ, wenn G abelsch ist. Man identifiziert $r \in R$ mit $r1_G \in R[G]$ und $g \in G$ mit $1_R g \in R[G]$.

thomas.kahle@ovgu.de

Beispiel 2.2.5: Sei $G = \mathbb{Z}_3 = \{1, x, x^2\}$ die zyklische Gruppe mit drei Elementen. Dann ist

$$\mathbb{Q}[\mathbb{Z}_3] = \{a + bx + cx^2 \colon a, b, c \in \mathbb{Q}\},$$

wobei jetzt $x^k x^l = x^{(k+l) \bmod 3}$ gilt, zum Beispiel $x^2 \cdot x^2 = x$ und $x^2 \cdot x = 1$. Das ist ein kommutativer Ring.

Für Fans: Dass die Elemente von G invertierbar sind, haben wir gar nicht benutzt, sondern nur die assoziative Multiplikation mit neutralem Element. Eigentlich genügt also ein sogenanntes *Monoid*. Man kann sich überlegen, dass $R[\mathbb{N}_0]$ für das (multiplikativ als $\{1, x, x^2, ...\}$ geschriebene) Monoid $(\mathbb{N}_0, +)$ genau der Polynomring $R[x]$ ist.

2.3 Ringhomomorphismen, Ideale und Quotienten

Wie bei Gruppen untersuchen wir Ringe über die strukturerhaltenden Abbildungen zwischen ihnen. Ihre Kerne werden die *Ideale* sein, und nach Idealen kann man, wie nach Normalteilern, Quotienten bilden.

Definition 2.3.1: Seien R und S Ringe.

1. Ein *Ringhomomorphismus* ist eine Abbildung $\varphi \colon R \to S$ mit
   - $\varphi(a + b) = \varphi(a) + \varphi(b)$ für alle $a, b \in R$, d.h. φ ist ein Gruppenhomomorphismus $(R, +) \to (S, +)$,
   - $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in R$,
   - $\varphi(1_R) = 1_S$.
2. Der *Kern* von φ ist
   $$\ker \varphi := \{x \in R \colon \varphi(x) = 0\},$$
   also der Kern des Gruppenhomomorphismus $(R, +) \to (S, +)$.
3. Ein bijektiver Ringhomomorphismus heißt *Isomorphismus*. Existiert ein Isomorphismus $R \to S$, so heißen R und S *isomorph*, und man schreibt $R \cong S$.

Die Bedingung $\varphi(1_R) = 1_S$ folgt nicht aus den anderen beiden (die Nullabbildung erfüllt diese zum Beispiel), deswegen fordern wir sie ausdrücklich. Wie bei Gruppen ist die Umkehrabbildung eines Ringisomorphismus wieder ein Ringisomorphismus.

Beispiel 2.3.2:

1. Die Abbildung $\varphi \colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $n \mapsto \overline{n}$, die jede ganze Zahl auf ihren Rest modulo 2 abbildet, ist ein Ringhomomorphismus mit Kern $2\mathbb{Z}$.

© 2026 Thomas Kahle

2. Sei $n \in \mathbb{Z}$. Die Abbildung $\varphi_n: \mathbb{Z} \to \mathbb{Z}$, $m \mapsto nm$, ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$, denn $\varphi_n(m + m') = nm + nm' = \varphi_n(m) + \varphi_n(m')$. Für $n \notin \{0, 1\}$ ist sie aber **kein** Ringhomomorphismus, denn
$$\varphi_n(m_1 m_2) = nm_1 m_2 \neq n^2 m_1 m_2 = \varphi_n(m_1)\varphi_n(m_2)$$
für $m_1, m_2 \neq 0$. Für $n = 0$ verletzt φ_0 die Bedingung $\varphi(1) = 1$.
3. Sei R ein kommutativer Ring. Die Abbildung
$$\text{const}: R[x] \to R, \quad p = a_n x^n + \ldots + a_1 x + a_0 \mapsto p(0) = a_0,$$
die einem Polynom seine Konstante zuordnet, ist ein Ringhomomorphismus, denn die Konstante eines Produkts von Polynomen ist das Produkt der Konstanten. Ihr Kern ist
$$\ker(\text{const}) = \{a_n x^n + \ldots + a_1 x : n \geq 1, a_i \in R\} = \{xq : q \in R[x]\},$$
die Menge aller Polynome ohne konstanten Term, also aller durch x teilbaren Polynome. Wir werden diese Menge gleich als das von x erzeugte Ideal $\langle x \rangle$ erkennen.

Im letzten Beispiel lohnt es sich, die Fasern anzusehen. Für $a \in R$ ist $\text{const}^{-1}(a)$ die Menge aller Polynome mit Konstante a. Die Fasern sind die Äquivalenzklassen der Relation „gleiche Konstante“, und es gibt genau eine Faser für jedes $a \in R$. Multipliziert man ein Polynom p mit Konstante $p(0) = a$ mit einem Polynom q mit Konstante $q(0) = b$, so hat pq die Konstante ab. Man kann also Fasern multiplizieren, indem man Repräsentanten multipliziert, und erhält dabei genau die Multiplikation von R. Das ist dieselbe Idee wie bei den Quotientengruppen in Kapitel 1 (siehe Abschnitt 1.11).

Proposition 2.3.3: Seien R, S Ringe und $\varphi: R \to S$ ein Ringhomomorphismus.
1. Das Bild $\text{im}\,\varphi \subseteq S$ ist ein Teilring von S.
2. Der Kern $\ker \varphi$ ist eine Untergruppe von $(R, +)$ mit der zusätzlichen Eigenschaft: Ist $x \in R$ und $y \in \ker \varphi$, so sind $xy \in \ker \varphi$ und $yx \in \ker \varphi$. Der Kern ist also abgeschlossen unter Multiplikation mit beliebigen Ringelementen, von links und von rechts.

Beweis.
1. Das Bild ist eine Untergruppe von $(S, +)$, da φ ein Gruppenhomomorphismus ist. Es ist abgeschlossen unter Multiplikation, denn $\varphi(a)\varphi(b) = \varphi(ab)$, und es enthält $1_S = \varphi(1_R)$.
2. Der Kern eines Gruppenhomomorphismus ist eine Untergruppe. Für $x \in R$ und $y \in \ker \varphi$ gilt $\varphi(xy) = \varphi(x)\varphi(y) = \varphi(x) \cdot 0 = 0$ und ebenso $\varphi(yx) = 0$.

■

Achtung! Der Kern ist im Allgemeinen *kein* Teilring, denn er enthält die 1 nur, wenn $\varphi(1) = 0$ ist, also nur, wenn S der Nullring ist.

Quotientenringe

Ein Ringhomomorphismus $\varphi\colon R \to S$ ist insbesondere ein Homomorphismus der abelschen Gruppen $(R,+) \to (S,+)$. Seine Fasern bilden also die Quotientengruppe nach dem Kern, die isomorph zum Bild ist. Wir zeigen nun, dass dieser Quotient sogar ein Ring ist. Sei $I = \ker\varphi$. Die Nebenklassen bezeichnen wir mit $r + I$ für $r \in R$. Sie bilden einen Ring mit den Verknüpfungen

$$(r+I)+(s+I) = (r+s)+I \quad \text{und} \quad (r+I)\cdot(s+I) = rs+I,$$

denn die Fasern von φ multiplizieren sich genau so, wie wir es oben beim Beispiel const gesehen haben. Dieser Ring ist per Konstruktion isomorph zu $\operatorname{im}\varphi$, denn $r + I \mapsto \varphi(r)$ ist wohldefiniert, bijektiv und verträglich mit Addition und Multiplikation. Dass er die Ringaxiome erfüllt, folgt also daraus, dass $\operatorname{im}\varphi$ ein Ring ist.

Wir können die Konstruktion aber auch für eine *beliebige* Untergruppe I von $(R,+)$ versuchen. Ist dann die Menge der Nebenklassen ein Ring? Die Antwort ist nein: Man braucht ein Ideal, d.h. eine Untergruppe, die abgeschlossen unter Multiplikation mit Ringelementen ist. Seien dazu $r + I$ und $s + I$ beliebige Nebenklassen der Untergruppe I. Die Addition ist wohldefiniert, da $(R,+)$ abelsch und damit I ein Normalteiler ist. Hängt aber die Multiplikation von den Repräsentanten ab? Seien $r' \in r + I$ und $s' \in s + I$ andere Repräsentanten, also $r' = r + \alpha$ und $s' = s + \beta$ mit $\alpha, \beta \in I$. Für die Wohldefiniertheit der Multiplikation benötigen wir

$$(r+\alpha)(s+\beta)+I = rs+I \quad \text{für alle } r,s \in R, \alpha,\beta \in I. \tag{2}$$

- Im Fall $r = s = 0$ ergibt sich $\alpha\beta + I = I$, d.h. $\alpha\beta \in I$ für alle $\alpha, \beta \in I$. Notwendig für (2) ist also, dass I unter Multiplikation abgeschlossen ist.
- Im Fall $s = 0$ und r beliebig ergibt sich $r\beta + \alpha\beta + I = 0 + I$. Mit dem ersten Fall folgt $r\beta \in I$ für alle $r \in R$ und $\beta \in I$. Notwendig für (2) ist also, dass I abgeschlossen unter Multiplikation mit beliebigen Elementen von R von links ist. Man schreibt dafür kurz $RI \subseteq I$.
- Analog folgt mit $r = 0$ und s beliebig, dass $IR \subseteq I$ notwendig ist.

Umgekehrt gilt (2), wenn $RI \subseteq I$ und $IR \subseteq I$ gilt, denn dann ist

$$(r+\alpha)(s+\beta) = rs + \underbrace{r\beta + \alpha s + \alpha\beta}_{\in I}.$$

In diesem Fall ist die Menge der Nebenklassen ein Ring, denn Assoziativität, Distributivgesetze und die Eins $1 + I$ erbt man direkt von R.

Definition 2.3.4: Sei R ein Ring und $I \subseteq R$ eine Untergruppe von $(R,+)$.

1. I ist ein *Linksideal* von R, falls $RI \subseteq I$ gilt, d.h. $ra \in I$ für alle $r \in R$ und $a \in I$.
2. I ist ein *Rechtsideal* von R, falls $IR \subseteq I$ gilt.
3. I ist ein *Ideal* von R, falls es sowohl Links- als auch Rechtsideal ist.

Ist I ein Ideal, so heißt der Ring R/I der Nebenklassen mit den obigen Verknüpfungen der *Quotientenring* von R nach I.

Man nennt Ideale auch *beidseitige* oder *zweiseitige* Ideale. In kommutativen Ringen muss natürlich nur $RI \subseteq I$ geprüft werden. Ein Ideal I ist genau dann ein Teilring, wenn $1 \in I$ ist, und dann ist schon $I = R$, denn $r = r \cdot 1 \in I$ für alle $r \in R$. Allgemeiner gilt $I = R$, sobald I eine Einheit u enthält, denn dann ist $1 = u^{-1}u \in I$.

Nach Proposition 2.3.3 sind Kerne von Ringhomomorphismen Ideale. Umgekehrt ist jedes Ideal $I \subseteq R$ der Kern der Abbildung

$$R \to R/I, \quad r \mapsto r + I.$$

Die Kerne von Ringhomomorphismen sind also genau die (zweiseitigen) Ideale. Wie bei Gruppen gibt es analoge Isomorphiesätze (siehe Abschnitt 1.13).

Satz 2.3.5:

1. Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Dann ist
$$R/\ker\varphi \cong \varphi(R) \quad (\text{als Ringe}).$$
2. Sei $I \subseteq R$ ein Ideal. Dann ist
$$\pi\colon R \to R/I, \quad r \mapsto r + I,$$
ein surjektiver Ringhomomorphismus mit Kern I. Er heißt die *natürliche Projektion*.

Beweis. Wir sammeln die Fakten, die wir schon gesehen haben.

1. Sei $I = \ker\varphi$. Die Abbildung $\overline{\varphi}\colon R/I \to \varphi(R)$, $r + I \mapsto \varphi(r)$, ist wohldefiniert und injektiv, denn $\varphi(r) = \varphi(r')$ gilt genau dann, wenn $r - r' \in \ker\varphi$ ist, also wenn $r + I = r' + I$ ist. Sie ist offensichtlich surjektiv und wegen $\overline{\varphi} \circ \pi = \varphi$ ein Ringhomomorphismus.
2. Nach Definition der Verknüpfungen in R/I ist π ein Ringhomomorphismus, und $\pi(1) = 1 + I$ ist die Eins von R/I. Er ist offensichtlich surjektiv, und es ist $\pi(r) = 0 + I$ genau dann, wenn $r \in I$ gilt.

■

Wie bei Gruppen bietet sich die Notation $\overline{r} := r + I$ an, wenn I klar ist.

thomas.kahle@ovgu.de

Beispiel 2.3.6:

1. Sei A ein Ring und $X \neq \varnothing$ eine Menge. Sei R der Ring der Abbildungen $f\colon X \to A$ mit punktweisen Operationen. Für $x \in X$ ist der *Einsetzhomomorphismus*

$$\varphi_x\colon R \to A, \quad f \mapsto f(x),$$

   ein Ringhomomorphismus. Er ist surjektiv, da R für jedes $a \in A$ die konstante Abbildung $x \mapsto a$ enthält. Sein Kern ist $\ker \varphi_x = \{f \in R\colon f(x) = 0\}$. Also ist $R/\ker \varphi_x \cong A$.
2. Für den Ringhomomorphismus $\mathrm{const}\colon R[x] \to R$, $p \mapsto p(0)$, aus Beispiel 2.3.2 erhalten wir $R[x]/\{xq\colon q \in R[x]\} \cong R$.
3. Wir können noch weiter abbilden: Sei $R = \mathbb{Z}$ und

$$\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}, \quad p \mapsto \overline{p(0)}.$$

   Der Kern ist $\{p \in \mathbb{Z}[x]\colon p(0) \equiv 0 \bmod 2\}$, die Menge der Polynome mit gerader Konstante. Die einzige andere Nebenklasse ist $1 + \ker \varphi$, die Menge der Polynome mit ungerader Konstante. Es ist $\mathbb{Z}[x]/\ker \varphi \cong \mathbb{Z}/2\mathbb{Z}$.

Satz 2.3.7: Sei R ein Ring.

1. Sei $A \subseteq R$ ein Teilring und $B \subseteq R$ ein Ideal. Dann ist $A + B = \{a + b\colon a \in A, b \in B\}$ ein Teilring von R und B ein Ideal von $A + B$. Außerdem ist $A \cap B$ ein Ideal von A, und es gilt

$$(A + B)/B \cong A/(A \cap B).$$

2. Seien $I \subseteq J \subseteq R$ Ideale. Dann ist J/I ein Ideal von R/I, und

$$(R/I)/(J/I) \cong R/J.$$

3. Sei $I \subseteq R$ ein Ideal. Die Zuordnung $A \mapsto A/I$ ist eine inklusionserhaltende Bijektion zwischen den Teilringen $A \subseteq R$, die I enthalten, und den Teilringen von R/I. Ebenso ist $J \mapsto J/I$ eine inklusionserhaltende Bijektion zwischen den Idealen $J \subseteq R$, die I enthalten, und den Idealen von R/I. Die Umkehrabbildung ist in beiden Fällen das Urbild unter der natürlichen Projektion $\pi\colon R \to R/I$.

Beweis. Übung. Man kann jeweils die entsprechenden Isomorphiesätze für Gruppen verwenden und muss nur zusätzlich die Verträglichkeit mit der Multiplikation prüfen. ■

© 2026 Thomas Kahle

Erzeugte Ideale

Wir wollen Ringe verstehen, indem wir alle ihre Ideale und Quotienten (und später ihre Moduln) verstehen. Zunächst stellen wir fest, dass Durchschnitte von Idealen wieder Ideale sind.

Lemma 2.3.8: Sei R ein Ring und $(I_j)_{j\in J}$ eine nichtleere Familie von Idealen von R. Dann ist $\bigcap_{j\in J} I_j$ ein Ideal von R.

Beweis. Sei $I = \bigcap_j I_j$. Es ist $0 \in I$. Seien $a, b \in I$ und $r \in R$. Für jedes j ist $a, b \in I_j$, also $a - b \in I_j$, $ra \in I_j$ und $ar \in I_j$, da I_j ein Ideal ist. Also liegen $a - b$, ra und ar in I. ∎

Definition 2.3.9: Sei R ein Ring und $A \subseteq R$ eine Teilmenge.

1. Das *von A erzeugte Ideal* ist
$$\langle A\rangle := \bigcap_{I\subseteq R \text{ Ideal},\, A\subseteq I} I.$$
2. Wir setzen
$$RA := \left\{\sum_{i=1}^{s} r_i a_i \colon s \in \mathbb{N}_0, r_i \in R, a_i \in A\right\},$$
$$AR := \left\{\sum_{i=1}^{s} a_i r_i \colon s \in \mathbb{N}_0, r_i \in R, a_i \in A\right\},$$
$$RAR := \left\{\sum_{i=1}^{s} r_i a_i r_i' \colon s \in \mathbb{N}_0, r_i, r_i' \in R, a_i \in A\right\},$$
wobei die leere Summe ($s = 0$) gleich 0 ist.
3. Ein Ideal $I \subseteq R$ ist *endlich erzeugt*, falls eine endliche Menge $A \subseteq R$ mit $\langle A\rangle = I$ existiert. Man schreibt dann auch $\langle a_1, \dots, a_n\rangle$ für $\langle\{a_1, \dots, a_n\}\rangle$.
4. Ein Ideal $I \subseteq R$ ist ein *Hauptideal*, falls ein $a \in R$ mit $I = \langle a\rangle := \langle\{a\}\rangle$ existiert.

Nach Lemma 2.3.8 ist $\langle A\rangle$ ein Ideal, und zwar das kleinste Ideal, das A enthält. Statt $\langle a\rangle$ schreibt man oft auch (a). Folgende Bemerkungen sind hilfreich:

- Es gilt $\langle A\rangle = RAR$. Wie bei der erzeugten Untergruppe (siehe Abschnitt 1.9) hat man also eine explizite Beschreibung. In der Tat ist RAR ein Ideal, das A enthält (wegen $a = 1 \cdot a \cdot 1$), und jedes Ideal, das A enthält, enthält auch alle Summen $\sum r_i a_i r_i'$.
- Genauso sind RA und AR das von A erzeugte Links- bzw. Rechtsideal.
- Für ein Hauptideal eines kommutativen Rings gilt
$$\langle a\rangle = \{ra \colon r \in R\}.$$

thomas.kahle@ovgu.de

Das ist analog zu zyklischen Untergruppen. Für $b \in R$ gilt also

$$b \in \langle a \rangle \iff \exists r \in R\colon ra = b \iff \langle b \rangle \subseteq \langle a \rangle,$$

d.h. $b \in \langle a \rangle$ genau dann, wenn „a teilt b in R“. In $\mathbb{Z}$ hat man zum Beispiel die Ideale $n\mathbb{Z} = \langle n \rangle$, und die Teilbarkeit bildet sich in der Inklusion von Idealen ab. Wir zeigen gleich, dass $\mathbb{Z}$ nur Hauptideale hat.

- Ideale bilden auch einen Verband. Seien $I, J \subseteq R$ Ideale.
  - Die *Summe* ist

    $$I + J = \langle I \cup J \rangle = \{a + b\colon a \in I, b \in J\}.$$

    Die Menge auf der rechten Seite ist schon ein Ideal, da $r(a+b) = ra + rb$ und $(a+b)r = ar + br$ gilt. Das ist bemerkenswert einfacher als bei Untergruppen, wo das Produkt HK nur unter Zusatzbedingungen eine Untergruppe ist (siehe Proposition 1.13.3).
  - Das *Produkt* $IJ = \langle ab\colon a \in I, b \in J \rangle$ ist das von den Produkten erzeugte Ideal. Die Menge der Produkte selbst ist im Allgemeinen kein Ideal (siehe die Übung unten).
  - Für $n \geq 1$ ist die *n-te Potenz* von I induktiv definiert als $I^1 = I$ und $I^n := I \cdot I^{n-1}$. Explizit ist $I^n = \langle a_1 \cdots a_n\colon a_i \in I \rangle$. Es gilt

    $$\ldots \subseteq I^n \subseteq I^{n-1} \subseteq \ldots \subseteq I^2 \subseteq I.$$

    Diese Inklusionen sind nicht notwendig strikt (z.B. für $I = R$), oft aber schon, zum Beispiel ist $(2\mathbb{Z})^n = 2^n\mathbb{Z}$.
  - Es gilt $IJ \subseteq I \cap J$, denn für $a \in I$, $b \in J$ liegt ab in I (da I ein Rechtsideal ist) und in J (da J ein Linksideal ist). Die Inklusion ist eventuell strikt, z.B. für $I = J = 2\mathbb{Z}$, wo $IJ = 4\mathbb{Z}$ und $I \cap J = 2\mathbb{Z}$ ist.

Übung. Sei $I = \langle 2, x \rangle \subseteq \mathbb{Z}[x]$. Zeigen Sie, dass $4 + x^2 \in I^2$ gilt, dass sich $4 + x^2$ aber nicht als Produkt ab mit $a, b \in I$ schreiben lässt.

Motto: Die Menge der Ideale und ihre Inklusionen geben uns Informationen über den Ring, insbesondere über seine Arithmetik, also die Teilbarkeit im Ring.

Definition 2.3.10: Ein Integritätsbereich R heißt *Hauptidealring*, falls jedes Ideal von R ein Hauptideal ist.

Beispiel 2.3.11: $\mathbb{Z}$ ist ein Hauptidealring. Ist nämlich $I \subseteq \mathbb{Z}$ ein Ideal, so ist I insbesondere eine Untergruppe der zyklischen Gruppe $(\mathbb{Z}, +)$. Jede Untergruppe einer zyklischen Gruppe ist zyklisch (siehe Abschnitt 1.8), also existiert ein $n \in \mathbb{Z}$ mit $I = \{kn\colon k \in \mathbb{Z}\} = \langle n \rangle$. Hier gilt

$$\langle m \rangle \subseteq \langle n \rangle \iff n \mid m,$$

© 2026 Thomas Kahle

die Inklusion von Idealen entspricht also der Teilbarkeit. Außerdem gilt $\langle m, n\rangle = \langle \mathrm{ggT}(m, n)\rangle$, denn nach dem Lemma von Bézout liegt $\mathrm{ggT}(m, n)$ in $\langle m, n\rangle$, und umgekehrt sind m und n Vielfache von $\mathrm{ggT}(m, n)$. Insbesondere ist $\langle m, n\rangle = \mathbb{Z} = \langle 1\rangle$, wenn $\mathrm{ggT}(m, n) = 1$ gilt.

Nicht jeder Ring ist ein Hauptidealring.

Beispiel 2.3.12: $\mathbb{Z}[x]$ ist kein Hauptidealring, denn $\langle 2, x\rangle$ ist kein Hauptideal. Es ist

$$\langle 2, x\rangle = \{2p + xq \colon p, q \in \mathbb{Z}[x]\}$$

die Menge der Polynome mit gerader Konstante, also der Kern des Homomorphismus $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, $p \mapsto \overline{p(0)}$, aus Beispiel 2.3.6. Angenommen, es gilt $\langle 2, x\rangle = \langle a\rangle$ für ein $a \in \mathbb{Z}[x]$. Da $2 \in \langle a\rangle$ ist, existiert ein $p \in \mathbb{Z}[x]$ mit $2 = pa$. Nach der Gradformel für Polynome über Integritätsbereichen gilt $0 = \deg(2) = \deg(p) + \deg(a)$, und da beide Grade nichtnegativ sind, folgt $\deg(a) = 0$. Also ist a eine ganze Zahl, die 2 teilt, d.h. $a \in \{\pm 1, \pm 2\}$.

- Wäre $a = \pm 1$, so wäre $\langle a\rangle = \mathbb{Z}[x]$. Aber $1 \notin \langle 2, x\rangle$, da 1 eine ungerade Konstante hat.
- Wäre $a = \pm 2$, so wäre $x \in \langle 2\rangle$, d.h. $x = 2q$ für ein $q \in \mathbb{Z}[x]$. Das ist offensichtlich falsch, da x einen ungeraden Koeffizienten hat.

Beide Fälle führen zum Widerspruch.

Die Bedeutung von $\langle A\rangle$ hängt natürlich vom Ring ab. Zum Beispiel ist $\langle 2\rangle \subseteq \mathbb{Q}[x]$ der ganze Ring $\mathbb{Q}[x]$, da 2 in $\mathbb{Q}[x]$ eine Einheit ist: Aus $2 \in \langle 2\rangle$ und $\frac{1}{2} \in \mathbb{Q}$ folgt $\frac{1}{2} \cdot 2 = 1 \in \langle 2\rangle$, also $\mathbb{Q}[x] = \{1 \cdot p \colon p \in \mathbb{Q}[x]\} \subseteq \langle 2\rangle$. Dabei haben wir eine beliebte Technik benutzt: Ist I ein Ideal und $a \in I$, so ist $\langle a\rangle \subseteq I$.

Ideale können auch Körper charakterisieren.

Proposition 2.3.13: Sei R ein kommutativer Ring mit $1 \neq 0$. Dann ist R genau dann ein Körper, wenn $\langle 0\rangle$ und R seine einzigen Ideale sind.

Beweis. Wir haben oben gesehen: Für ein Ideal I gilt $I = R$ genau dann, wenn $1 \in I$ ist.

Sei R ein Körper und $I \subseteq R$ ein Ideal mit $I \neq \langle 0\rangle$. Sei $x \in I$ mit $x \neq 0$. In R existiert x^{-1}, und da I ein Ideal ist, folgt $1 = x^{-1}x \in I$, also $I = R$.

Sei umgekehrt R ein kommutativer Ring mit $1 \neq 0$, der nur die beiden Ideale $\langle 0\rangle$ und R hat. Es genügt zu zeigen, dass jedes $x \in R \setminus \{0\}$ invertierbar ist. Betrachte $\langle x\rangle \subseteq R$.

Da $\langle x\rangle \neq \langle 0\rangle$ ist, folgt $\langle x\rangle = R$. Also ist $1 \in \langle x\rangle$, d.h. es existiert ein $v \in R$ mit $1 = vx$. Damit ist $x \in R^*$, und R ist ein Körper. ■

Korollar 2.3.14: Sei K ein Körper und S ein Ring mit $1 \neq 0$. Dann ist jeder Ringhomomorphismus $\varphi\colon K \to S$ injektiv.

Beweis. Der Kern ist ein Ideal, also nach Proposition 2.3.13 gleich $\langle 0\rangle$ oder K. Wegen $\varphi(1) = 1 \neq 0$ ist $1 \notin \ker\varphi$, also $\ker\varphi = \langle 0\rangle$. ■

Homomorphismen zwischen Körpern spielen trotzdem eine große Rolle. Nach Korollar 2.3.14 sind sie alle Einbettungen oder Isomorphismen. In der Körpertheorie studiert man viele Isomorphismen. Ist zum Beispiel $K \subseteq L$ ein Teilkörper, so bezeichnet $\mathrm{Gal}(L/K)$ die Gruppe der Automorphismen von L, die K punktweise festhalten. Diese Gruppe werden wir am Ende der Vorlesung genauer kennenlernen (siehe Abschnitt 3.6).

2.4 Maximale Ideale und Primideale

In $\mathbb{Z}$ entsprechen die Primzahlen p den Idealen $p\mathbb{Z}$, die in keinem anderen echten Ideal enthalten sind. Diese Beobachtung verallgemeinern wir auf beliebige Ringe auf zwei Arten.

Definition 2.4.1: Ein Ideal $M \subseteq R$ eines Rings R heißt *maximal*, falls
1. $M \neq R$ ist und
2. für jedes Ideal N mit $M \subseteq N \subseteq R$ gilt $N = M$ oder $N = R$.

Der Nullring hat kein maximales Ideal, denn sein einziges Ideal ist er selbst. Jeder andere Ring hat aber eines. Das ist gar nicht selbstverständlich: Für „Ringe ohne Eins“ ist es falsch. Versieht man zum Beispiel $(\mathbb{Q}, +)$ mit der trivialen Multiplikation $ab = 0$ für alle $a, b \in \mathbb{Q}$, so erfüllt man alle Ringaxiome außer der Existenz einer Eins. In diesem „Ring“ ist jede Untergruppe von $(\mathbb{Q}, +)$ ein Ideal, und $(\mathbb{Q}, +)$ hat keine maximalen echten Untergruppen.

Für den Beweis der Existenz braucht man das Auswahlaxiom in der Gestalt des *Zornschen Lemmas*: Ist $(X, \leq)$ eine nichtleere partiell geordnete Menge, in der jede Kette (d.h. jede total geordnete Teilmenge) eine obere Schranke in X besitzt, so besitzt X ein maximales Element.

Proposition 2.4.2: Sei R ein Ring. Dann ist jedes echte Ideal $I \neq R$ in einem maximalen Ideal enthalten.

© 2026 Thomas Kahle

Beweis. Sei $I \neq R$ ein Ideal. Sei

$$\mathcal{I} = \{J \subseteq R \text{ Ideal: } I \subseteq J \neq R\},$$

partiell geordnet per Inklusion. Es ist $\mathcal{I} \neq \varnothing$, da $I \in \mathcal{I}$ ist. Wir suchen ein maximales Element in $\mathcal{I}$, denn ein solches ist ein maximales Ideal von R, das I enthält. Sei $\mathcal{C} \subseteq \mathcal{I}$ eine nichtleere Kette. Wir setzen

$$I_{\mathcal{C}} = \bigcup_{J \in \mathcal{C}} J$$

und prüfen, dass $I_{\mathcal{C}}$ ein Ideal ist. Seien $a, b \in I_{\mathcal{C}}$ und $r \in R$. Dann gibt es $J_1, J_2 \in \mathcal{C}$ mit $a \in J_1$ und $b \in J_2$. Da $\mathcal{C}$ eine Kette ist, gilt $J_1 \subseteq J_2$ oder $J_2 \subseteq J_1$, also liegen a und b in einem gemeinsamen $J \in \mathcal{C}$. Damit sind $a - b$, ra und ar in $J \subseteq I_{\mathcal{C}}$. Außerdem ist $I_{\mathcal{C}} \neq R$, da 1 in keinem $J \in \mathcal{C}$ liegt. Also ist $I_{\mathcal{C}} \in \mathcal{I}$ eine obere Schranke von $\mathcal{C}$. Für die leere Kette ist I eine obere Schranke. Nach dem Zornschen Lemma hat $\mathcal{I}$ ein maximales Element. ■

Insbesondere hat jeder Ring $R \neq 0$ ein maximales Ideal (wende Proposition 2.4.2 auf $I = \langle 0 \rangle$ an). Für kommutative Ringe lassen sich maximale Ideale über ihre Quotienten charakterisieren.

Proposition 2.4.3: Sei R ein kommutativer Ring. Ein Ideal $M \subseteq R$ ist genau dann maximal, wenn R/M ein Körper ist.

Beweis. Nach dem Korrespondenzsatz (Satz 2.3.7, Teil 3) entsprechen die Ideale von R/M bijektiv und inklusionserhaltend den Idealen von R, die M enthalten. Dabei entspricht M dem Nullideal und R dem ganzen Ring R/M. Also ist M genau dann maximal, wenn $R/M \neq 0$ ist und R/M keine weiteren Ideale als $\langle 0 \rangle$ und R/M hat. Nach Proposition 2.3.13 ist das genau dann der Fall, wenn R/M ein Körper ist. ■

So werden wir viele Körper konstruieren:

- Alle endlichen Körper können als Quotienten $\mathbb{Z}[x]/M$ nach maximalen Idealen konstruiert werden (siehe Abschnitt 3.5).
- Es ist $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\} \cong \mathbb{Q}[x]/\langle x^2 - 2 \rangle$ (siehe Abschnitt 3.1).

Beispiel 2.4.4: Der Kern von $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, $p \mapsto \overline{p(0)}$, also das Ideal $\langle 2, x \rangle$ aus Beispiel 2.3.12, ist maximal, da $\mathbb{Z}/2\mathbb{Z}$ ein Körper ist. Dagegen ist $\langle x \rangle$, der Kern von $\mathbb{Z}[x] \to \mathbb{Z}$, $p \mapsto p(0)$, nicht maximal, denn $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ ist kein Körper. In der Tat ist $\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$.

Die zweite Verallgemeinerung von Primzahlen benutzt die Eigenschaft „$p \mid ab \Rightarrow p \mid a$ oder $p \mid b$“.

Definition 2.4.5: Sei R ein kommutativer Ring. Ein Ideal $P \subseteq R$ heißt *prim* oder *Primideal*, falls $P \neq R$ ist und für alle $a, b \in R$ gilt:

$$ab \in P \Longrightarrow a \in P \text{ oder } b \in P.$$

Zum Vergleich: Eine ganze Zahl $p \notin \{0, \pm 1\}$ ist genau dann eine Primzahl (bis auf Vorzeichen), wenn aus $p \mid ab$ folgt, dass $p \mid a$ oder $p \mid b$ gilt. Mit Idealen von $\mathbb{Z}$ ausgedrückt heißt das: $ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ oder $b \in \langle p \rangle$. Die Primideale von $\mathbb{Z}$ sind also die $\langle p \rangle$ für Primzahlen p und zusätzlich das Nullideal $\langle 0 \rangle$.

Zur Erinnerung: Ein *Integritätsbereich* ist ein kommutativer Ring mit $1 \neq 0$, der nullteilerfrei ist.

Proposition 2.4.6: Sei R ein kommutativer Ring. Ein Ideal $P \subseteq R$ ist genau dann prim, wenn R/P ein Integritätsbereich ist.

Beweis. Wir schreiben $\overline{a} = a + P$ für die Elemente von R/P. Der Ring R/P ist kommutativ. Er ist genau dann ein Integritätsbereich, wenn

- $\overline{1} \neq \overline{0}$ gilt, also $1 \notin P$, d.h. $P \neq R$, und
- aus $\overline{a} \cdot \overline{b} = \overline{0}$ folgt, dass $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$ gilt. Wegen $\overline{a} \cdot \overline{b} = \overline{ab}$ heißt das: aus $ab \in P$ folgt $a \in P$ oder $b \in P$.

Das sind genau die Bedingungen in Definition 2.4.5. ∎

Korollar 2.4.7: Sei R ein kommutativer Ring. Jedes maximale Ideal von R ist prim.

Beweis. Ist M maximal, so ist R/M nach Proposition 2.4.3 ein Körper. Körper sind Integritätsbereiche, also ist M nach Proposition 2.4.6 prim. ∎

Die Umkehrung gilt nicht: In $\mathbb{Z}[x]$ ist $\langle x \rangle$ prim, da $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ ein Integritätsbereich ist, aber nach Beispiel 2.4.4 nicht maximal.

Diese Technik wird gerne mit dem ersten Isomorphiesatz kombiniert. Sei zum Beispiel $\varphi\colon R \to S$ ein Ringhomomorphismus von kommutativen Ringen, und S ein Integritätsbereich. Dann ist $\operatorname{im} \varphi$ als Teilring von S ebenfalls ein Integritätsbereich, und wegen $R/\ker \varphi \cong \operatorname{im} \varphi$ ist $\ker \varphi$ nach Proposition 2.4.6 ein Primideal.

Wie die Arithmetik von $\mathbb{Z}$ in allgemeineren Ringen aussieht, untersuchen wir im nächsten Abschnitt.

© 2026 Thomas Kahle

2.5 Teilbarkeit in Integritätsbereichen

Die Ringtheorie beschäftigt sich mit vielen weiteren spannenden Klassen von Ringen, die alle Verallgemeinerungen der ganzen Zahlen sind. Zum Beispiel:

- *Euklidische Ringe*: Ringe, in denen ein euklidischer Algorithmus einen größten gemeinsamen Teiler berechnet. Sie sind eine gemeinsame Verallgemeinerung von $\mathbb{Z}$ und dem Polynomring $K[x]$ über einem Körper K.
- *Hauptidealringe* als weitere solche Verallgemeinerung.
- *Faktorielle Ringe*, in denen sich jedes Element auf (bis auf Einheiten) eindeutige Weise in Primelemente zerlegen, also faktorisieren, lässt.

Wir werden diese Begriffe in diesem Abschnitt präzisieren und danach den Polynomring über einem Körper im Detail studieren. Er ist ein Beispiel für alles Obige. Zunächst übertragen wir den Begriff der Teilbarkeit aus $\mathbb{Z}$ auf beliebige Integritätsbereiche.

Definition 2.5.1: Sei R ein Integritätsbereich und seien $a, b \in R$. Das Element b ist ein *Teiler* von a, geschrieben $b \mid a$, falls ein $c \in R$ existiert mit $a = bc$.

Die folgenden Rechenregeln kennt man aus $\mathbb{Z}$. Sei R ein Integritätsbereich und seien $a, b, c \in R$.

- Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$ (Transitivität).
- Aus $a \mid b$ und $a \mid c$ folgt $a \mid (fb + gc)$ für alle $f, g \in R$.
- Es gilt $a \mid b$ genau dann, wenn $\langle b \rangle \subseteq \langle a \rangle$.
- Aus $a \mid b$ und $b \mid a$ folgt, dass ein $\varepsilon \in R^*$ existiert mit $a = \varepsilon b$. Man nennt a und b dann *assoziiert*.

  Ist nämlich $a = 0$ oder $b = 0$, so sind beide gleich Null und die Aussage ist trivial. Seien also $a \neq 0$ und $b \neq 0$. Nach Voraussetzung gilt $a = fb$ und $b = ga$ für gewisse $f, g \in R$. Damit ist $a = fb = fga$, und da man in einem Integritätsbereich durch $a \neq 0$ kürzen darf, folgt $1 = fg$. Also ist $f \in R^*$.
- Ist $a \in R$ und $\varepsilon \in R^*$, so gilt $\varepsilon \mid a$ und $\varepsilon a \mid a$, denn $a = \varepsilon(\varepsilon^{-1}a) = (\varepsilon a)\varepsilon^{-1}$. Diese Teiler heißen *triviale Teiler* von a (vergleiche in $\mathbb{Z}$: $a \mid a$, $-a \mid a$, $1 \mid a$, $-1 \mid a$).

Übung. Beweisen Sie die ersten drei Rechenregeln.

In $\mathbb{Z}$ haben wir zwei vertraute Definitionen von Primzahlen: Eine Primzahl p hat nur triviale Teiler, und aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$. In $\mathbb{Z}$ sind beide Eigenschaften äquivalent. In allgemeinen Integritätsbereichen fallen sie auseinander, weshalb die folgende Definition zwei Teile hat.

Definition 2.5.2: Sei R ein Integritätsbereich.

1. Ein Element $r \in R$ mit $r \neq 0$ und $r \notin R^*$ heißt *irreduzibel*, falls aus $r = ab$ mit $a, b \in R$ folgt, dass $a \in R^*$ oder $b \in R^*$ ist. Andernfalls heißt r *reduzibel*.

2. Ein Element $p \in R$ mit $p \neq 0$ heißt *prim* oder *Primelement*, falls $\langle p \rangle$ ein Primideal ist, d.h. falls $p \notin R^*$ ist und
$$p \mid ab \quad \Rightarrow \quad p \mid a \text{ oder } p \mid b$$
für alle $a, b \in R$ gilt.

Irreduzible Elemente sind also die Elemente, die nur triviale Zerlegungen haben. Einheiten und die Null sind nach Definition weder irreduzibel noch reduzibel. Dass p keine Einheit ist, ist äquivalent zu $\langle p \rangle \neq R$, und diese Bedingung ist Teil der Definition eines Primideals.

Die beiden Begriffe sind nicht identisch, prim ist stärker. Dass prim irreduzibel impliziert, zeigen wir in Satz 2.5.4. Umgekehrt gibt es irreduzible Elemente, die nicht prim sind.

Beispiel 2.5.3: Wir betrachten den Teilring
$$R = \mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\right\}$$
von $\mathbb{C}$. Als Teilring eines Körpers ist R ein Integritätsbereich. Wir behaupten: $3 \in R$ ist irreduzibel, aber nicht prim.

Dazu benutzen wir die *Normabbildung*
$$N \colon R \to \mathbb{Z}_{\geq 0}, \quad a + b\sqrt{-5} \mapsto a^2 + 5b^2,$$
also das Quadrat des komplexen Betrags. Da der komplexe Betrag multiplikativ ist, gilt $N(xy) = N(x)N(y)$ für alle $x, y \in R$. Ist $u \in R^*$, so ist $1 = N(1) = N(u)N(u^{-1})$, also $N(u) = 1$. Umgekehrt hat $a^2 + 5b^2 = 1$ nur die Lösungen $b = 0$, $a = \pm 1$. Die Einheiten von R sind also genau ± 1, und das sind genau die Elemente mit Norm 1.

3 *ist irreduzibel:* Es ist $3 \neq 0$, und wegen $N(3) = 9$ ist 3 keine Einheit. Sei $3 = ab$ mit $a, b \in R$. Dann ist $9 = N(3) = N(a)N(b)$. Die Gleichung $x^2 + 5y^2 = 3$ hat keine ganzzahligen Lösungen, also ist $N(a) \neq 3$. Damit ist $N(a) = 1$ oder $N(b) = 1$, d.h. $a \in R^*$ oder $b \in R^*$.

3 *ist nicht prim:* Es gilt
$$\left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right) = 4 + 5 = 9 = 3 \cdot 3,$$
also $3 \mid \left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right)$. Aber 3 teilt keinen der beiden Faktoren: Aus $2 \pm \sqrt{-5} = 3\left(c + d\sqrt{-5}\right)$ mit $c, d \in \mathbb{Z}$ würde $3c = 2$ folgen.

© 2026 Thomas Kahle

Satz 2.5.4: Sei R ein Hauptidealring und $p \in R$ mit $p \neq 0$ und $p \notin R^*$. Dann ist p genau dann prim, wenn p irreduzibel ist.

Beweis. Sei zunächst p irreduzibel, und seien $a, b \in R$ mit $p \mid ab$. Angenommen, $p \nmid a$. Wir betrachten das Ideal $\langle p, a\rangle$. Da R ein Hauptidealring ist, existiert ein $c \in R$ mit $\langle c\rangle = \langle p, a\rangle$. Insbesondere gilt $c \mid p$ und $c \mid a$, etwa $p = fc$ und $a = gc$. Da p irreduzibel ist, ist $f \in R^*$ oder $c \in R^*$. Wäre $f \in R^*$, so wäre $c = f^{-1}p$ und damit $a = gf^{-1}p$, also $p \mid a$, im Widerspruch zur Annahme. Also ist $c \in R^*$ und damit $\langle p, a\rangle = \langle c\rangle = R$. Insbesondere ist $1 \in \langle p, a\rangle$, d.h. es gibt $u, v \in R$ mit

$$1 = up + va.$$

Multiplikation mit b liefert $b = upb + vab$. Da p beide Summanden auf der rechten Seite teilt, folgt $p \mid b$. Also ist p prim.

Sei nun p prim und $p = ab$ mit $a, b \in R$. Dann gilt $p \mid ab$, also $p \mid a$ oder $p \mid b$, ohne Einschränkung $a = pc$ für ein $c \in R$. Dann ist $p = ab = pcb$, und Kürzen von $p \neq 0$ ergibt $1 = cb$. Also ist $b \in R^*$, und p ist irreduzibel. ∎

Der zweite Teil des Beweises benutzt nicht, dass R ein Hauptidealring ist. Die Implikation „prim $\Rightarrow$ irreduzibel“ gilt also in jedem Integritätsbereich. Da 3 in $\mathbb{Z}\left[\sqrt{-5}\right]$ irreduzibel, aber nicht prim ist, zeigt Satz 2.5.4 außerdem, dass $\mathbb{Z}\left[\sqrt{-5}\right]$ kein Hauptidealring ist.

Was ist nun die richtige Verallgemeinerung der Primfaktorzerlegung?

Definition 2.5.5: Ein *faktorieller Ring* ist ein Integritätsbereich R, in dem sich jedes $r \in R$ mit $r \neq 0$ und $r \notin R^*$ als endliches Produkt

$$r = p_1 \cdots p_n$$

von irreduziblen Elementen $p_1, \ldots, p_n$ schreiben lässt und die Faktoren bis auf Einheiten eindeutig sind. Das heißt: Ist $r = q_1 \cdots q_m$ eine weitere Zerlegung in irreduzible Elemente, so ist $m = n$, und nach Umordnung der q_i existieren Einheiten $u_i \in R^*$ mit $p_i = u_i q_i$ für $i = 1, \ldots, n$.

In $\mathbb{Z}\left[\sqrt{-5}\right]$ ist zum Beispiel

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right),$$

und man zeigt wie in Beispiel 2.5.3 mit der Norm, dass alle vier Faktoren irreduzibel und keine zwei davon assoziiert sind. Also ist $\mathbb{Z}\left[\sqrt{-5}\right]$ nicht faktoriell.

Um auch den ersten Begriff vom Anfang des Abschnitts präzise zu machen, fassen wir die Division mit Rest axiomatisch.

Definition 2.5.6: Ein Integritätsbereich R heißt *euklidischer Ring*, falls es eine Abbildung $\delta\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ gibt, sodass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

$$a = qb + r \quad \text{und} \quad r = 0 \text{ oder } \delta(r) < \delta(b).$$

In $\mathbb{Z}$ leistet das der Betrag $\delta(a) = |a|$, im Polynomring $K[x]$ über einem Körper der Grad, wie wir unten in Proposition 2.6.1 sehen. In einem euklidischen Ring kann man den euklidischen Algorithmus wie in $\mathbb{Z}$ durchführen, um einen größten gemeinsamen Teiler zu bestimmen.

Proposition 2.5.7: Jeder euklidische Ring ist ein Hauptidealring.

Beweis. Sei $I \subseteq R$ ein Ideal. Ist $I = \{0\}$, so ist $I = \langle 0 \rangle$. Andernfalls wählen wir $b \in I \setminus \{0\}$ mit minimalem $\delta(b)$. Sei $a \in I$ beliebig. Wir schreiben $a = qb + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$. Da a und qb in I liegen, ist auch $r = a - qb \in I$. Wegen der Minimalität von $\delta(b)$ ist $r = 0$, also $a = qb \in \langle b \rangle$. Damit ist $I = \langle b \rangle$. ∎

Ohne Beweis halten wir die folgende Hierarchie fest:

$$\{\text{Körper}\} \subsetneq \{\text{euklidische Ringe}\} \subsetneq \{\text{Hauptidealringe}\} \subsetneq \{\text{faktorielle Ringe}\}$$
$$\subsetneq \{\text{Integritätsbereiche}\} \subsetneq \{\text{kommutative Ringe}\}.$$

Die erste Inklusion ist klar (man nimmt $\delta = 1$ und $r = 0$), die zweite ist Proposition 2.5.7, und die vorletzte und letzte sind Definitionen. Dass jeder Hauptidealring faktoriell ist, erfordert etwas mehr Arbeit; Satz 2.5.4 ist dabei der Schlüssel zur Eindeutigkeit. Beispiele, die zeigen, dass die Inklusionen echt sind:

- $\mathbb{Z}$ ist euklidisch, aber kein Körper.
- $\mathbb{Z}\left[\left(1 + \sqrt{-19}\right)/2\right]$ ist ein Hauptidealring, aber nicht euklidisch (ohne Beweis).
- $\mathbb{Z}[x]$ ist faktoriell, aber kein Hauptidealring, denn das Ideal $\langle 2, x \rangle$ ist kein Hauptideal.
- $\mathbb{Z}\left[\sqrt{-5}\right]$ ist ein Integritätsbereich, aber nicht faktoriell.
- $\mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsbereich, denn $\overline{2} \cdot \overline{2} = \overline{0}$.

Ebenfalls ohne Beweis: *Ist R ein Integritätsbereich, so ist $R[x]$ genau dann faktoriell, wenn R faktoriell ist.* Insbesondere sind $\mathbb{Z}[x]$ und $K[x_1, \ldots, x_n]$ für einen Körper K faktoriell.

2.6 Polynomringe über Körpern

Sei in diesem Abschnitt K ein Körper und $K[x]$ der Polynomring über K. Wir wissen bereits:

- $K[x]$ ist ein Integritätsbereich, und für $f, g \neq 0$ gilt $\deg(fg) = \deg(f) + \deg(g)$ (siehe Abschnitt 2.2).

© 2026 Thomas Kahle

- Die Einheiten von $K[x]$ sind genau die konstanten Polynome ungleich Null: $K[x]^* = K^* = K \setminus \{0\}$.

Unser Ziel ist, Körper als Quotienten $K[x]/M$ nach maximalen Idealen M zu konstruieren. Dazu müssen wir verstehen, welche Ideale in $K[x]$ maximal sind. Grundlage dafür ist die Polynomdivision, die zeigt, dass $K[x]$ ein euklidischer Ring ist.

Proposition 2.6.1: Seien $a, b \in K[x]$ mit $b \neq 0$. Dann existieren eindeutige $q, r \in K[x]$ mit

$$a = qb + r \quad \text{und} \quad r = 0 \text{ oder } \deg(r) < \deg(b).$$

Insbesondere ist $K[x]$ mit $\delta = \deg$ ein euklidischer Ring und damit ein Hauptidealring.

Beweis. *Existenz* per Induktion nach dem Grad von a. Ist $a = 0$ oder $\deg(a) < \deg(b)$, so nehmen wir $q = 0$ und $r = a$. Sei nun $n = \deg(a) \geq m = \deg(b)$, und seien a_n und b_m die Leitkoeffizienten. Da K ein Körper ist, ist b_m invertierbar, und das Polynom

$$a' = a - a_n b_m^{-1} x^{n-m} b$$

hat kleineren Grad als a (oder ist Null), denn der Leitterm hebt sich weg. Nach Induktionsvoraussetzung ist $a' = q'b + r$ mit $r = 0$ oder $\deg(r) < \deg(b)$, und mit $q = q' + a_n b_m^{-1} x^{n-m}$ folgt $a = qb + r$.

Eindeutigkeit: Ist $a = qb + r = q'b + r'$, so ist $(q - q')b = r' - r$. Wäre $q \neq q'$, so hätte die linke Seite Grad mindestens $\deg(b)$, die rechte aber kleineren Grad (oder sie wäre Null). Also ist $q = q'$ und damit $r = r'$. Der Zusatz folgt aus Proposition 2.5.7. ∎

Ein Beispiel für die Hierarchie sehen wir hier schon: Über $\mathbb{Z}$ ist der Leitkoeffizient von b im Allgemeinen nicht invertierbar, und tatsächlich ist $\mathbb{Z}[x]$ kein Hauptidealring.

Satz 2.6.2: Sei $f \in K[x]$. Das Ideal $\langle f \rangle \subseteq K[x]$ ist genau dann maximal, wenn f irreduzibel ist. Äquivalent dazu ist, dass $K[x]/\langle f \rangle$ ein Körper ist.

Beweis. Die Äquivalenz zur letzten Aussage ist die Charakterisierung maximaler Ideale durch Quotienten, die Körper sind (siehe Abschnitt 2.4).

Sei $\langle f \rangle$ maximal. Dann ist $\langle f \rangle$ ein Primideal, da jedes maximale Ideal prim ist (siehe Abschnitt 2.4). Außerdem ist $f \neq 0$, denn $\langle 0 \rangle$ ist nicht maximal: Es liegt echt im echten Ideal $\langle x \rangle$. Also ist f prim und damit nach der Bemerkung nach Satz 2.5.4 irreduzibel.

Sei umgekehrt f irreduzibel. Dann ist f keine Einheit, also $\langle f \rangle \neq K[x]$. Sei J ein Ideal mit $\langle f \rangle \subseteq J \subseteq K[x]$. Da $K[x]$ ein Hauptidealring ist, ist $J = \langle g \rangle$ für ein $g \in K[x]$. Wegen

$f \in \langle g \rangle$ ist $f = gh$ für ein $h \in K[x]$. Da f irreduzibel ist, ist entweder $g \in K^*$, also $J = K[x]$, oder $h \in K^*$, also $g = h^{-1}f$ und $J = \langle f \rangle$. Also ist $\langle f \rangle$ maximal. ∎

Der Beweis benutzt von $K[x]$ nur, dass es ein Hauptidealring ist. In jedem Hauptidealring sind die maximalen Ideale also genau die von irreduziblen Elementen erzeugten Ideale; in $\mathbb{Z}$ sind das die Ideale $p\mathbb{Z}$ für Primzahlen p.

Nullstellen und Linearfaktoren hängen eng zusammen.

Proposition 2.6.3: Sei $f \in K[x]$ und $\alpha \in K$. Dann ist α genau dann eine Nullstelle (*Wurzel*) von f, wenn $(x - \alpha) \mid f$ gilt.

Beweis. Gilt $f = (x - \alpha)g$, so ist $f(\alpha) = 0 \cdot g(\alpha) = 0$. Umgekehrt liefert Division mit Rest $f = q \cdot (x - \alpha) + r$ mit $r = 0$ oder $\deg(r) < 1$, also einer Konstanten $r \in K$. Einsetzen von α ergibt $0 = f(\alpha) = r$, also $(x - \alpha) \mid f$. ∎

Insbesondere hat ein irreduzibles Polynom f vom Grad mindestens 2 keine Nullstelle in K, denn eine Nullstelle liefert einen echten Linearfaktor. Die Konstruktion

$$K \to L := K[y]/\langle f(y) \rangle$$

fügt zu K eine Nullstelle von f hinzu. Hier haben wir die Variable y genannt, um sie von der Variablen x des Polynoms $f \in K[x]$ zu unterscheiden. Nach Satz 2.6.2 ist L ein Körper. Die Abbildung $K \to L$, die $c \in K$ auf die Restklasse des konstanten Polynoms c abbildet, ist ein Ringhomomorphismus. Ihr Kern ist ein Ideal von K, das wegen $1 \mapsto \overline{1} \neq \overline{0}$ nicht ganz K ist, also ist der Kern $\{0\}$ und die Abbildung injektiv. Wir fassen deshalb K als Teilkörper von L auf, also $K \subseteq L$, und können $f \in K[x]$ auch als Polynom in $L[x]$ betrachten. Dieses Polynom hat eine Nullstelle in L, nämlich

$$\overline{y} = y + \langle f \rangle.$$

Einsetzen in f ergibt nämlich, weil die Restklassenabbildung ein Ringhomomorphismus ist,

$$f(\overline{y}) = f(y) + \langle f \rangle = 0 + \langle f \rangle = \overline{0} \in L.$$

Beispiel 2.6.4: Sei $K = \mathbb{Q}$. Das Polynom $x^2 - 2$ hat Grad 2 und keine rationale Nullstelle, da $\sqrt{2}$ irrational ist. Es ist also irreduzibel (siehe unten), und

$$\mathbb{Q}[x]/\langle x^2 - 2 \rangle$$

ist ein Körper. In dieser Darstellung spielt die Restklasse von x die Rolle von $\sqrt{2}$, denn

$$\left(x + \langle x^2 - 2 \rangle\right)^2 = x^2 + \langle x^2 - 2 \rangle = 2 + \langle x^2 - 2 \rangle.$$

© 2026 Thomas Kahle

In der Körpertheorie werden wir sehen, dass dieser Körper isomorph zum Teilkörper $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ von $\mathbb{R}$ ist, dem kleinsten Teilkörper von $\mathbb{C}$, der $\mathbb{Q}$ und $\sqrt{2}$ enthält (siehe Abschnitt 3.1).

Hier beginnt eigentlich schon die Körpertheorie. Vorher fragen wir uns aber, welche Polynome in $K[x]$ irreduzibel sind. Aus Proposition 2.6.3 folgt:

Korollar 2.6.5: Ein Polynom $f \in K[x]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle in K hat.

Beweis. Hat f eine Nullstelle, so hat f einen Linearfaktor und ist wegen $\deg(f) \geq 2$ reduzibel. Ist umgekehrt $f = gh$ mit $g, h \notin K^*$, so ist $\deg(g) + \deg(h) = \deg(f) \in \{2, 3\}$ mit $\deg(g), \deg(h) \geq 1$. Also hat einer der beiden Faktoren Grad 1, etwa $g = cx + d$ mit $c \neq 0$, und $-d/c$ ist eine Nullstelle von f. ∎

Ab Grad 4 reicht das nicht mehr: Ein Polynom kann als Produkt von zwei irreduziblen Polynomen vom Grad 2 zerfallen und hat dann keine Nullstelle. Zum Beispiel hat $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ keine rationale Nullstelle, ist aber reduzibel über $\mathbb{Q}$.

Algorithmische und weitere Techniken für die Irreduzibilität betreffen vor allem $K = \mathbb{Q}$. Häufig hat man ein Polynom $p \in \mathbb{Z}[x]$ und fragt, ob p irreduzibel über $\mathbb{Z}$ oder über $\mathbb{Q}$ ist. Für ein Polynom $p = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ mit $p \neq 0$ heißt

$$c(p) := \mathrm{ggT}(a_n, \ldots, a_0) > 0$$

der *Inhalt* von p. Ist $c(p) = 1$, so heißt p *primitiv*. Ist $c(p) > 1$ und $\deg(p) \geq 1$, so faktorisiert p in $\mathbb{Z}[x]$ als

$$p = c(p) \cdot \frac{p}{c(p)}$$

in zwei Nicht-Einheiten und ist damit reduzibel über $\mathbb{Z}$.

Beispiel 2.6.6: Das Polynom $2x^2 - 4 = 2 \cdot (x^2 - 2)$ ist reduzibel in $\mathbb{Z}[x]$, aber irreduzibel in $\mathbb{Q}[x]$, da $2 \in \mathbb{Q}^*$ dort eine Einheit ist.

Die Irreduzibilität über $\mathbb{Z}$ und über $\mathbb{Q}$ hängen wie folgt zusammen.

Lemma 2.6.7: Sind $g, h \in \mathbb{Z}[x]$ primitiv, so ist auch gh primitiv.

thomas.kahle@ovgu.de

Beweis. Angenommen, eine Primzahl q teilt alle Koeffizienten von gh. Wir reduzieren die Koeffizienten modulo q, d.h. wir wenden den Ringhomomorphismus $\mathbb{Z}[x] \to (\mathbb{Z}/q\mathbb{Z})[x]$ an, der jeden Koeffizienten auf seine Restklasse abbildet. Dann ist $\overline{g} \cdot \overline{h} = \overline{gh} = 0$. Da $\mathbb{Z}/q\mathbb{Z}$ ein Körper ist, ist $(\mathbb{Z}/q\mathbb{Z})[x]$ ein Integritätsbereich, also ist $\overline{g} = 0$ oder $\overline{h} = 0$. Dann teilt q alle Koeffizienten von g oder von h, im Widerspruch zur Primitivität. ■

Satz 2.6.8 (Lemma von Gauß): Sei $p \in \mathbb{Z}[x]$ mit $\deg(p) \geq 1$. Dann ist p genau dann irreduzibel in $\mathbb{Z}[x]$, wenn p primitiv und irreduzibel in $\mathbb{Q}[x]$ ist.

Beweis. Jedes $f \in \mathbb{Q}[x]$ mit $f \neq 0$ lässt sich als $f = \lambda f^*$ mit $\lambda \in \mathbb{Q}^*$ und einem primitiven $f^* \in \mathbb{Z}[x]$ schreiben: Man multipliziert mit dem Hauptnenner der Koeffizienten und teilt dann durch den Inhalt.

Sei p primitiv und irreduzibel in $\mathbb{Q}[x]$, und sei $p = gh$ mit $g, h \in \mathbb{Z}[x]$. Da p in $\mathbb{Q}[x]$ irreduzibel ist, ist g oder h eine Einheit in $\mathbb{Q}[x]$, also konstant, etwa $g = c \in \mathbb{Z}$. Dann teilt c alle Koeffizienten von p, und da p primitiv ist, folgt $c = \pm 1 \in \mathbb{Z}[x]^*$. Da p wegen $\deg(p) \geq 1$ keine Einheit ist, ist p irreduzibel in $\mathbb{Z}[x]$.

Sei umgekehrt p irreduzibel in $\mathbb{Z}[x]$. Nach der Vorbemerkung zum Inhalt ist p primitiv. Wegen $\deg(p) \geq 1$ ist p in $\mathbb{Q}[x]$ weder Null noch eine Einheit. Angenommen, $p = gh$ mit $g, h \in \mathbb{Q}[x]$ vom Grad mindestens 1. Wir schreiben $g = \lambda g^*$ und $h = \mu h^*$ wie oben. Dann ist $p = \lambda\mu g^* h^*$, und $g^* h^*$ ist nach Lemma 2.6.7 primitiv. Schreiben wir $\lambda\mu = r/s$ mit teilerfremden $r, s \in \mathbb{Z}$, $s > 0$, so ist $sp = rg^* h^*$. Vergleich der Inhalte beider Seiten ergibt $s = |r|$, also $\lambda\mu = \pm 1$. Damit ist $p = \pm g^* h^*$ eine Zerlegung in $\mathbb{Z}[x]$ in zwei Faktoren vom Grad mindestens 1, also in zwei Nicht-Einheiten. Das widerspricht der Irreduzibilität von p in $\mathbb{Z}[x]$. ■

Das wichtigste Werkzeug, um die Irreduzibilität konkreter Polynome nachzuweisen, ist das folgende Kriterium.

Satz 2.6.9 (Eisensteinkriterium): Sei p eine Primzahl und

$$a = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

mit $n \geq 1$ und
- $p \nmid a_n$,
- $p \mid a_i$ für $i = 0, \ldots, n-1$,
- $p^2 \nmid a_0$.

Dann ist a irreduzibel in $\mathbb{Q}[x]$. Ist a zusätzlich primitiv, so ist a auch irreduzibel in $\mathbb{Z}[x]$.

Beweis. Teilen wir a durch seinen Inhalt $c(a)$, so bleiben die Voraussetzungen erhalten: Wegen $p \nmid a_n$ ist $p \nmid c(a)$. Außerdem ändert sich die Irreduzibilität in $\mathbb{Q}[x]$ nicht, da $c(a)$ dort eine Einheit ist. Wir dürfen also annehmen, dass a primitiv ist. Nach Satz 2.6.8 genügt es dann zu zeigen, dass a in $\mathbb{Z}[x]$ irreduzibel ist.

Angenommen, $a = bc$ mit Nicht-Einheiten $b, c \in \mathbb{Z}[x]$. Wäre b konstant, so würde b alle Koeffizienten von a teilen, also $b = \pm 1$, was keine Nicht-Einheit ist. Also sind b und c nicht konstant, sagen wir $b = b_r x^r + \ldots + b_0$ und $c = c_s x^s + \ldots + c_0$ mit $r, s \geq 1$ und $r + s = n$.

Wir betrachten die Reduktion modulo p, also den Ringhomomorphismus $\mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$. Aus $a = bc$ folgt $\overline{a} = \overline{b} \cdot \overline{c}$. Nach Voraussetzung ist $\overline{a} = \overline{a_n} x^n$ mit $\overline{a_n} \neq \overline{0}$. Wegen $b_r c_s = a_n$ ist $p \nmid b_r$ und $p \nmid c_s$, also haben $\overline{b}$ und $\overline{c}$ die Grade r und s. Sei i minimal mit $\overline{b_i} \neq \overline{0}$ und j minimal mit $\overline{c_j} \neq \overline{0}$. Dann ist der Koeffizient von x^{i+j} in $\overline{b} \cdot \overline{c}$ gleich $\overline{b_i} \cdot \overline{c_j} \neq \overline{0}$, da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist. Also ist $i + j = n = r + s$, und wegen $i \leq r$, $j \leq s$ folgt $i = r \geq 1$ und $j = s \geq 1$. Insbesondere sind $\overline{b_0} = \overline{0}$ und $\overline{c_0} = \overline{0}$, d.h. $p \mid b_0$ und $p \mid c_0$. Dann gilt aber $p^2 \mid b_0 c_0 = a_0$, im Widerspruch zur Voraussetzung. Also ist a irreduzibel. ∎

Manchmal kann man das Eisensteinkriterium direkt anwenden.

Beispiel 2.6.10: Das Polynom $x^4 + 10x + 5 \in \mathbb{Z}[x]$ ist irreduzibel nach Satz 2.6.9 mit $p = 5$. Ebenso ist $x^n - 2$ für jedes $n \geq 1$ irreduzibel über $\mathbb{Q}$ (mit $p = 2$).

Falls das Eisensteinkriterium nicht direkt anwendbar ist, kann man versuchen, einen Ringautomorphismus $\mathbb{Z}[x] \to \mathbb{Z}[x]$ anzuwenden, zum Beispiel $f(x) \mapsto f(x + k)$ für ein $k \in \mathbb{Z}$. Das ist ein Ringhomomorphismus mit der Umkehrabbildung $f(x) \mapsto f(x - k)$, und Ringisomorphismen bilden irreduzible Elemente auf irreduzible Elemente ab. Also ist $f(x)$ genau dann irreduzibel, wenn $f(x + k)$ es ist.

Beispiel 2.6.11: Sei p eine Primzahl. Das Polynom

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

heißt das p-te *Kreisteilungspolynom*. Auf Φ_p selbst ist Eisenstein nicht anwendbar, denn kein Koeffizient ist durch eine Primzahl teilbar. Wir betrachten deshalb

$$\begin{aligned}\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} &= \frac{x^p + \binom{p}{p-1} x^{p-1} + \ldots + \binom{p}{1} x + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{p-1} x^{p-2} + \ldots + \binom{p}{2} x + \binom{p}{1}.\end{aligned}$$

thomas.kahle@ovgu.de

Für $1 \leq k \leq p-1$ ist $p \mid \binom{p}{k}$, denn p teilt $p! = \binom{p}{k} \cdot k! \cdot (p-k)!$, aber nicht $k!(p-k)!$. Der Leitkoeffizient ist 1, und der konstante Term ist $\binom{p}{1} = p$, also nicht durch p^2 teilbar. Das Eisensteinkriterium mit der Primzahl p zeigt also, dass $\Phi_p(x+1)$ und damit Φ_p irreduzibel ist.

Darüber hinaus kann man mit Computeralgebra testen, ob Polynome in $\mathbb{Q}[x]$ irreduzibel sind, bzw. ihre Faktorisierungen bestimmen.

3 Körpertheorie

Ein *Körper* ist ein kommutativer Ring K mit $1 \neq 0$, in dem jedes Element außer der Null invertierbar ist, also $K^* = K \setminus \{0\}$ gilt. Körper haben nur die beiden trivialen Ideale $\langle 0 \rangle$ und K. Daher gibt es kaum Quotienten, und die interessante Struktur liegt woanders: im Verhältnis eines Körpers zu seinen Teilkörpern und Erweiterungskörpern. Das zentrale Thema dieses Kapitels sind daher *Körpererweiterungen* und ihr Zusammenhang mit Nullstellen von Polynomen. Am Ende werden wir in einem Ausblick sehen, wie die Gruppentheorie aus dem ersten Kapitel hilft, Körpererweiterungen zu verstehen.

3.1 Charakteristik und Körpererweiterungen

Die Charakteristik

Wir beginnen mit einer Invariante, die jeder Ring und insbesondere jeder Körper hat.

Definition 3.1.1: Sei R ein Ring. Die *Charakteristik* $\operatorname{char}(R)$ ist die kleinste positive ganze Zahl n mit

$$\underbrace{1+1+\ldots+1}_{n \text{ mal}} = 0,$$

oder $\operatorname{char}(R) = 0$, falls alle solchen Summen von Einsen ungleich Null sind.

Jeder Ring R besitzt genau einen Ringhomomorphismus $\mathbb{Z} \to R$: Er muss $1 \in \mathbb{Z}$ auf $1 \in R$ abbilden und ist dadurch eindeutig festgelegt, nämlich durch

$$n \mapsto n \cdot 1 := \underbrace{1+\ldots+1}_{n \text{ mal}} \quad \text{für } n > 0, \quad 0 \mapsto 0, \quad -n \mapsto -(n \cdot 1).$$

Allgemeiner schreiben wir für $n \in \mathbb{Z}$ und $a \in R$ kurz $na := a + \ldots + a$ (n Summanden), wie bei additiven Gruppen in Abschnitt 1.1. Der Kern des Homomorphismus $\mathbb{Z} \to R$ ist ein Ideal von $\mathbb{Z}$, also von der Form $n\mathbb{Z}$ für genau ein $n \geq 0$, und dieses n ist genau die Charakteristik:

$$\ker(\mathbb{Z} \to R) = \operatorname{char}(R)\mathbb{Z}.$$

Die Charakteristik ist also der nichtnegative Erzeuger des Kerns. (Für den Nullring ist $\operatorname{char}(R) = 1$; dieser Fall ist uninteressant.)

Proposition 3.1.2: Ist R ein Integritätsbereich, so ist $\operatorname{char}(R)$ eine Primzahl oder Null.

Beweis. Nach dem Homomorphiesatz für Ringe ist $\mathbb{Z}/\ker(\mathbb{Z} \to R)$ isomorph zum Bild von $\mathbb{Z} \to R$. Das Bild ist ein Teilring des Integritätsbereichs R und damit selbst ein Integritätsbereich. Also ist $\ker(\mathbb{Z} \to R)$ ein Primideal von $\mathbb{Z}$ (ein Ideal ist genau dann prim, wenn der Quotient ein Integritätsbereich ist, siehe Proposition 2.4.6). Die Primideale von $\mathbb{Z}$ sind $\langle 0 \rangle$ und $p\mathbb{Z}$ für Primzahlen p. Also ist $\operatorname{char}(R) = 0$ oder $\operatorname{char}(R) = p$. ∎

Beispiel 3.1.3:
- $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ haben Charakteristik Null, denn sie enthalten $\mathbb{Z}$.
- $\mathbb{Z}/p\mathbb{Z}$ hat für eine Primzahl p die Charakteristik p. Man spricht hier auch gern von *endlicher Charakteristik*.
- Es gibt weitere Körper positiver Charakteristik. Zum Beispiel ist $x^2 + x + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ irreduzibel, denn weder 0 noch 1 ist eine Nullstelle, und ein reduzibles Polynom vom Grad 2 hätte einen Linearfaktor. Damit ist $(\mathbb{Z}/2\mathbb{Z})[x]/\langle x^2 + x + 1 \rangle$ ein Körper der Charakteristik 2. Wie wir gleich in Satz 3.1.10 sehen, hat er 4 Elemente.
- Es gibt auch unendliche Körper mit endlicher Charakteristik, zum Beispiel den Körper $(\mathbb{Z}/2\mathbb{Z})(t)$ der rationalen Funktionen mit Koeffizienten in $\mathbb{Z}/2\mathbb{Z}$ oder den algebraischen Abschluss von $\mathbb{Z}/2\mathbb{Z}$, den wir später kennenlernen (siehe Abschnitt 3.4).

Endliche Körper mit q Elementen werden gerne mit $\mathbb{F}_q$ bezeichnet. Wir werden später sehen, dass q dabei stets eine Primzahlpotenz ist und dass es zu jeder Primzahlpotenz bis auf Isomorphie genau einen solchen Körper gibt (siehe Abschnitt 3.5). Insbesondere ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für Primzahlen p.

Definition 3.1.4: Ein *Teilkörper* eines Körpers L ist ein Teilring $K \subseteq L$, der selbst ein Körper ist.

Proposition 3.1.5: Jeder Körper K enthält einen kleinsten Teilkörper, den *Primkörper* von K. Er ist isomorph zu $\mathbb{Q}$, falls $\operatorname{char}(K) = 0$, und isomorph zu $\mathbb{F}_p$, falls $\operatorname{char}(K) = p$ ist.

thomas.kahle@ovgu.de

Beweis. Sei $\varphi\colon \mathbb{Z} \to K$ der eindeutige Ringhomomorphismus. Jeder Teilkörper von K enthält die 1 und damit das Bild $\varphi(\mathbb{Z})$. Nach dem Homomorphiesatz gilt $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\operatorname{char}(K)\mathbb{Z}$, und nach Proposition 3.1.2 ist $\operatorname{char}(K) = 0$ oder eine Primzahl p, denn Körper sind Integritätsbereiche.

Ist $\operatorname{char}(K) = p$, so ist $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ bereits ein Körper und damit der kleinste Teilkörper.

Ist $\operatorname{char}(K) = 0$, so ist φ injektiv und $\varphi(\mathbb{Z}) \cong \mathbb{Z}$ kein Körper. Ein Teilkörper, der $\varphi(\mathbb{Z})$ enthält, enthält aber auch alle Inversen $\varphi(b)^{-1}$ für $b \neq 0$ und damit alle „Brüche“ $\varphi(a)\varphi(b)^{-1}$. Die Abbildung

$$\mathbb{Q} \to K, \quad \frac{a}{b} \mapsto \varphi(a)\varphi(b)^{-1}$$

ist wohldefiniert (aus $\frac{a}{b} = \frac{a'}{b'}$ folgt $\varphi(a)\varphi(b') = \varphi(a')\varphi(b)$) und ein injektiver Ringhomomorphismus. Ihr Bild ist ein zu $\mathbb{Q}$ isomorpher Teilkörper, der in jedem Teilkörper von K enthalten ist. ∎

Körpererweiterungen

Definition 3.1.6: Eine *Körpererweiterung* L/K ist eine Inklusion $K \subseteq L$ von Körpern K, L, d.h. K ist ein Teilkörper von L. Man nennt L einen *Erweiterungskörper* von K und schreibt auch

$$\begin{array}{c} L \\ | \\ K \end{array}$$

Dazu einige Bemerkungen.

- Jeder Körper ist eine Erweiterung seines Primkörpers.
- **Achtung!** Die Schreibweise L/K bezeichnet keinen Quotienten. Das ist unproblematisch, denn Körper haben nur triviale Ideale, und Quotienten von Körpern spielen keine Rolle.
- *Körperhomomorphismen* sind Ringhomomorphismen zwischen Körpern. Sie sind stets injektiv: Der Kern ist ein Ideal, also $\langle 0 \rangle$ oder der ganze Körper, und Letzteres ist wegen $\varphi(1) = 1 \neq 0$ ausgeschlossen. Deshalb identifizieren wir einen Körper K oft mit seinem Bild unter einem Homomorphismus $K \to L$ und schreiben einfach $K \subseteq L$. **Achtung!** Später werden wir verschiedene Isomorphismen $K \to K$ unterscheiden wollen. Dann muss man mit dieser Identifikation vorsichtig sein.
- Ist $K \subseteq L$, so ist L ein K-Vektorraum: $(L, +)$ ist eine abelsche Gruppe, und die Skalarmultiplikation $K \times L \to L$ ist einfach die Multiplikation in L. Die Vektorraumaxiome folgen aus den Ringaxiomen von L.

Damit stehen uns die Begriffe der linearen Algebra zur Verfügung.

© 2026 Thomas Kahle

Definition 3.1.7: Der *Grad* einer Körpererweiterung L/K, geschrieben $[L : K]$, ist $\dim_K L$, die Dimension von L als K-Vektorraum. Falls $[L : K] < \infty$ ist, heißt L/K eine *endliche Körpererweiterung*, andernfalls eine *unendliche Körpererweiterung*.

Beispiel 3.1.8:
- $\mathbb{C}/\mathbb{R}$ ist eine endliche Erweiterung vom Grad 2, denn $\mathbb{C} = \mathbb{R} + i\mathbb{R}$ ist ein zweidimensionaler $\mathbb{R}$-Vektorraum mit Basis $\{1, i\}$. Die Zahl i ist eine Nullstelle von $x^2 + 1 \in \mathbb{R}[x]$, und es gilt $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$ (siehe die Übung nach Proposition 3.1.9).
- $\mathbb{R}/\mathbb{Q}$ ist eine unendliche Erweiterung. Wäre nämlich $[\mathbb{R} : \mathbb{Q}] = n < \infty$, so wäre $\mathbb{R} \cong \mathbb{Q}^n$ als $\mathbb{Q}$-Vektorraum und damit abzählbar.

Wir werden sehen, dass endliche Körpererweiterungen immer durch das „Lösen von Polynomgleichungen“ entstehen, nämlich durch Konstruktionen der Form $K[x]/\langle p\rangle$ mit irreduziblen Polynomen p. Diese Konstruktion untersuchen wir jetzt.

Nullstellen hinzufügen

Proposition 3.1.9: Sei K ein Körper und $p \in K[x]$ irreduzibel. Dann ist $L = K[x]/\langle p\rangle$ ein Körper, der K erweitert und in dem p eine Nullstelle hat, nämlich die Restklasse $\overline{x} = x + \langle p\rangle$.

Beweis. Da p irreduzibel ist, ist $\langle p\rangle$ ein maximales Ideal von $K[x]$ und L daher ein Körper (siehe Abschnitt 2.6). Sei

$$\pi\colon K[x] \to L, \quad f \mapsto \overline{f} := f + \langle p\rangle$$

die kanonische Projektion und $\varphi := \pi|_K\colon K \to L$ ihre Einschränkung auf die konstanten Polynome. Dann ist φ ein Körperhomomorphismus (wegen $\varphi(1) = 1$ nicht Null) und damit injektiv. Also erweitert L den Körper K, wenn wir K mit $\varphi(K)$ identifizieren.

Sei $\overline{x} = \pi(x) = x + \langle p\rangle \in L$. Mittels $K \subseteq L$ fassen wir $p = \sum_i a_i x^i$ als Polynom in $L[y]$ auf und setzen $\overline{x}$ ein. Da π ein Ringhomomorphismus ist, erhalten wir

$$p(\overline{x}) = \sum_i a_i \overline{x}^i = \overline{\sum_i a_i x^i} = \overline{p} = p + \langle p\rangle = 0 + \langle p\rangle.$$

Also ist $\overline{x}$ eine Nullstelle von p in L. ∎

Übung. Probieren Sie die Konstruktion mit $\mathbb{C}/\mathbb{R}$ aus: Zeigen Sie, dass $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$ gilt, wobei $\overline{x}$ auf i abgebildet wird.

thomas.kahle@ovgu.de

Man beachte, dass p in L nur *eine* Nullstelle garantiert hat; im Allgemeinen zerfällt p in $L[x]$ nicht in Linearfaktoren (siehe Beispiel 3.1.11 unten). Man kann den Prozess aber mit den verbleibenden Faktoren wiederholen und so einen sogenannten *Zerfällungskörper* konstruieren, über dem p in Linearfaktoren zerfällt. Dieser ist bis auf Isomorphie eindeutig, wie wir später zeigen werden (siehe Abschnitt 3.4).

Satz 3.1.10: Sei $p \in K[x]$ irreduzibel vom Grad n, sei $L = K[x]/\langle p\rangle$ und $\theta = x + \langle p\rangle \in L$. Dann ist $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ eine K-Basis von L. Insbesondere ist

$$[L : K] = n = \deg(p).$$

Beweis. Sei $a \in K[x]$ beliebig. Die Division mit Rest durch p liefert einen kanonischen Repräsentanten von $\overline{a} \in L$: Wir schreiben

$$a = qp + r \quad \text{mit } \deg(r) < \deg(p) = n.$$

Also ist $a \equiv r \bmod p$, d.h. $\overline{a} = \overline{r}$. Wegen $r \in \operatorname{span}\{1, x, ..., x^{n-1}\}$ ist $\overline{a} = \overline{r} \in \operatorname{span}\{1, \theta, ..., \theta^{n-1}\}$. Also erzeugen $1, \theta, ..., \theta^{n-1}$ den K-Vektorraum L.

Sie sind auch linear unabhängig: Angenommen,

$$b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1} = 0 \quad \text{in } L$$

mit $b_i \in K$. Das bedeutet, dass p das Polynom $b = b_0 + b_1 x + ... + b_{n-1}x^{n-1}$ teilt. Wegen $\deg(b) < n = \deg(p)$ geht das nur für $b = 0$, also $b_0 = b_1 = ... = b_{n-1} = 0$. ∎

Für die Basisaussage haben wir die Irreduzibilität von p gar nicht benutzt; sie gilt für jedes p vom Grad $n \geq 1$. Die Irreduzibilität braucht man dafür, dass L ein Körper ist.

Mit Satz 3.1.10 kann man in L gut rechnen:

- Die Addition ist die Vektorraumaddition bezüglich der Basis $1, \theta, ..., \theta^{n-1}$.
- Zur Multiplikation fasst man zwei Elemente $\overline{f}, \overline{g}$ als Linearkombinationen von $1, \theta, ..., \theta^{n-1}$ auf, multipliziert als Polynome und bildet dann wieder den Rest modulo p. Ist $p = x^n + p_{n-1}x^{n-1} + ... + p_0$ normiert, so gilt

  $$\theta^n = -p_{n-1}\theta^{n-1} - ... - p_1\theta - p_0,$$

  und damit lässt sich jede Potenz von θ in der Basis ausdrücken.
- Die Inversion geht mit dem euklidischen Algorithmus: Ist $0 \neq f \in \operatorname{span}\{1, x, ..., x^{n-1}\}$, so ist $\operatorname{ggT}(f, p) = 1$, denn p ist irreduzibel und $\deg(f) < \deg(p)$. Der erweiterte euklidische Algorithmus liefert $a, b \in K[x]$ mit

  $$1 = af + bp$$

  (Lemma von Bézout), und damit ist $\overline{a}\overline{f} = \overline{1}$, also $\overline{a}$ das Inverse von $\overline{f}$ in L.

© 2026 Thomas Kahle

Beispiel 3.1.11: Sei $K = \mathbb{Q}$ und $p = x^3 - 2$. Das Polynom ist irreduzibel nach dem Eisensteinkriterium mit der Primzahl 2 (siehe Abschnitt 2.6). Sei $L = \mathbb{Q}[x]/\langle x^3 - 2\rangle$ und $\theta = \overline{x}$. Dann ist $[L : \mathbb{Q}] = 3$, und L hat die Basis $\{1, \theta, \theta^2\}$. Wegen $\theta^3 = 2$ bietet es sich an, θ mit $\sqrt[3]{2}$ zu bezeichnen; dass das gerechtfertigt ist, zeigt Satz 3.1.14 unten: L ist isomorph zum Teilkörper $\mathbb{Q}\big(\sqrt[3]{2}\big) \subseteq \mathbb{R}$.

Als Beispiel für die Inversion berechnen wir $(1+\theta)^{-1}$. Hier sieht man es sogar ohne euklidischen Algorithmus: Es ist $(1+\theta)(1-\theta+\theta^2) = 1+\theta^3 = 3$, also

$$(1+\theta)^{-1} = \frac{1}{3}(1-\theta+\theta^2).$$

In $L[x]$ zerfällt $x^3 - 2$ als

$$x^3 - 2 = (x-\theta)(x^2+\theta x+\theta^2).$$

Der quadratische Faktor hat keine Nullstelle in L: Fasst man L als Teilkörper von $\mathbb{R}$ auf, so ist seine Diskriminante $\theta^2 - 4\theta^2 = -3\theta^2 < 0$. Also ist L nicht der Zerfällungskörper von $x^3 - 2$. Es fehlen die beiden anderen Nullstellen $\sqrt[3]{2}\omega$ und $\sqrt[3]{2}\omega^2$ in $\mathbb{C}$, wobei $\omega = e^{2\pi i/3}$ eine dritte Einheitswurzel ist (siehe Abbildung 6).

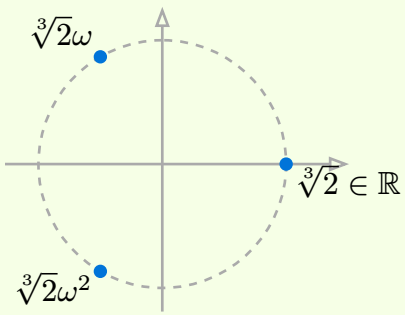


Abbildung 6: Die drei komplexen Nullstellen von $x^3 - 2$.

Adjunktion

Wir können also zu einem Körper K eine Nullstelle eines irreduziblen Polynoms $p \in K[x]$ „aus dünner Luft“ hinzufügen, indem wir $L = K[x]/\langle p\rangle$ bilden. Was passiert, wenn die Nullstelle schon in K enthalten ist?

Beispiel 3.1.12: Sei $K = \mathbb{Q}$. Können wir 2 noch einmal hinzufügen? Dazu betrachten wir $p = x - 2 \in \mathbb{Q}[x]$. Das Polynom ist irreduzibel und hat 2 als Nullstelle. Für $L = \mathbb{Q}[x]/\langle x-2\rangle$ gilt nach Satz 3.1.10 $[L : \mathbb{Q}] = 1$, also $L \cong \mathbb{Q}$. Konkret: Die Division mit Rest durch $x - 2$ ist einfach das „Einsetzen von 2“, zum Beispiel $x = 1 \cdot (x-2) + 2$. Die Abbildung

$$L \to \mathbb{Q}, \quad \overline{x} \mapsto 2, \quad \overline{1} \mapsto 1$$

thomas.kahle@ovgu.de

ist ein Körperhomomorphismus und surjektiv, also ein Isomorphismus. Es entsteht also nichts Neues.

Wir betrachten nun Erweiterungen L/K genauer. Ist zum Beispiel $\alpha \in L$, so gibt es einen kleinsten Teilkörper von L, der K und α enthält. Dazu wieder der übliche Trick: Die Menge der Teilkörper von L, die K und α enthalten, ist nicht leer, denn L selbst gehört dazu. Wir bilden ihren Schnitt.

Übung. Zeigen Sie, dass der Schnitt einer beliebigen nichtleeren Familie von Teilkörpern eines Körpers L wieder ein Teilkörper ist.

Definition 3.1.13: Sei L/K eine Körpererweiterung, I eine Indexmenge und $\alpha_i \in L$ für $i \in I$. Der von den α_i über K *erzeugte Teilkörper* ist

$$K(\alpha_i \colon i \in I) := \bigcap_{\substack{G \subseteq L \text{ Teilkörper} \\ K \subseteq G \\ \{\alpha_i \colon i \in I\} \subseteq G}} G.$$

Man sagt auch „K adjungiert die α_i“. Ist I endlich, so schreibt man $K(\alpha_1, ..., \alpha_n)$. Eine Erweiterung L/K heißt *einfach*, falls $L = K(\alpha)$ für ein $\alpha \in L$ gilt. Ein solches α heißt dann *primitives Element* der Erweiterung.

Man kann zeigen, dass jedenfalls in Charakteristik 0 jede endliche Erweiterung einfach ist (*Satz vom primitiven Element*): Ist $[L : K] < \infty$, so existiert ein $\alpha \in L$ mit $L = K(\alpha)$. Die Umkehrung gilt nicht: Eine einfache Erweiterung muss nicht endlich sein. In $\mathbb{Q}(\pi) \subseteq \mathbb{R}$ sind zum Beispiel alle Potenzen $1, \pi, \pi^2, ...$ linear unabhängig über $\mathbb{Q}$, da π nicht Nullstelle eines Polynoms mit rationalen Koeffizienten ist (Satz von Lindemann). Also ist $\mathbb{Q}(\pi)/\mathbb{Q}$ einfach, aber unendlich.

Unser Ziel ist nun, das Verhältnis von $K(\alpha)$ und $K[x]/\langle p \rangle$ besser zu verstehen, wenn α eine Nullstelle von p ist. Zum Beispiel haben wir $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{R}$ durch Definition 3.1.13 definiert, aber wir würden auch gerne $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ mit $\mathbb{Q}\left(\sqrt{2}\right)$ bezeichnen. Das rechtfertigen wir jetzt.

Satz 3.1.14: Sei K ein Körper und $p \in K[x]$ irreduzibel. Sei L/K eine Erweiterung, die eine Nullstelle α von p enthält, d.h. fasst man p als Polynom in $L[x]$ auf, so gilt $p(\alpha) = 0$. Sei $K(\alpha) \subseteq L$ der von α über K erzeugte Teilkörper. Dann ist

$$K(\alpha) \cong K[x]/\langle p \rangle.$$

© 2026 Thomas Kahle

Genauer ist $K[x]/\langle p\rangle \to K(\alpha)$, $\overline{x} \mapsto \alpha$, ein Isomorphismus, der auf K die Identität ist.

Beweis. Wir betrachten den Einsetzungshomomorphismus

$$\varphi\colon K[x] \to K(\alpha) \subseteq L, \quad a \mapsto a(\alpha).$$

Er bildet tatsächlich nach $K(\alpha)$ ab, denn $K(\alpha)$ ist ein Teilkörper, der K und α enthält und daher unter Addition und Multiplikation abgeschlossen ist. Es gilt:

- $\varphi|_K\colon K \to K(\alpha)$ ist die Identität auf K,
- $\varphi(x) = \alpha$,
- φ ist ein Ringhomomorphismus.

Nach Voraussetzung ist $\varphi(p) = p(\alpha) = 0$, also $\langle p\rangle \subseteq \ker(\varphi)$. Daher ist

$$\overline{\varphi}\colon K[x]/\langle p\rangle \to K(\alpha), \quad \overline{a} \mapsto a(\alpha),$$

wohldefiniert, denn zwei Repräsentanten von $\overline{a}$ unterscheiden sich um ein Vielfaches von p, und dieses wird auf 0 abgebildet. Insbesondere ist $\overline{\varphi}(\overline{x}) = \alpha$.

Nun ist $K[x]/\langle p\rangle$ ein Körper und $\overline{\varphi}$ ein Körperhomomorphismus, also injektiv. Sein Bild ist ein Teilkörper von $K(\alpha)$, der K und α enthält, und damit nach Definition von $K(\alpha)$ gleich $K(\alpha)$. Also ist $\overline{\varphi}$ auch surjektiv. ∎

Zusammen mit Satz 3.1.10 erhalten wir eine explizite Beschreibung: Ist $\alpha \in L$ eine Nullstelle des irreduziblen Polynoms $p \in K[x]$ vom Grad n, so ist

$$K(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}\colon a_0, \ldots, a_{n-1} \in K\} \subseteq L$$

und $[K(\alpha) : K] = n$.

Fortsetzung von Isomorphismen

Eine wichtige Konsequenz von Satz 3.1.14 ist, dass die Nullstellen eines irreduziblen Polynoms mit den Mitteln der abstrakten Körpertheorie nicht zu unterscheiden sind. Die Idee ist: Sind α und β beide Nullstellen von p, so sind $K(\alpha)$ und $K(\beta)$ beide isomorph zu $K[x]/\langle p\rangle$. Wir formulieren das etwas allgemeiner.

Sei $\varphi\colon K \to K'$ ein Isomorphismus von Körpern. Dann erhält man einen Ringisomorphismus

$$\varphi\colon K[x] \to K'[x], \quad \sum_i a_i x^i \mapsto \sum_i \varphi(a_i)x^i$$

durch Anwenden von φ auf die Koeffizienten (wir bezeichnen ihn wieder mit φ). Da Isomorphismen Faktorisierungen erhalten, gilt: $p \in K[x]$ ist genau dann irreduzibel, wenn $\varphi(p)$ in $K'[x]$ irreduzibel ist. Gleichbedeutend: $\langle p\rangle$ ist genau dann maximal, wenn $\varphi(\langle p\rangle) = \langle\varphi(p)\rangle$ maximal ist. Insbesondere induziert φ einen Isomorphismus

$$K[x]/\langle p\rangle \to K'[x]/\langle\varphi(p)\rangle, \quad \overline{x} \mapsto \overline{x}.$$

Satz 3.1.15: Sei $\varphi\colon K \to K'$ ein Isomorphismus von Körpern, $p \in K[x]$ irreduzibel und $p' = \varphi(p) \in K'[x]$. Sei α eine Nullstelle von p in einem Erweiterungskörper von K und β eine Nullstelle von p' in einem Erweiterungskörper von K'. Dann existiert ein Isomorphismus

$$\sigma\colon K(\alpha) \to K'(\beta), \quad \alpha \mapsto \beta,$$

der auf K mit φ übereinstimmt, d.h. $\sigma|_K = \varphi$.

Beweis. Nach Satz 3.1.14 und der Vorüberlegung haben wir Isomorphismen

$$K(\alpha) \cong K[x]/\langle p\rangle \cong K'[x]/\langle p'\rangle \cong K'(\beta),$$

die $\alpha \mapsto \overline{x} \mapsto \overline{x} \mapsto \beta$ abbilden. Auf K sind der erste und der letzte die Identität und der mittlere ist φ. Ihre Komposition ist das gesuchte σ. ∎

Insbesondere liefert der Fall $\varphi = \mathrm{id}\colon K \to K$ die Ununterscheidbarkeit von Nullstellen:

Korollar 3.1.16: Sind α und β Nullstellen desselben irreduziblen Polynoms $p \in K[x]$ (in Erweiterungskörpern von K), so gibt es einen Isomorphismus $K(\alpha) \to K(\beta)$ mit $\alpha \mapsto \beta$, der auf K die Identität ist.

Beispiel 3.1.17: Die Körper $\mathbb{Q}\big(\sqrt[3]{2}\big) \subseteq \mathbb{R}$ und $\mathbb{Q}\big(\sqrt[3]{2}\omega\big) \subseteq \mathbb{C}$ aus Beispiel 3.1.11 sind isomorph, obwohl der erste in $\mathbb{R}$ liegt und der zweite nicht. Ebenso gibt es einen Isomorphismus $\mathbb{Q}\big(\sqrt{2}\big) \to \mathbb{Q}\big(\sqrt{2}\big)$ mit $\sqrt{2} \mapsto -\sqrt{2}$, denn $\sqrt{2}$ und $-\sqrt{2}$ sind Nullstellen von $x^2 - 2$.

Aber: Verschiedene Einbettungen $K(\alpha) \hookrightarrow L$ in einen festen Erweiterungskörper L kann man sehr wohl unterscheiden und zählen. Zum Beispiel gibt es genau drei Einbettungen $\mathbb{Q}\big(\sqrt[3]{2}\big) \hookrightarrow \mathbb{C}$, je eine für jede Nullstelle von $x^3 - 2$ in $\mathbb{C}$, aber nur eine Einbettung $\mathbb{Q}\big(\sqrt[3]{2}\big) \hookrightarrow \mathbb{R}$. Das Zählen solcher Einbettungen wird in der Galoistheorie wichtig (siehe Abschnitt 3.6).

3.2 Algebraische Erweiterungen

Wir haben gesehen, dass man zu einem irreduziblen Polynom $p \in K[x]$ eine Erweiterung $K[x]/\langle p\rangle$ bauen kann, in der p eine Nullstelle hat (siehe Abschnitt 3.1). Nun drehen wir die Blickrichtung um: Gegeben ist eine Erweiterung L/K und ein Element $\alpha \in L$. Gibt es überhaupt ein Polynom über K, das α als Nullstelle hat?

© 2026 Thomas Kahle

Definition 3.2.1: Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *algebraisch* über K, falls ein Polynom $p \in K[x]$ mit $p \neq 0$ existiert, sodass $p(\alpha) = 0$ gilt. Andernfalls heißt α *transzendent* über K.

Die Erweiterung L/K heißt *algebraisch*, falls jedes $\alpha \in L$ algebraisch über K ist.

Beispiel 3.2.2: Die *algebraischen Zahlen* sind alle komplexen Zahlen, die über $\mathbb{Q}$ algebraisch sind, die sich also als Nullstellen von Polynomen mit rationalen Koeffizienten schreiben lassen. Zum Beispiel sind $\sqrt{2}$, $\sqrt[3]{5}$ und i algebraische Zahlen. Die algebraischen Zahlen bilden einen Teilkörper von $\mathbb{C}$. Das ist nicht offensichtlich, denn warum sollte $\sqrt{2} + \sqrt[3]{5}$ wieder Nullstelle eines rationalen Polynoms sein? Der Beweis wird aber bald ganz leicht (Korollar 3.2.16).

Ob ein Element algebraisch ist, hängt nur von K ab und fast gar nicht von L: Ist etwa $L' \supseteq L \supseteq K$ und $\alpha \in L$ algebraisch über K, so ist $\alpha \in L'$ auch algebraisch über K, mit demselben Polynom. Außer, dass L das Element α enthalten muss, spielt L keine Rolle. Auf den Grundkörper K kommt es dagegen sehr wohl an:

Beispiel 3.2.3: Die Zahl π ist transzendent über $\mathbb{Q}$. Das ist ein Satz von Lindemann (1882) und nicht leicht zu zeigen. Aber π ist algebraisch über $\mathbb{R}$, denn π ist eine Nullstelle von $x - \pi \in \mathbb{R}[x]$.

Ist α algebraisch, so gibt es unter allen Polynomen mit Nullstelle α ein ausgezeichnetes. Ein Polynom heißt *monisch* (oder *normiert*), wenn sein Leitkoeffizient 1 ist.

Proposition 3.2.4: Sei α algebraisch über K. Dann existiert ein eindeutiges monisches irreduzibles Polynom $m_{\alpha,K} \in K[x]$, das α als Nullstelle hat. Ein beliebiges Polynom $p \in K[x]$ hat genau dann α als Nullstelle, wenn $m_{\alpha,K} \mid p$.

Beweis. Sei $p \in K[x] \setminus \{0\}$ ein Polynom von minimalem Grad, welches α als Nullstelle hat. Indem wir durch den Leitkoeffizienten teilen, können wir ohne Einschränkung annehmen, dass p monisch ist. Da $p(\alpha) = 0$ gilt, ist $\deg(p) \geq 1$.

Angenommen $p = ab$ mit $a, b \in K[x]$. Dann gilt $0 = p(\alpha) = a(\alpha)b(\alpha)$, und da L ein Körper ist, folgt $a(\alpha) = 0$ oder $b(\alpha) = 0$. Also hat a oder b die Nullstelle α. Da $\deg(p)$ minimal war, hat dieser Faktor den Grad $\deg(p)$, und der andere ist eine Konstante $\lambda \in K^*$. Also ist p irreduzibel. Wir setzen $m_{\alpha,K} := p$.

Ist ein Polynom durch $m_{\alpha,K}$ teilbar, so hat es offensichtlich α als Nullstelle. Umgekehrt habe $q \in K[x]$ die Nullstelle α. Division mit Rest durch $m_{\alpha,K}$ liefert

$$q = a \cdot m_{\alpha,K} + r \quad \text{mit } \deg(r) < \deg\big(m_{\alpha,K}\big).$$

Einsetzen von α ergibt $0 = q(\alpha) = a(\alpha) \cdot m_{\alpha,K}(\alpha) + r(\alpha) = r(\alpha)$. Wegen der Minimalität von $\deg\big(m_{\alpha,K}\big)$ folgt $r = 0$, d.h. $m_{\alpha,K} \mid q$.

Zur Eindeutigkeit: Hat $\tilde{p}$ die gleichen Eigenschaften wie $m_{\alpha,K}$, so gilt nach dem eben Gezeigten $\tilde{p} \mid m_{\alpha,K}$ und $m_{\alpha,K} \mid \tilde{p}$. Da beide monisch sind, folgt $\tilde{p} = m_{\alpha,K}$. ∎

Definition 3.2.5: Das Polynom $m_{\alpha,K}$ aus Proposition 3.2.4 heißt *Minimalpolynom* von α über K, und $\deg\big(m_{\alpha,K}\big)$ heißt der *Grad* von α über K.

- Ist α algebraisch über K, so ist nach dem Satz über einfache Erweiterungen (siehe Abschnitt 3.1)

  $$K(\alpha) \cong K[x]/\langle m_{\alpha,K} \rangle,$$

  und $1, \alpha, ..., \alpha^{n-1}$ mit $n = \deg\big(m_{\alpha,K}\big)$ ist eine K-Basis von $K(\alpha)$. Insbesondere ist der Grad von α über K gleich $[K(\alpha) : K]$.
- Das Minimalpolynom von $\sqrt[n]{2} \in \mathbb{R}$ über $\mathbb{Q}$ ist $x^n - 2$, denn dieses Polynom ist monisch, hat $\sqrt[n]{2}$ als Nullstelle und ist nach dem Eisensteinkriterium mit $p = 2$ irreduzibel (siehe Abschnitt 2.6). Über $\mathbb{R}$ ist das Minimalpolynom natürlich $x - \sqrt[n]{2}$.

Proposition 3.2.6: Sei L/K eine Körpererweiterung und $\alpha \in L$.
1. Liegt α in einer Erweiterung von K vom Grad $n < \infty$, so erfüllt α ein Polynom über K vom Grad höchstens n.
2. Erfüllt α ein Polynom $p \neq 0$ über K vom Grad n, so ist $[K(\alpha) : K] \leq n$.

Beweis.

1. Sei $\alpha \in E$ für eine Erweiterung E/K mit $[E : K] = n$. Dann sind die $n + 1$ Elemente $1, \alpha, \alpha^2, ..., \alpha^n$ des n-dimensionalen K-Vektorraums E linear abhängig. Es gibt also $b_0, ..., b_n \in K$, nicht alle gleich 0, mit

   $$0 = b_0 + b_1\alpha + ... + b_n\alpha^n.$$

   Das heißt, α ist eine Nullstelle des Polynoms $b_0 + b_1 x + ... + b_n x^n \neq 0$ vom Grad höchstens n.

2. Der Grad $[K(\alpha) : K]$ ist $\deg\big(m_{\alpha,K}\big)$, und nach Proposition 3.2.4 teilt $m_{\alpha,K}$ das Polynom p. Also ist $\deg\big(m_{\alpha,K}\big) \leq \deg(p) = n$. ∎

Insbesondere ist jedes Element einer endlichen Erweiterung algebraisch, d.h. *endliche Erweiterungen sind algebraisch*.

Beispiel 3.2.7: Wir bestimmen alle *quadratischen Erweiterungen*, also alle Erweiterungen vom Grad 2. Sei K ein Körper der Charakteristik $\neq 2$ und L eine Erweiterung von K mit $[L : K] = 2$. Sei $\alpha \in L \setminus K$. Nach Proposition 3.2.6 erfüllt α ein Polynom vom Grad ≤ 2. Wäre der Grad von α gleich 1, so wäre $\alpha \in K$. Also ist das Minimalpolynom von α quadratisch,

$$m_\alpha(x) = x^2 + bx + c \quad \text{mit } b, c \in K.$$

Wegen $K \subseteq K(\alpha) \subseteq L$ ist $K(\alpha)$ ein 2-dimensionaler Untervektorraum des 2-dimensionalen K-Vektorraums L, also ist $K(\alpha) = L$.

Die quadratische Gleichung $m_\alpha(x) = 0$ kann mit der Lösungsformel gelöst werden:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}. \tag{3}$$

Hier sieht man, wo $\mathrm{char}(K) \neq 2$ gebraucht wird: Wir teilen durch 2. Dabei ist $\sqrt{b^2 - 4c}$ ein formales Symbol für eine Nullstelle des Polynoms $x^2 - (b^2 - 4c)$ in L. Wir behaupten

$$K(\alpha) = K\left(\sqrt{b^2 - 4c}\right).$$

Offensichtlich ist $\alpha \in K\left(\sqrt{b^2 - 4c}\right)$ wegen (3). Andersherum gilt $\pm(2\alpha + b) = \sqrt{b^2 - 4c}$ in L, und damit ist $\sqrt{b^2 - 4c} \in K(\alpha)$.

Die Erweiterung $L = K(\alpha)$ war eine beliebige Erweiterung vom Grad 2. Wir haben also gezeigt: Jede quadratische Erweiterung ist von der Form $K\left(\sqrt{D}\right)$ mit $D \in K$, und D ist kein Quadrat in K (sonst wäre $\sqrt{D} \in K$ und der Grad 1).

Der folgende Satz ist das wichtigste Werkzeug, um Grade von Körpererweiterungen zu berechnen.

Satz 3.2.8 (Gradformel): Seien $F \subseteq K \subseteq L$ Körper. Dann gilt

$$[L : F] = [L : K] \cdot [K : F].$$

Dabei ist die linke Seite genau dann unendlich, wenn einer der Faktoren rechts unendlich ist.

Beweis. Zunächst seien $[L : K] = m$ und $[K : F] = n$ endlich. Sei $\alpha_1, \ldots, \alpha_m$ eine Basis von L über K und $\beta_1, \ldots, \beta_n$ eine Basis von K über F. Wir zeigen, dass die mn Produkte $\alpha_i \beta_j$ eine Basis von L über F bilden.

Jedes Element von L ist eine Linearkombination $a_1\alpha_1 + ... + a_m\alpha_m$ mit $a_i \in K$, wobei nun jedes a_i als

$$a_i = b_{i1}\beta_1 + ... + b_{in}\beta_n \quad \text{mit } b_{ij} \in F$$

ausgedrückt werden kann. Insgesamt schreibt sich jedes Element von L als

$$\sum_{i,j} b_{ij}\alpha_i\beta_j \quad \text{mit } b_{ij} \in F,$$

d.h. die Produkte $\alpha_i\beta_j$ spannen L als F-Vektorraum auf.

Angenommen, es gilt $\sum_{i,j} b_{ij}\alpha_i\beta_j = 0$ mit $b_{ij} \in F$. Mit $a_i := \sum_j b_{ij}\beta_j \in K$ schreibt sich dies als $a_1\alpha_1 + ... + a_m\alpha_m = 0$. Da die α_i eine Basis über K bilden, folgt $a_i = 0$ für alle i. Also ist $\sum_j b_{ij}\beta_j = 0$, und da die β_j eine Basis über F bilden, folgt $b_{ij} = 0$ für alle i, j. Also ist $\{\alpha_i\beta_j : i = 1, ..., m, j = 1, ..., n\}$ eine Basis von L über F, und die Formel gilt im endlichen Fall.

Ist $[K : F] = \infty$, so ist sicher auch $[L : F] = \infty$, denn K ist ein F-Untervektorraum von L. Ist $[L : K] = \infty$, so existieren beliebig große über K linear unabhängige Teilmengen von L. Diese sind erst recht über $F \subseteq K$ linear unabhängig, also ist $[L : F] = \infty$. Sind umgekehrt $[L : K]$ und $[K : F]$ beide endlich, so zeigt der Beweis oben $[L : F] < \infty$. Ist also $[L : F] = \infty$, so ist einer der beiden Faktoren unendlich. ■

Die Gradformel erinnert an den Satz von Lagrange (siehe Satz 1.12.1) und ist ebenso extrem nützlich:

- Ist L/F endlich und K ein Zwischenkörper, d.h. $F \subseteq K \subseteq L$, so teilt $[K : F]$ den Grad $[L : F]$.
- Ist $[L : F]$ eine Primzahl, so gibt es keine echten Zwischenkörper: Jeder Zwischenkörper ist F oder L.

Beispiel 3.2.9: Sei $\alpha \in \mathbb{R}$ eine Nullstelle von $x^3 - 3x - 1$. (Das Polynom hat drei reelle Nullstellen; welche wir nehmen, spielt keine Rolle.) Das Polynom ist irreduzibel über $\mathbb{Q}$, denn es hat Grad 3 und keine rationale Nullstelle: Eine solche müsste ± 1 sein, aber $1 - 3 - 1 = -3$ und $-1 + 3 - 1 = 1$. Also ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Wir behaupten $\sqrt{2} \notin \mathbb{Q}(\alpha)$. Wäre $\sqrt{2} \in \mathbb{Q}(\alpha)$, so hätte man $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}(\alpha)$, und nach der Gradformel würde $2 = \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right]$ den Grad $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ teilen. Widerspruch.

Das zeigt, dass $\sqrt{2}$ keine $\mathbb{Q}$-Linearkombination von $1, \alpha, \alpha^2$ ist. So etwas ist ohne diesen Trick nicht leicht zu zeigen!

© 2026 Thomas Kahle

Beispiel 3.2.10: Sei $\sqrt[6]{2}$ die reelle sechste Wurzel aus 2. Dann ist $\left[\mathbb{Q}\left(\sqrt[6]{2}\right) : \mathbb{Q}\right] = 6$, da $x^6 - 2$ nach Eisenstein irreduzibel ist. In $\mathbb{R}$ gilt $\left(\sqrt[6]{2}\right)^3 = \sqrt{2}$, also ist $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt[6]{2}\right)$. Aus der Gradformel erhalten wir sofort

$$\left[\mathbb{Q}\left(\sqrt[6]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[6]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right],$$

also ist

$$\left[\mathbb{Q}\left(\sqrt[6]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = \frac{6}{2} = 3.$$

Insbesondere hat das Minimalpolynom von $\sqrt[6]{2}$ über $\mathbb{Q}\left(\sqrt{2}\right)$ den Grad 3. Das Polynom $x^3 - \sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)[x]$ ist monisch, hat Grad 3 und die Nullstelle $\sqrt[6]{2}$. Nach Proposition 3.2.4 wird es vom Minimalpolynom geteilt, und da beide Grad 3 haben, ist es das Minimalpolynom. Es folgt: $x^3 - \sqrt{2}$ ist irreduzibel über $\mathbb{Q}\left(\sqrt{2}\right)$. Auch das ist ohne diesen Trick nicht leicht zu zeigen!

Man kann auch mehrere Elemente adjungieren.

Definition 3.2.11: Eine Erweiterung L/K ist *endlich erzeugt*, falls $\alpha_1, ..., \alpha_n \in L$ existieren mit $L = K(\alpha_1, ..., \alpha_n)$.

Lemma 3.2.12: Für eine Erweiterung L/K und $\alpha, \beta \in L$ gilt $K(\alpha, \beta) = K(\alpha)(\beta)$.

Beweis. Der Körper $K(\alpha, \beta)$ enthält K und α, also auch $K(\alpha)$, und außerdem β. Also enthält er $K(\alpha)(\beta)$. Umgekehrt enthält $K(\alpha)(\beta)$ die Elemente von K sowie α und β, also auch $K(\alpha, \beta)$. ∎

Zu jeder endlich erzeugten Erweiterung $L = K(\alpha_1, ..., \alpha_n)$ hat man also mit Lemma 3.2.12 eine Kette

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n = L, \quad \text{wobei } K_i = K_{i-1}(\alpha_i).$$

Sind die α_i algebraisch über K, etwa α_i vom Grad d_i, so sind sie auch algebraisch über jedem K_j, eventuell mit kleinerem Grad: Das Minimalpolynom $m_{\alpha_i, K}$ ist auch ein Polynom über K_{i-1}, also wird es nach Proposition 3.2.4 von $m_{\alpha_i, K_{i-1}}$ geteilt. Damit ist $[K_i : K_{i-1}] \leq d_i$, und nach der Gradformel ist L in diesem Fall endlich:

$$[L : K] = \underbrace{[L : K_{n-1}]}_{\leq d_n} \cdot \underbrace{[K_{n-1} : K_{n-2}]}_{\leq d_{n-1}} \cdots \underbrace{[K_1 : K]}_{= d_1} \leq d_n d_{n-1} \cdots d_1.$$

Aus dem Beweis der Gradformel sieht man auch: Die Produkte der Basen $1, \alpha_i, ..., \alpha_i^{d_i-1}$ der Erweiterungen $K(\alpha_i)/K$ bilden ein Erzeugendensystem von L als K-Vektorraum.

Achtung! Die echten Grade $[K_i : K_{i-1}]$ sind nicht offensichtlich.

Beispiel 3.2.13: Sei $L = \mathbb{Q}\left(\sqrt[6]{2}, \sqrt{2}\right)$. Wir können L auf zwei Arten als Kette schreiben (die Zahlen über den Inklusionen sind die Grade):

$$L \overset{1}{\supseteq} \mathbb{Q}\left(\sqrt[6]{2}\right) \overset{6}{\supseteq} \mathbb{Q} \quad \text{und} \quad L \overset{3}{\supseteq} \mathbb{Q}\left(\sqrt{2}\right) \overset{2}{\supseteq} \mathbb{Q}.$$

Im ersten Fall ist $\sqrt{2} = \left(\sqrt[6]{2}\right)^3 \in \mathbb{Q}\left(\sqrt[6]{2}\right)$, also kommt im zweiten Schritt nichts hinzu, obwohl $\sqrt{2}$ über $\mathbb{Q}$ den Grad 2 hat. Im zweiten Fall hat $\sqrt[6]{2}$ über $\mathbb{Q}\left(\sqrt{2}\right)$ den Grad 3 (Beispiel 3.2.10) und nicht 6.

Beispiel 3.2.14: Sei $L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ mit der Kette $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq L$. Da $\sqrt{2}$ und $\sqrt{3}$ jeweils Grad 2 über $\mathbb{Q}$ haben, ist $[L : \mathbb{Q}] \leq 2 \cdot 2 = 4$ und insbesondere $\left[L : \mathbb{Q}\left(\sqrt{2}\right)\right] \leq 2$.

Ist $x^2 - 3$ irreduzibel über $\mathbb{Q}\left(\sqrt{2}\right)$? Da das Polynom Grad 2 hat, ist das die Frage, ob es eine Nullstelle in $\mathbb{Q}\left(\sqrt{2}\right)$ hat. Angenommen $\sqrt{3} = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$. Quadrieren liefert

$$3 = (a^2 + 2b^2) + 2ab\sqrt{2}.$$

- Falls $ab \neq 0$, ist $\sqrt{2} = (3 - a^2 - 2b^2)/(2ab)$ rational. Widerspruch.
- Falls $b = 0$, ist $\sqrt{3} = a$ rational. Widerspruch.
- Falls $a = 0$, ist $\sqrt{3} = b\sqrt{2}$, also $\sqrt{6} = \sqrt{2}\sqrt{3} = 2b \in \mathbb{Q}$. Widerspruch.

Also ist $x^2 - 3$ irreduzibel über $\mathbb{Q}\left(\sqrt{2}\right)$, und es folgt

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 4$$

mit der Basis $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ (die Produkte der Basen $\left\{1, \sqrt{2}\right\}$ und $\left\{1, \sqrt{3}\right\}$ wie im Beweis der Gradformel).

Satz 3.2.15: Eine Erweiterung L/K ist genau dann endlich, wenn sie von endlich vielen algebraischen Elementen erzeugt wird, d.h. $L = K(\alpha_1, ..., \alpha_n)$ mit $\alpha_1, ..., \alpha_n \in L$ algebraisch über K.

Beweis. Ist $L = K(\alpha_1, ..., \alpha_n)$ mit α_i algebraisch über K vom Grad d_i, so ist $[L : K] \leq \prod_i d_i$, wie wir oben gesehen haben.

© 2026 Thomas Kahle

Sei umgekehrt L/K endlich und $\alpha_1, ..., \alpha_n$ eine K-Basis von L. Dann erzeugen die α_i ganz sicher den Körper L, d.h. $L = K(\alpha_1, ..., \alpha_n)$, denn schon ihre K-Linearkombinationen ergeben ganz L. Außerdem ist jedes α_i nach Proposition 3.2.6 algebraisch, da es in der endlichen Erweiterung L liegt. ■

Korollar 3.2.16: Sind α, β algebraisch über K, so auch $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ und α/β (für $\beta \neq 0$).

Beweis. Alle diese Elemente liegen in $K(\alpha, \beta)$, und diese Erweiterung ist nach Satz 3.2.15 endlich. Nach Proposition 3.2.6 ist jedes Element einer endlichen Erweiterung algebraisch. ■

Korollar 3.2.17: Sei L/K eine beliebige Erweiterung. Die Elemente von L, die über K algebraisch sind, bilden einen Teilkörper von L.

Beweis. Die Menge enthält K, und Korollar 3.2.16 zeigt, dass „algebraisch über K“ unter den Körperoperationen abgeschlossen ist. ■

Beispiel 3.2.18: Wir betrachten die Erweiterung $\mathbb{C}/\mathbb{Q}$. Sei $\overline{\mathbb{Q}}$ der Körper der algebraischen Zahlen über $\mathbb{Q}$, also der Teilkörper der über $\mathbb{Q}$ algebraischen Elemente von $\mathbb{C}$ nach Korollar 3.2.17 (siehe Abschnitt 3.4).

- Die Erweiterung $\overline{\mathbb{Q}}/\mathbb{Q}$ ist algebraisch, aber nicht endlich (also auch nicht endlich erzeugt), denn $\overline{\mathbb{Q}}$ enthält $\sqrt[n]{2}$ für jedes n, also Elemente von beliebig großem Grad n über $\mathbb{Q}$.
- Aber $\overline{\mathbb{Q}}$ ist als Menge abzählbar: $\mathbb{Q}$ ist abzählbar, also ist auch $\mathbb{Q}[x]$ abzählbar (für jeden Grad gibt es abzählbar viele Polynome), und jedes Polynom $\neq 0$ hat nur endlich viele Nullstellen. Damit ist $\overline{\mathbb{Q}}$ eine abzählbare Vereinigung endlicher Mengen, also abzählbar.

Insbesondere ist $\overline{\mathbb{Q}} \cap \mathbb{R}$ „viel kleiner“ als $\mathbb{R}$, denn $\mathbb{R}$ ist überabzählbar. Fast alle reellen Zahlen sind also transzendent über $\mathbb{Q}$. Für konkrete Zahlen ist es aber sehr schwer zu zeigen, dass sie nicht algebraisch sind. Die Zahlen e (Hermite 1873) und π (Lindemann 1882) sind transzendent; das sind tiefe Sätze.

3.3 Konstruktionen mit Zirkel und Lineal

Schon die alten Griechen fragten sich, ob es möglich ist,

1. einen *Würfel zu verdoppeln*, d.h. die Kantenlänge eines Würfels mit doppeltem Volumen zu konstruieren,

2. einen *Winkel zu dritteln*, d.h. einen gegebenen Winkel in drei gleich große Teile zu teilen,
3. einen *Kreis zu quadrieren*, d.h. zu einem gegebenen Kreis ein Quadrat mit gleichem Flächeninhalt zu konstruieren.

Dabei dürfen nur ein Zirkel und ein unmarkiertes Lineal verwendet werden. Wir werden sehen, dass die Körpertheorie alle drei Fragen mit Nein beantwortet.

Gegeben ist eine Länge 1. Längen sind hier einfach reelle Zahlen. Wir starten mit zwei Punkten $(0,0)$ und $(1,0)$ in der Ebene $\mathbb{R}^2$. Die erlaubten Operationen sind:
1. eine Gerade durch zwei gegebene Punkte ziehen,
2. zwei Geraden schneiden,
3. einen Kreis um einen gegebenen Punkt ziehen, dessen Radius der Abstand zweier gegebener Punkte ist,
4. einen Kreis und eine Gerade oder zwei Kreise schneiden.

Die so entstehenden Schnittpunkte dürfen in weiteren Schritten verwendet werden.

Definition 3.3.1: Eine Zahl $a \in \mathbb{R}$ ist *konstruierbar*, wenn die Länge $|a|$ als Abstand zweier Punkte auftaucht, die mit endlich vielen Zirkel-und-Lineal-Konstruktionen aus $(0,0)$ und $(1,0)$ entstehen.

Ein Punkt $(x,y) \in \mathbb{R}^2$ ist genau dann konstruierbar, wenn x und y konstruierbar sind, denn man kann Lote fällen und Längen auf den Achsen abtragen. Die Probleme 1–3 wollen gewisse Zahlen konstruieren: im ersten Problem die Kantenlänge $\sqrt[3]{2}$ des verdoppelten Einheitswürfels, im zweiten den Kosinus des Drittelwinkels und im dritten die Kantenlänge des Quadrats.

Proposition 3.3.2: Sind a und b konstruierbar, so auch $a+b$, $a-b$, ab und (für $b \neq 0$) a/b. Ist $a > 0$ konstruierbar, so auch $\sqrt{a}$. Insbesondere bilden die konstruierbaren Zahlen einen Teilkörper von $\mathbb{R}$, der $\mathbb{Q}$ enthält und unter Quadratwurzeln positiver Elemente abgeschlossen ist.

Beweis. Summe und Differenz sind klar: Man trägt die Längen mit dem Zirkel auf einer Geraden ab. Für das Produkt und den Quotienten verwendet man den Strahlensatz, d.h. man zieht Parallelen (eine Parallele zu einer Geraden durch einen gegebenen Punkt lässt sich mit Zirkel und Lineal konstruieren), siehe Abbildung 7.

Für $\sqrt{a}$ konstruiert man einen Halbkreis mit Durchmesser $1+a$, den man in Stücke der Länge a und 1 teilt. Im Teilungspunkt errichtet man die Senkrechte und erhält die Höhe z wie in Abbildung 8. Nach dem Satz des Thales ist das Dreieck mit den Seiten x, y und $1+a$ rechtwinklig, und mit Pythagoras gilt

$$x^2 = z^2 + a^2, \quad y^2 = z^2 + 1^2, \quad (1+a)^2 = x^2 + y^2.$$

Einsetzen der ersten beiden Gleichungen in die dritte liefert $1 + 2a + a^2 = 2z^2 + a^2 + 1$, also $2a = 2z^2$ und damit $z = \sqrt{a}$.

Da 0 und 1 konstruierbar sind, erhält man aus den Körperoperationen alle rationalen Zahlen. ■

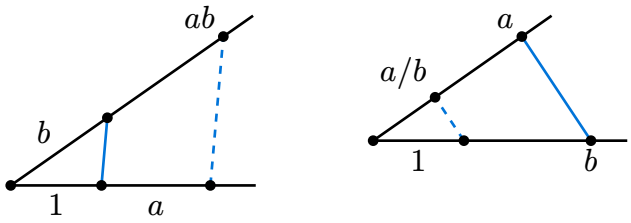


Abbildung 7: Konstruktion von ab (links) und a/b (rechts) mit dem Strahlensatz. Die gestrichelte Gerade ist parallel zur durchgezogenen blauen.

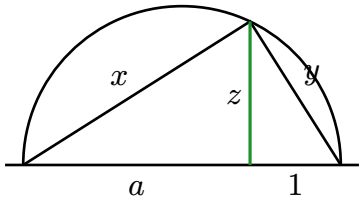


Abbildung 8: Konstruktion von $z = \sqrt{a}$ im Halbkreis über einer Strecke der Länge $1 + a$.

Die konstruierbaren Zahlen bilden also einen Körper, der $\mathbb{Q}$ und alle iterierten Quadratwurzeln enthält. Wir zeigen nun, dass das schon alles ist. Sei dazu $K \subseteq \mathbb{R}$ ein Körper, und seien alle bisher konstruierten Punkte in K^2.

- **Schnitt zweier Geraden.** Eine Gerade durch zwei Punkte aus K^2 hat eine Gleichung $ax + by = c$ mit $a, b, c \in K$. Der Schnittpunkt zweier solcher Geraden

  $$ax + by = c, \quad a'x + b'y = c' \quad \text{mit } a, a', b, b', c, c' \in K$$

  ist die Lösung eines linearen Gleichungssystems über K und liegt daher wieder in K^2.
- **Schnitt von Kreis und Gerade.** Ein Kreis um $(h, k) \in K^2$, dessen Radius r der Abstand zweier Punkte aus K^2 ist, hat die Gleichung $(x-h)^2 + (y-k)^2 = r^2$ mit $r^2 \in K$. Die Schnittpunkte mit einer Geraden erhält man, indem man das System

  $$(x-h)^2 + (y-k)^2 = r^2, \quad ax + by = c$$

  löst: Auflösen der zweiten Gleichung nach y (oder x) und Einsetzen in die erste liefert eine quadratische Gleichung mit Koeffizienten in K für x. Die lineare Gleichung bestimmt daraus y. Nach der Lösungsformel liegen die Schnittpunkte also in $K\left(\sqrt{D}\right)^2$ für ein $D \in K$ mit $D \geq 0$, d.h. in einer Erweiterung vom Grad 1 oder 2. Nach unserer Charakterisierung der quadratischen Erweiterungen (Beispiel 3.2.7) ist das nur Wurzelziehen.
- **Schnitt zweier Kreise.** Schneidet man zwei Kreise

$$(x-h)^2+(y-k)^2=r^2,\quad (x-h')^2+(y-k')^2=r'^2,$$

so kann man die erste Gleichung von der zweiten abziehen und das System äquivalent umformen zu

$$(x-h)^2+(y-k)^2=r^2,\quad 2(h-h')x+2(k-k')y=r'^2-r^2+h^2-h'^2+k^2-k'^2.$$

Bei verschiedenen Mittelpunkten ist die zweite Gleichung eine Gerade (bei gleichen Mittelpunkten schneiden sich die Kreise nicht oder sind gleich). Man hat also wieder den Schnitt eines Kreises mit einer Geraden und erhält eine Erweiterung vom Grad höchstens 2.

Satz 3.3.3: Sei $\alpha \in \mathbb{R}$ konstruierbar. Dann gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^l$ für ein $l \geq 0$.

Beweis. Nach den Überlegungen oben liegen alle Punkte einer Konstruktion in K_m^2 für eine Kette von Körpern

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m \subseteq \mathbb{R} \quad \text{mit } [K_i : K_{i-1}] \in \{1,2\}.$$

Der Abstand $|\alpha|$ zweier solcher Punkte (x,y) und (x',y') ist $\sqrt{(x-x')^2+(y-y')^2}$ und liegt daher in einer Erweiterung K_{m+1} von K_m vom Grad 1 oder 2. Nach der Gradformel ist $[K_{m+1} : \mathbb{Q}] = 2^s$ für ein $s \geq 0$. Wegen $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K_{m+1}$ teilt $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ nach der Gradformel die Zahl 2^s, ist also selbst eine Zweierpotenz. ∎

Die Umkehrung von Satz 3.3.3 gilt nicht ohne Weiteres; das genaue Kriterium liefert die Galoistheorie. Für die griechischen Probleme reicht aber die eine Richtung.

Satz 3.3.4: Die drei griechischen Probleme sind mit Zirkel und Lineal nicht lösbar.

Beweis.

1. Zur Verdopplung eines Würfels mit Volumen 1, d.h. Kantenlänge 1, muss die Kantenlänge $\sqrt[3]{2}$ konstruiert werden. Wir wissen aber $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$, denn $x^3 - 2$ ist nach Eisenstein irreduzibel. Das ist keine Zweierpotenz.
2. Zur Dreiteilung eines Winkels θ: Der Kosinus führt Winkel in Längen über, d.h. ein Winkel θ ist genau dann konstruierbar, wenn $\cos\theta$ konstruierbar ist (man trägt auf einem Schenkel die Länge 1 ab und fällt das Lot auf den anderen Schenkel). Die Aufgabe ist also, $\cos(\theta/3)$ aus $\cos\theta$ zu konstruieren. Das ist für manche θ möglich, z.B. ist $\cos(180°/3) = 1/2$, d.h. $180°$ kann man dreiteilen. Sei nun aber $\theta = 60°$, d.h. $\cos\theta = 1/2$; dieser Winkel ist konstruierbar (gleichseitiges Dreieck). Nach dem Tschebyschow-Polynom $T_3 = 4x^3 - 3x$ gilt

$$\cos\theta = 4\cos^3\left(\frac{\theta}{3}\right) - 3\cos\left(\frac{\theta}{3}\right).$$

© 2026 Thomas Kahle

Mit $\beta = \cos 20°$ ist also

$$\frac{1}{2} = 4\beta^3 - 3\beta \quad \Longleftrightarrow \quad (2\beta)^3 - 3(2\beta) - 1 = 0.$$

Die Zahl $\alpha = 2\beta$ ist also eine Nullstelle des irreduziblen Polynoms $x^3 - 3x - 1$ aus Beispiel 3.2.9, und es ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Also ist α und damit auch $\beta = \alpha/2$ nicht konstruierbar.

3. Der Flächeninhalt eines Einheitskreises ist π. Also ist ein Quadrat mit Kantenlänge $\sqrt{\pi}$ zu konstruieren. Aber π ist transzendent über $\mathbb{Q}$, und damit auch $\sqrt{\pi}$ (wäre $\sqrt{\pi}$ algebraisch, so nach Korollar 3.2.16 auch $\pi = \sqrt{\pi}^2$). Konstruierbare Zahlen sind nach Satz 3.3.3 algebraisch. ■

Die Unlösbarkeit der ersten beiden Probleme bewies Wantzel 1837, die des dritten folgt aus Lindemanns Satz von 1882.

Reguläre n-Ecke

Für manche Winkel θ, die ganzzahlig in Grad sind, ist $\cos\theta$ konstruierbar, z.B. für $\theta = 72°$, den Mittelpunktswinkel im regulären Fünfeck, welches konstruierbar ist. Welche regulären n-Ecke sind konstruierbar? Die Antwort (Gauß 1796 für die eine Richtung, Wantzel 1837 für die andere) lautet: Das reguläre n-Eck ist genau dann konstruierbar, wenn

$$n = 2^k p_1 \cdots p_l$$

mit $k \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_l$.

Fermatsche Primzahlen sind Primzahlen der Form $2^{2^m} + 1$.

- Es sind nur fünf bekannt: $3, 5, 17, 257, 65537$. Man vermutet, dass dies alle sind.
- Die Zahl $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ ist nicht prim (Euler).

Also ist das reguläre 65537-Eck konstruierbar! Johann Gustav Hermes hat die Konstruktion nach etwa zehnjähriger Arbeit 1894 abgeschlossen. Das Manuskript füllt einen Koffer, der in Göttingen aufbewahrt wird.

Lässt man zu, dass das Lineal mit konstruierten Längen markiert wird, so gibt es die sogenannte *Neusis* („Einschiebung“), mit der man unter anderem Gleichungen dritten Grades lösen kann. Damit lassen sich zum Beispiel Winkel dreiteilen.

3.4 Zerfällungskörper und algebraischer Abschluss

Bisher haben wir einem Körper K immer eine Wurzel eines irreduziblen Polynoms hinzugefügt, indem wir $K[x]/\langle p\rangle$ gebildet haben (siehe Abschnitt 3.1). Nun wollen wir *alle* Wurzeln eines Polynoms auf einmal hinzufügen.

Definition 3.4.1: Sei K ein Körper und $f \in K[x]$. Eine Erweiterung L/K heißt *Zerfällungskörper* von f, falls f über L in Linearfaktoren zerfällt, aber über keinem echten Teilkörper $M \subsetneq L$ mit $K \subseteq M$ in Linearfaktoren zerfällt.

Ein Zerfällungskörper ist also eine kleinste Erweiterung von K, über der f zerfällt. Er wird von den Wurzeln von f erzeugt:

Lemma 3.4.2: Sei L/K eine Körpererweiterung und $f \in K[x]$ ein Polynom, das über L in Linearfaktoren zerfällt, $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ mit $c \in K$ und $\alpha_1, ..., \alpha_n \in L$. Dann ist $K(\alpha_1, ..., \alpha_n)$ ein Zerfällungskörper von f über K. Umgekehrt ist jeder Zerfällungskörper L von f von der Form $L = K(\alpha_1, ..., \alpha_n)$.

Beweis. Sei M ein Körper mit $K \subseteq M \subseteq L$, über dem f in Linearfaktoren zerfällt, $f = c(x-\beta_1)\cdots(x-\beta_n)$ mit $\beta_i \in M$. Das ist auch eine Zerlegung in $L[x]$, und da die Zerlegung in Linearfaktoren in $L[x]$ eindeutig ist (der Polynomring über einem Körper ist faktoriell), stimmen die β_i bis auf die Reihenfolge mit den α_i überein. Also enthält M alle α_i und damit $K(\alpha_1, ..., \alpha_n)$.

Über $K(\alpha_1, ..., \alpha_n)$ zerfällt f offensichtlich. Nach dem eben Gezeigten zerfällt f über keinem echten Teilkörper davon, der K enthält. Ist umgekehrt L ein Zerfällungskörper, so ist $K(\alpha_1, ..., \alpha_n) \subseteq L$ ein Teilkörper, über dem f zerfällt, und wegen der Minimalität von L gilt Gleichheit. ∎

Satz 3.4.3: Sei K ein Körper und $f \in K[x]$ nicht konstant. Dann existiert ein Zerfällungskörper L/K von f.

Beweis. Nach Lemma 3.4.2 genügt es, eine Erweiterung E/K zu finden, über der f in Linearfaktoren zerfällt. Dann ist $K(\alpha_1, ..., \alpha_n) \subseteq E$ mit den Wurzeln α_i von f in E ein Zerfällungskörper. Wir zeigen die Existenz von E per Induktion nach $n = \deg f$, und zwar gleichzeitig für alle Körper K.

Für $n = 1$ ist f linear und $E = K$ tut es. Sei nun $n > 1$. Wir betrachten die Zerlegung von f in irreduzible Faktoren. Sind alle Faktoren linear, so ist wieder $E = K$. Andernfalls sei g ein irreduzibler Faktor mit $\deg g \geq 2$. Dann ist $K' := K[x]/\langle g \rangle$ ein Erweiterungskörper von K, in dem g und damit auch f eine Wurzel θ hat (siehe Abschnitt 3.1). In $K'[x]$ gilt also $f = (x-\theta)f_1$ mit $\deg f_1 = n-1$. Nach Induktionsvoraussetzung (angewendet auf den Körper K') existiert ein Erweiterungskörper E von K', über dem f_1 in Linearfaktoren zerfällt. Dann zerfällt auch $f = (x-\theta)f_1$ über E, und E ist eine Erweiterung von K. ∎

© 2026 Thomas Kahle

Beispiel 3.4.4: Sei $f = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$. Die Wurzeln von f in $\mathbb{C}$ sind $\pm\sqrt{2}$ und $\pm\sqrt{3}$, ein Zerfällungskörper ist also $L = \mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$. Wir haben schon gesehen, dass $[L:\mathbb{Q}] = 4$ ist (siehe Abschnitt 3.2). Die Teilkörper von L, die $\mathbb{Q}$ enthalten, sind $\mathbb{Q}$, $\mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(\sqrt{3}\big)$, $\mathbb{Q}\big(\sqrt{6}\big)$ und L selbst. Sie sind links in Abbildung 9 dargestellt, die Kanten sind mit den Graden der Erweiterungen beschriftet.

Andererseits kann man die Automorphismen von L betrachten, die $\mathbb{Q}$ (und damit jedes Element von $\mathbb{Q}$) festlassen. Ein solcher Automorphismus muss $\sqrt{2}$ wieder auf eine Wurzel von x^2-2 abbilden, also auf $\pm\sqrt{2}$, und ebenso $\sqrt{3}$ auf $\pm\sqrt{3}$. Man kann zeigen, dass alle vier Möglichkeiten tatsächlich Automorphismen liefern. Schreiben wir $\sigma_{a,b}$ für den Automorphismus mit

$$\sigma_{a,b}\big(\sqrt{2}\big) = (-1)^a\sqrt{2}, \quad \sigma_{a,b}\big(\sqrt{3}\big) = (-1)^b\sqrt{3}, \quad a,b \in \{0,1\},$$

so ist $\sigma_{a,b} \circ \sigma_{c,d} = \sigma_{a+c,b+d}$ (Exponenten modulo 2), d.h. die Automorphismengruppe ist isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$. Ihr Untergruppenverband ist rechts in Abbildung 9 dargestellt, allerdings auf den Kopf gestellt: Die kleinste Untergruppe steht oben.

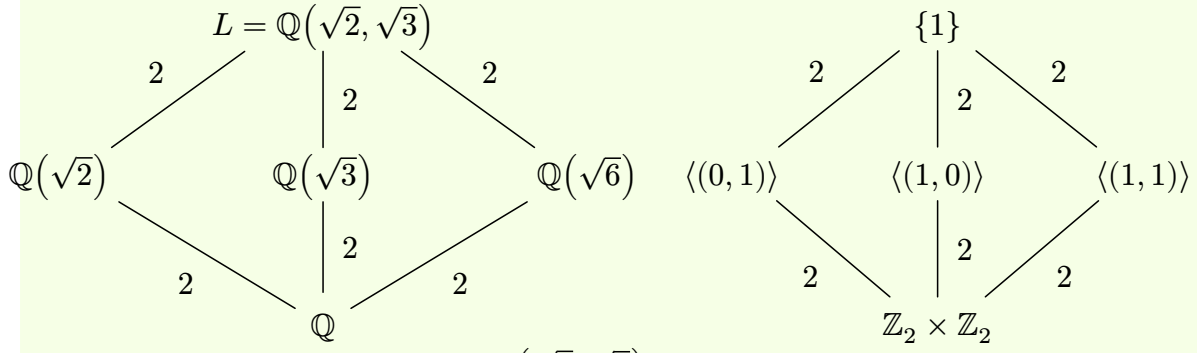


Abbildung 9: Teilkörper von $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$ und Untergruppen von $\mathbb{Z}_2 \times \mathbb{Z}_2$ (mit (a,b) für $\sigma_{a,b}$). Die Kanten rechts sind mit den Indizes beschriftet.

Man beobachtet: Das Untergruppendiagramm von $\mathbb{Z}_2 \times \mathbb{Z}_2$ entspricht dem Diagramm der Teilkörper von $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$, wenn man es auf den Kopf stellt. Genauer entsprechen sich Positionen in den beiden Diagrammen so: Einer Untergruppe H entspricht der Körper der Elemente, die von allen Automorphismen in H festgelassen werden. Zum Beispiel lässt $\sigma_{0,1}$ genau die Elemente von $\mathbb{Q}\big(\sqrt{2}\big)$ fest, und $\sigma_{1,1}$ lässt $\sqrt{6} = \sqrt{2}\sqrt{3}$ fest. Die Abbildung in die andere Richtung ordnet einem Teilkörper die Gruppe der Automorphismen von L zu, die ihn punktweise festlassen. Dahinter steckt die *Galoistheorie*, auf die wir in Abschnitt 3.6 einen Ausblick geben.

thomas.kahle@ovgu.de

Beispiel 3.4.5: Wir bestimmen einen Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$. Die Wurzeln in $\mathbb{C}$ sind

$$\theta_1 = \sqrt[3]{2}, \quad \theta_2 = \sqrt[3]{2} \cdot \frac{-1+\sqrt{-3}}{2}, \quad \theta_3 = \sqrt[3]{2} \cdot \frac{-1-\sqrt{-3}}{2}.$$

Mit $\zeta_3 := \big(-1+\sqrt{-3}\big)/2$ ist $\theta_2 = \sqrt[3]{2}\zeta_3$ und $\theta_3 = \sqrt[3]{2}\zeta_3^2$, denn $\zeta_3^2 = \big(-1-\sqrt{-3}\big)/2$. Ein Zerfällungskörper ist

$$L = \mathbb{Q}(\theta_1, \theta_2, \theta_3) = \mathbb{Q}\big(\sqrt[3]{2}, \sqrt{-3}\big).$$

Die Inklusion „$\subseteq$“ ist klar. Umgekehrt enthält $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$ das Element $\sqrt[3]{2} = \theta_1$ und $\sqrt{-3} = 2\theta_2/\theta_1 + 1$. Der Grad ist $[L : \mathbb{Q}] = 6$: Er ist nach der Gradformel durch $\big[\mathbb{Q}\big(\sqrt[3]{2}\big) : \mathbb{Q}\big] = 3$ und durch $\big[\mathbb{Q}\big(\sqrt{-3}\big) : \mathbb{Q}\big] = 2$ teilbar, also durch 6, und andererseits ist $[L : \mathbb{Q}] = \big[L : \mathbb{Q}\big(\sqrt[3]{2}\big)\big] \cdot 3 \leq 2 \cdot 3$, da $\sqrt{-3}$ Wurzel von $x^2 + 3$ ist (siehe Abschnitt 3.2).

Die Automorphismen von L permutieren die drei Wurzeln $\theta_1, \theta_2, \theta_3$, und man kann zeigen, dass jede der sechs Permutationen von genau einem Automorphismus kommt. Die Automorphismengruppe ist also S_3 (wobei wir die Wurzeln mit $1, 2, 3$ nummerieren). In Abbildung 10 sind die Teilkörper von L und die Untergruppen von S_3 dargestellt, wieder an entsprechenden Positionen. Die Transposition (23) vertauscht θ_2 und θ_3 und lässt θ_1 fest, ihr entspricht $\mathbb{Q}(\theta_1)$. Der 3-Zykel (123) bildet $\sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$ und $\sqrt[3]{2}\zeta_3 \mapsto \sqrt[3]{2}\zeta_3^2$ ab, also $\zeta_3 \mapsto \zeta_3$, und lässt damit $\mathbb{Q}(\zeta_3) = \mathbb{Q}\big(\sqrt{-3}\big)$ fest.

© 2026 Thomas Kahle

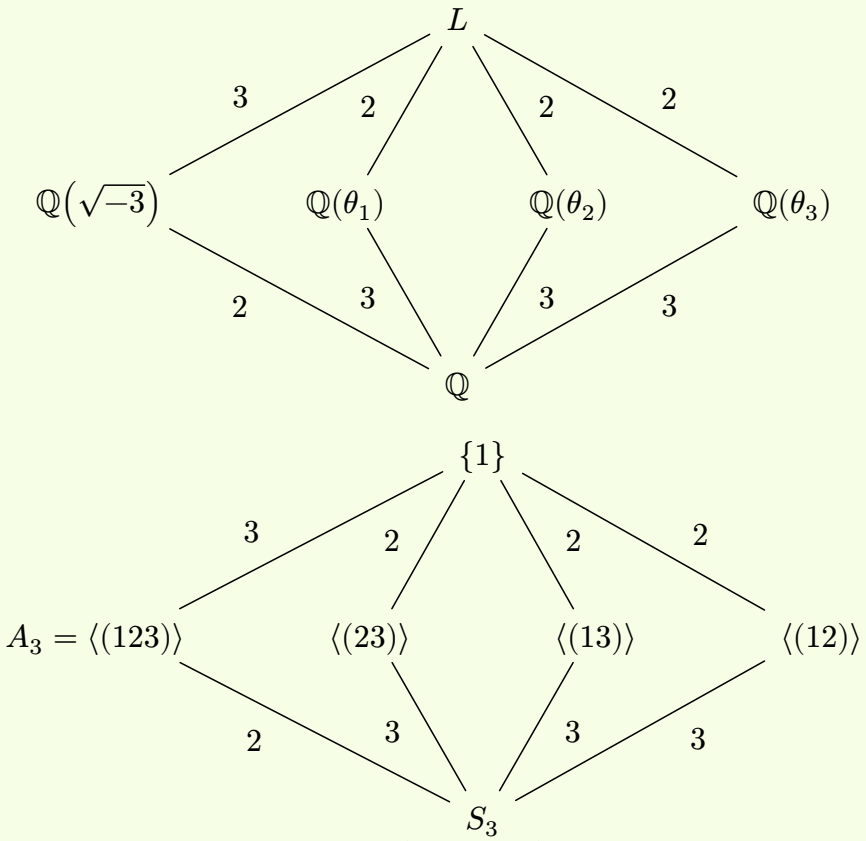


Abbildung 10: Teilkörper von $L = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right)$ (oben) und Untergruppen von S_3 (unten) an entsprechenden Positionen. Dabei ist $\theta_2 = \sqrt[3]{2}\zeta_3$ und $\theta_3 = \sqrt[3]{2}\zeta_3^2$.

Hier wird die Theorie komplizierter, da nicht alle Untergruppen von S_3 Normalteiler sind.

Wie groß kann ein Zerfällungskörper werden? Im letzten Beispiel hatte ein Polynom vom Grad 3 einen Zerfällungskörper vom Grad $6 = 3!$. Mehr geht nicht:

Proposition 3.4.6: Sei $f \in K[x]$ vom Grad $n \geq 1$ und L ein Zerfällungskörper von f über K. Dann ist $[L : K] \leq n!$.

Beweis. Induktion nach n. Für $n = 1$ ist $L = K$. Sei $n > 1$ und $f = c(x - \alpha_1)\cdots(x - \alpha_n)$ in $L[x]$. Das Minimalpolynom von α_1 über K teilt f, also ist $[K(\alpha_1) : K] \leq n$. Über $K_1 := K(\alpha_1)$ gilt $f = (x - \alpha_1)f_1$ mit $f_1 = c(x - \alpha_2)\cdots(x - \alpha_n) \in K_1[x]$, und nach Lemma 3.4.2 ist $L = K_1(\alpha_2, ..., \alpha_n)$ ein Zerfällungskörper von f_1 über K_1. Nach Induktionsvoraussetzung ist $[L : K_1] \leq (n-1)!$, und mit der Gradformel folgt $[L : K] = [L : K_1][K_1 : K] \leq (n-1)! \cdot n = n!$. ∎

Der Zerfällungskörper von $x^n - 1$

Die Wurzeln von $x^n - 1$ heißen *n-te Einheitswurzeln*. Über $\mathbb{C}$ sind das die Zahlen

$$e^{2\pi ik/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right), \quad k = 0, \ldots, n-1.$$

Sie liegen auf dem Einheitskreis und bilden die Ecken eines regulären n-Ecks (siehe Abbildung 11).

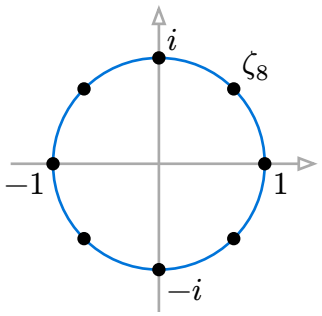


Abbildung 11: Die achten Einheitswurzeln in $\mathbb{C}$.

Die n-ten Einheitswurzeln bilden eine Untergruppe der Gruppe $\mathbb{C}^*$, und diese ist zyklisch, erzeugt von $e^{2\pi i/n}$. Die Erzeuger dieser Gruppe heißen *primitive n-te Einheitswurzeln*. Nach unseren Ergebnissen über zyklische Gruppen sind das genau die $e^{2\pi ik/n}$ mit $\mathrm{ggT}(k, n) = 1$ (siehe Abschnitt 1.8). Adjungiert man eine primitive n-te Einheitswurzel ζ_n zu $\mathbb{Q}$, so erhält man alle n-ten Einheitswurzeln als ihre Potenzen. Damit ist $\mathbb{Q}(\zeta_n)$ ein Zerfällungskörper von $x^n - 1$ über $\mathbb{Q}$.

Definition 3.4.7: Sei ζ_n eine primitive n-te Einheitswurzel. Der Körper $\mathbb{Q}(\zeta_n)$ heißt *n-ter Kreisteilungskörper*. Das Minimalpolynom von ζ_n über $\mathbb{Q}$ heißt *n-tes Kreisteilungspolynom*.

Man kann zeigen, dass das n-te Kreisteilungspolynom den Grad

$$\varphi(n) = |\{k \in \{1, \ldots, n\} : \mathrm{ggT}(k, n) = 1\}|$$

hat. Die Funktion φ heißt *Eulersche φ-Funktion*. Es gilt also $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Beispiel 3.4.8: Für eine Primzahl p haben wir mit dem Eisensteinkriterium gezeigt, dass

$$\frac{x^p - 1}{x - 1} = 1 + x + \ldots + x^{p-1}$$

irreduzibel ist (siehe Abschnitt 2.6). Da ζ_p eine Wurzel dieses Polynoms ist, ist es das p-te Kreisteilungspolynom, und es gilt $\left[\mathbb{Q}(\zeta_p) : \mathbb{Q}\right] = p - 1 = \varphi(p)$.

Eindeutigkeit des Zerfällungskörpers

Ein Zerfällungskörper ist bis auf Isomorphie eindeutig. Wir zeigen sogar eine etwas allgemeinere Aussage, die für den Induktionsbeweis nötig ist. Für einen Isomorphis-

mus $\varphi: K \to K'$ und $f \in K[x]$ bezeichnet $\varphi(f) \in K'[x]$ das Polynom, das man durch Anwenden von φ auf die Koeffizienten erhält.

Satz 3.4.9: Sei $\varphi: K \to K'$ ein Isomorphismus von Körpern, $f \in K[x]$ nicht konstant, L ein Zerfällungskörper von f über K und L' ein Zerfällungskörper von $\varphi(f)$ über K'. Dann gibt es einen Isomorphismus $\sigma: L \to L'$ mit $\sigma|_K = \varphi$. Insbesondere sind je zwei Zerfällungskörper von f über K isomorph.

Beweis. Induktion nach $[L : K]$, was nach Proposition 3.4.6 endlich ist. Ist $[L : K] = 1$, so zerfällt $f = c(x - a_1)\cdots(x - a_n)$ schon über K. Dann zerfällt auch $\varphi(f) = \varphi(c)(x - \varphi(a_1))\cdots(x - \varphi(a_n))$ über K', und nach Lemma 3.4.2 ist $L' = K'$. Wir können $\sigma = \varphi$ nehmen.

Sei nun $[L : K] > 1$. Dann zerfällt f nicht über K, hat also einen irreduziblen Faktor g mit $\deg g \geq 2$. Sei $\alpha \in L$ eine Wurzel von g. Da $\varphi: K[x] \to K'[x]$ ein Ringisomorphismus ist, ist $\varphi(g)$ ein irreduzibler Faktor von $\varphi(f)$ und hat eine Wurzel $\beta \in L'$. Nach dem Satz über die Fortsetzung von Isomorphismen auf einfache Erweiterungen gibt es einen Isomorphismus $\sigma_1: K(\alpha) \to K'(\beta)$ mit $\sigma_1(\alpha) = \beta$ und $\sigma_1|_K = \varphi$ (siehe Abschnitt 3.1). Nach Lemma 3.4.2 ist L ein Zerfällungskörper von f über $K(\alpha)$ und L' ein Zerfällungskörper von $\sigma_1(f) = \varphi(f)$ über $K'(\beta)$. Da g bis auf einen Faktor aus K das Minimalpolynom von α ist, gilt $[L : K(\alpha)] = [L : K]/\deg g < [L : K]$. Nach Induktionsvoraussetzung setzt sich σ_1 zu einem Isomorphismus $\sigma: L \to L'$ fort, und dieser setzt φ fort.

Für die zweite Aussage wendet man das auf $K = K'$ und $\varphi = \mathrm{id}_K$ an. ∎

Wegen Satz 3.4.9 spricht man oft von *dem* Zerfällungskörper von f.

Der algebraische Abschluss

Nun wollen wir zu Körpern übergehen, die *alle* Wurzeln *aller* Polynome enthalten.

Definition 3.4.10:
- Ein Körper $\overline{K}$ heißt *algebraischer Abschluss* eines Körpers K, falls $\overline{K}$ algebraisch über K ist und jedes $f \in K[x]$ über $\overline{K}$ in Linearfaktoren zerfällt.
- Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes nicht konstante Polynom $f \in K[x]$ über K in Linearfaktoren zerfällt, d.h. falls jedes nicht konstante Polynom in $K[x]$ eine Wurzel in K hat.

Es ist zunächst nicht klar, ob diese Dinge existieren. Ist K algebraisch abgeschlossen, so ist offensichtlich $\overline{K} = K$ ein algebraischer Abschluss. Der Name ist gerechtfertigt, denn der Abschluss ist wirklich abgeschlossen:

Proposition 3.4.11: Sei $\overline{K}$ ein algebraischer Abschluss von K. Dann ist $\overline{K}$ algebraisch abgeschlossen, d.h. $\overline{\overline{K}} = \overline{K}$.

Beweis. Sei $f \in \overline{K}[x]$ nicht konstant und α eine Wurzel von f in einer Erweiterung von $\overline{K}$ (zum Beispiel in einem Zerfällungskörper). Wir zeigen, dass α algebraisch über K ist. Seien $c_0, ..., c_m \in \overline{K}$ die Koeffizienten von f. Da die c_i algebraisch über K sind, ist $K' := K(c_0, ..., c_m)$ eine endliche Erweiterung von K (siehe Abschnitt 3.2). Da $f \in K'[x]$ ist, ist α algebraisch über K', also ist auch $K'(\alpha)/K'$ endlich. Nach der Gradformel ist $K'(\alpha)/K$ endlich, also ist α algebraisch über K.

Das Minimalpolynom $m \in K[x]$ von α zerfällt nach Definition des algebraischen Abschlusses über $\overline{K}$ in Linearfaktoren. Da α eine Wurzel von m ist, folgt $\alpha \in \overline{K}$. Also hat f eine Wurzel in $\overline{K}$. ■

Die Konstruktion eines Zerfällungskörpers ist endlich: Man bildet nur endlich oft Quotienten der Form $K[x]/\langle g \rangle$. Zur Konstruktion eines algebraischen Abschlusses eines beliebigen Körpers müssen im Allgemeinen unendlich viele Wurzeln adjungiert werden. Diese Idee kann mit dem Zornschen Lemma präzise gemacht werden (siehe Abschnitt 2.4). Wir geben den folgenden Satz ohne Beweis an.

Satz 3.4.12:
- Jeder Körper ist in einem algebraisch abgeschlossenen Körper enthalten.
- Jeder Körper K besitzt einen algebraischen Abschluss $\overline{K}$, und dieser ist bis auf Isomorphie eindeutig.

Ist $K \subseteq F$ mit F algebraisch abgeschlossen, so ist die Menge der über K algebraischen Elemente von F ein algebraischer Abschluss von K.

Beispiel 3.4.13:
- $\mathbb{C}$ ist algebraisch abgeschlossen. Das ist der *Fundamentalsatz der Algebra*, der sich am elegantesten mit Methoden der Analysis beweisen lässt.
- Der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ besteht also genau aus den algebraischen Zahlen in $\mathbb{C}$. Der Körper $\overline{\mathbb{Q}}$ ist abzählbar (siehe Abschnitt 3.2).

Ein paar Bemerkungen zum algebraischen Abschluss:
- $\overline{K}$ und K haben die gleiche Charakteristik, da K ein Teilkörper von $\overline{K}$ ist.
- $\overline{K}$ ist stets unendlich, auch wenn K endlich ist. Wäre nämlich $\overline{K} = \{a_1, ..., a_n\}$ endlich, so hätte das Polynom $(x - a_1) \cdots (x - a_n) + 1$ keine Wurzel in $\overline{K}$, im Widerspruch zu Proposition 3.4.11.

© 2026 Thomas Kahle

3.5 Endliche Körper und Separabilität

Zunächst ein Phänomen: Mehrfache Wurzeln von irreduziblen Polynomen können Probleme machen. Zu jedem Polynom f denken wir an seinen Zerfällungskörper. Dort zerfällt f in Linearfaktoren und kann mehrfache Wurzeln haben, d.h. Linearfaktoren mit Exponenten größer als 1 wie bei $f = (x-a)^2$.

Definition 3.5.1: Ein Polynom $f \in K[x]$ heißt *separabel*, falls alle Wurzeln von f in seinem Zerfällungskörper verschieden sind, und *inseparabel* sonst.

Für ein irreduzibles Polynom würde man erwarten, dass es nur einfache Wurzeln hat. Das ist falsch:

Beispiel 3.5.2: Sei $K = \mathbb{F}_2(t)$ der Körper der rationalen Funktionen mit Koeffizienten in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, d.h. der Körper der Quotienten p/q mit $p, q \in \mathbb{F}_2[t]$ und $q \neq 0$. Wir betrachten

$$f = x^2 - t \in K[x].$$

- f ist irreduzibel, da f vom Grad 2 ist und keine Wurzel in K hat: Aus $(p/q)^2 = t$ folgt $p^2 = tq^2$, aber links steht ein Polynom geraden Grades und rechts eines ungeraden Grades.
- Im Zerfällungskörper gibt es eine Wurzel $\sqrt{t}$ von f, und es gilt

$$\left(x - \sqrt{t}\right)^2 = x^2 - 2x\sqrt{t} + \left(\sqrt{t}\right)^2 = x^2 - t = f,$$

  da $2 = 0$ in Charakteristik 2 ist.

Also ist f irreduzibel, aber nicht separabel. Die einzige Wurzel $\sqrt{t}$ ist eine doppelte Wurzel.

Die Rechnung im Beispiel ist ein Spezialfall der „binomischen Formel für Anfänger“: In einem kommutativen Ring der Charakteristik p (mit p prim) gilt

$$(a+b)^p = a^p + b^p,$$

denn der Binomialkoeffizient $\binom{p}{k}$ ist für $0 < k < p$ durch p teilbar. Über $\mathbb{F}_2$ selbst funktioniert das Beispiel nicht, denn dort ist jedes Element ein Quadrat ($0 = 0^2$, $1 = 1^2$), sodass $x^2 - a$ für $a \in \mathbb{F}_2$ nie irreduzibel ist.

Um Separabilität zu testen, braucht man den Zerfällungskörper nicht. Die *formale Ableitung* eines Polynoms $f = \sum_{k=0}^{n} a_k x^k \in K[x]$ ist

$$D_x f := \sum_{k=1}^{n} k a_k x^{k-1},$$

thomas.kahle@ovgu.de

d.h. $D_x x^k := kx^{k-1}$, linear fortgesetzt. Sie erfüllt die Produktregel $D_x(fg) = (D_x f)g + f(D_x g)$, wie man durch Nachrechnen auf Monomen prüft.

Proposition 3.5.3: Sei K ein Körper und $f \in K[x]$ nicht konstant.
1. f ist genau dann separabel, wenn $\mathrm{ggT}(f, D_x f) = 1$ ist (f ist teilerfremd zu seiner Ableitung).
2. Ist $\mathrm{char}(K) = 0$, so ist jedes irreduzible Polynom in $K[x]$ separabel.
3. Ist K endlich, so ist jedes irreduzible Polynom in $K[x]$ separabel.

Beweis.

1. Sei L der Zerfällungskörper von f. Der ggT von f und $D_x f$ ist in $K[x]$ und in $L[x]$ derselbe, denn der euklidische Algorithmus liefert in beiden Fällen dasselbe Ergebnis. Hat f eine mehrfache Wurzel $a \in L$, also $f = (x-a)^2 g$, so ist $D_x f = 2(x-a)g + (x-a)^2 D_x g$ und $x - a$ ist ein gemeinsamer Teiler. Hat f nur einfache Wurzeln und ist a eine davon, so ist $f = (x-a)g$ mit $g(a) \neq 0$ und $(D_x f)(a) = g(a) + 0 = g(a) \neq 0$. Also haben f und $D_x f$ keine gemeinsame Wurzel in L. Da jeder nicht konstante gemeinsame Teiler von f und $D_x f$ in $L[x]$ eine Wurzel von f in L hätte, ist $\mathrm{ggT}(f, D_x f) = 1$.

2. Sei f irreduzibel vom Grad $n \geq 1$ mit Leitkoeffizient a_n. Der ggT von f und $D_x f$ ist ein Teiler von f, also bis auf Einheiten 1 oder f. In Charakteristik 0 ist der Leitkoeffizient na_n von $D_x f$ nicht null, also ist $D_x f \neq 0$ ein Polynom vom Grad $n - 1 < \deg f$, das nicht durch f teilbar ist. Also ist $\mathrm{ggT}(f, D_x f) = 1$.

3. Sei $\mathrm{char}(K) = p$. Wie in 2. ist $\mathrm{ggT}(f, D_x f) = 1$, außer wenn $f \mid D_x f$, was wegen $\deg D_x f < \deg f$ nur für $D_x f = 0$ möglich ist. Dann ist $k a_k = 0$ für alle k, d.h. $a_k = 0$ außer für durch p teilbare k, und $f = \sum_j a_{pj} x^{pj}$. Die Abbildung $K \to K$, $a \mapsto a^p$ ist nach der binomischen Formel für Anfänger ein Ringhomomorphismus, als Körperhomomorphismus injektiv und, da K endlich ist, auch surjektiv. Also gibt es $b_j \in K$ mit $b_j^p = a_{pj}$, und es folgt

$$f = \sum_j b_j^p (x^j)^p = \left(\sum_j b_j x^j \right)^p .$$

   Das widerspricht der Irreduzibilität von f. ∎

Endliche Körper

Wir kennen die endlichen Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p. Die Idee ist nun, endliche Erweiterungen davon zu betrachten. Ist $F/\mathbb{F}_p$ eine Erweiterung vom Grad n, so ist F als $\mathbb{F}_p$-Vektorraum isomorph zu $\mathbb{F}_p^n$ und hat daher $q = p^n$ Elemente. Wir werden sehen, dass dies die einzigen möglichen Ordnungen endlicher Körper sind.

Sei $n > 0$ beliebig. Wir betrachten den Zerfällungskörper L von

$$f = x^{p^n} - x$$

über $\mathbb{F}_p$. Es ist

$$D_x f = p^n x^{p^n-1} - 1 = -1,$$

also ist $\mathrm{ggT}(f, D_x f) = 1$ und f ist nach Proposition 3.5.3 separabel. Daher hat f genau p^n verschiedene Wurzeln in L. Die Idee ist, dass diese Wurzeln bereits einen Körper bilden. Seien α, β zwei Wurzeln, also $\alpha^{p^n} = \alpha$ und $\beta^{p^n} = \beta$. Dann gilt

$$(\alpha\beta)^{p^n} = \alpha\beta, \quad (\alpha^{-1})^{p^n} = \alpha^{-1} \text{ (für } \alpha \neq 0), \quad (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

wobei wir die binomische Formel für Anfänger n-mal angewendet haben. Ebenso ist $(-\alpha)^{p^n} = -\alpha$ (für $p = 2$ ist $-\alpha = \alpha$), und 0 und 1 sind Wurzeln. Die Wurzeln von f bilden also einen Teilkörper von L mit p^n Elementen. Da der Zerfällungskörper von den Wurzeln erzeugt wird (Lemma 3.4.2), ist L genau die Menge der Wurzeln von f. Insbesondere ist $|L| = p^n$, und durch Abzählen folgt $[L : \mathbb{F}_p] = n$. Es gibt also endliche Körper von jedem Erweiterungsgrad n über jedem $\mathbb{F}_p$, nämlich mit p^n Elementen.

Nun zur Eindeutigkeit. Sei F ein beliebiger endlicher Körper. Dann ist $\mathrm{char}(F) = p$ für eine Primzahl p (siehe Abschnitt 3.1), und F enthält $\mathbb{F}_p$ als Primkörper. Da F endlich ist, ist $[F : \mathbb{F}_p] = n < \infty$, also ist $|F| = p^n$ eine Primzahlpotenz. Die multiplikative Gruppe F^* hat $p^n - 1$ Elemente. Nach dem Satz von Lagrange ist daher $\alpha^{p^n-1} = 1$ für jedes $\alpha \neq 0$ in F, denn die Ordnung jedes Elements teilt die Gruppenordnung (siehe Abschnitt 1.12). Jedes $\alpha \neq 0$ ist also eine Wurzel von $x^{p^n-1} - 1$, und damit ist jedes $\alpha \in F$ eine Wurzel von $x^{p^n} - x$. Also zerfällt $x^{p^n} - x$ über F in Linearfaktoren, und F besteht genau aus den p^n Wurzeln. Nach Lemma 3.4.2 ist F ein Zerfällungskörper von $x^{p^n} - x$ über $\mathbb{F}_p$, und nach Satz 3.4.9 ist er bis auf Isomorphie eindeutig. Wir haben gezeigt:

Satz 3.5.4: Sei F ein endlicher Körper der Charakteristik p. Dann hat F die Ordnung $q = p^n$ für ein $n \geq 1$ und ist isomorph zum Zerfällungskörper von $x^{p^n} - x$ über seinem Primkörper $\mathbb{F}_p$. Umgekehrt gibt es zu jeder Primzahlpotenz $q = p^n$ einen Körper mit q Elementen.

Der bis auf Isomorphie eindeutige Körper der Ordnung $q = p^n$ wird mit $\mathbb{F}_q$ bezeichnet. Endliche Körper haben viele Anwendungen, vor allem in der Kryptographie und der Kodierungstheorie.

Achtung! Für $n \geq 2$ ist $\mathbb{F}_{p^n}$ *nicht* der Ring $\mathbb{Z}/p^n\mathbb{Z}$. Letzterer ist kein Körper, da $\overline{p}$ ein Nullteiler ist.

3.6 Ausblick: Galoistheorie

Zum Abschluss geben wir einen Ausblick auf die Galoistheorie, in der Gruppen-, Ring- und Körpertheorie zusammenkommen. Die Grundidee haben wir in Beispiel 3.4.4 und Beispiel 3.4.5 schon gesehen.

Definition 3.6.1: Sei L/K eine Körpererweiterung. Die Gruppe

$$\mathrm{Aut}(L/K) := \{\sigma\colon L \to L \text{ Automorphismus mit } \sigma(\alpha) = \alpha \text{ für alle } \alpha \in K\}$$

heißt die *Automorphismengruppe* der Erweiterung.

Dass $\mathrm{Aut}(L/K)$ mit der Komposition eine Gruppe ist, prüft man leicht nach. Ein paar Bemerkungen dazu:

- Jeder Automorphismus $\sigma\colon L \to L$ fixiert den Primkörper, denn aus $\sigma(1) = 1$ folgt $\sigma(n \cdot 1) = n \cdot 1$ für alle $n \in \mathbb{Z}$ und damit auch $\sigma((n \cdot 1)(m \cdot 1)^{-1}) = (n \cdot 1)(m \cdot 1)^{-1}$.
- $\mathrm{Aut}(L/K)$ ist eine Untergruppe der Gruppe $\mathrm{Aut}(L)$ aller Automorphismen von L. Zum Beispiel ist $\mathrm{Aut}(\mathbb{C})$ eine „wilde“ Gruppe: Wenn man das Auswahlaxiom voraussetzt, gibt es außer der Identität und der komplexen Konjugation noch sehr viele weitere, nicht stetige Automorphismen.

Lemma 3.6.2: Sei $\sigma \in \mathrm{Aut}(L/K)$, $f \in K[x]$ und $\alpha \in L$ eine Wurzel von f. Dann ist auch $\sigma(\alpha)$ eine Wurzel von f.

Beweis. Sei $f = \sum_k a_k x^k$ mit $a_k \in K$. Da σ ein Ringhomomorphismus ist, der die a_k festlässt, gilt

$$f(\sigma(\alpha)) = \sum_k a_k \sigma(\alpha)^k = \sigma\left(\sum_k a_k \alpha^k\right) = \sigma(f(\alpha)) = \sigma(0) = 0. \qquad \blacksquare$$

Die Automorphismen in $\mathrm{Aut}(L/K)$ permutieren also die Wurzeln jedes Polynoms aus $K[x]$, die in L liegen. Das ist der Zusammenhang zu den Lösungsformeln aus der Einleitung (Abschnitt 1.1).

Definition 3.6.3: Sei $H \leq \mathrm{Aut}(L/K)$ eine Untergruppe. Der *Fixkörper* von H ist

$$\mathrm{Fix}(H) := \{\alpha \in L\colon \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\}.$$

Man prüft leicht nach:

- $\mathrm{Fix}(H)$ ist ein Teilkörper von L mit $K \subseteq \mathrm{Fix}(H) \subseteq L$.
- Aus $K \subseteq K_1 \subseteq K_2 \subseteq L$ folgt $\mathrm{Aut}(L/K_2) \leq \mathrm{Aut}(L/K_1)$.
- Aus $H_1 \leq H_2 \leq \mathrm{Aut}(L/K)$ folgt $\mathrm{Fix}(H_2) \subseteq \mathrm{Fix}(H_1)$.

© 2026 Thomas Kahle

Beide Zuordnungen kehren also Inklusionen um. Das **Dogma der Galoistheorie** lautet: Für Zerfällungskörper besteht ein starker Zusammenhang zwischen dem Untergruppenverband von $\mathrm{Aut}(L/K)$ und dem Teilkörperverband von L/K. Man beweist zunächst:

Satz 3.6.4: Sei L/K ein Zerfällungskörper von $f \in K[x]$. Dann gilt

$$|\mathrm{Aut}(L/K)| \leq [L : K],$$

mit Gleichheit genau dann, wenn jeder irreduzible Faktor von f separabel ist.

Beweis (Idee). Man zählt Isomorphismen per Induktion wie im Beweis von Satz 3.4.9. Ist $\varphi\colon K \to K'$ ein Isomorphismus, α eine Wurzel eines irreduziblen Faktors g von f und L' ein Zerfällungskörper von $\varphi(f)$, so lässt sich φ zu einem Isomorphismus $K(\alpha) \to K'(\beta)$ fortsetzen, für jede Wurzel β von $\varphi(g)$ in L', und auf keine andere Weise:

$$\begin{array}{ccc} L & \xrightarrow{\sim} & L' \\ | & & | \\ K(\alpha) & \xrightarrow{\sim} & K'(\beta) \\ | & & | \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Es gibt höchstens $\deg g = [K(\alpha) : K]$ solche β, und genau $\deg g$ viele, wenn $\varphi(g)$ keine mehrfachen Wurzeln hat. Per Induktion erhält man höchstens $[L : K]$ Fortsetzungen von φ zu Isomorphismen $L \to L'$, mit Gleichheit im separablen Fall. Für $K = K'$, $L = L'$ und $\varphi = \mathrm{id}_K$ sind die Fortsetzungen genau die Elemente von $\mathrm{Aut}(L/K)$. ∎

Definition 3.6.5: Ist L/K eine endliche Erweiterung mit $|\mathrm{Aut}(L/K)| = [L : K]$, so heißt L/K *Galoiserweiterung* und $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$ die *Galoisgruppe* der Erweiterung.

Man kann zeigen, dass eine endliche Erweiterung L/K genau dann galoissch ist, wenn L der Zerfällungskörper eines separablen Polynoms über K ist. Da in Charakteristik 0 alle irreduziblen Polynome separabel sind, ist insbesondere über $\mathbb{Q}$ jeder Zerfällungskörper eine Galoiserweiterung.

Satz 3.6.6 (Hauptsatz der Galoistheorie): Sei L/K eine Galoiserweiterung und $G = \mathrm{Gal}(L/K)$. Es gibt eine Bijektion

$$\{E\colon K \subseteq E \subseteq L \text{ Zwischenkörper}\} \quad \longleftrightarrow \quad \{H\colon H \leq G \text{ Untergruppe}\},$$

gegeben durch

$$E \mapsto \mathrm{Aut}(L/E) = \{\sigma \in G\colon \sigma(\alpha) = \alpha \text{ für alle } \alpha \in E\} \quad \text{und} \quad H \mapsto \mathrm{Fix}(H).$$

Diese beiden Abbildungen sind zueinander invers. Weiter gilt:

1. Die Abbildungen sind inklusionsumkehrend.
2. Entsprechen sich E und H, so ist $[L : E] = |H|$ und $[E : K] = |G\colon H|$, der Index von H in G.
3. L/E ist galoissch mit $\mathrm{Gal}(L/E) = H$. Die Erweiterung E/K ist genau dann galoissch, wenn $H \trianglelefteq G$ ein Normalteiler ist. In diesem Fall ist $\mathrm{Gal}(E/K) \cong G/H$.
4. Die Verbandsstrukturen sind verträglich: Entsprechen sich E_1, H_1 und E_2, H_2, so entspricht der Schnitt $E_1 \cap E_2$ der von H_1 und H_2 erzeugten Untergruppe, und der kleinste Teilkörper, der E_1 und E_2 enthält, entspricht $H_1 \cap H_2$.

Dieser Satz ermöglicht viele Einsichten. Zum Beispiel folgt sofort, dass eine Galoiserweiterung nur endlich viele Zwischenkörper hat, denn die endliche Gruppe G hat nur endlich viele Untergruppen.

Ist H kein Normalteiler, so permutiert die Konjugation in G die Untergruppe H und andere Untergruppen, und entsprechend permutieren die Automorphismen die zugehörigen Zwischenkörper. Zum Beispiel ist $\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ der Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$ (Beispiel 3.4.5), und es gibt Automorphismen davon, die die Teilkörper $\mathbb{Q}\left(\sqrt[3]{2}\zeta_3^i\right)$, $i = 0, 1, 2$, vertauschen. Ihnen entsprechen die drei zueinander konjugierten Untergruppen der Ordnung 2 in S_3, die keine Normalteiler sind. Die Erweiterungen $\mathbb{Q}\left(\sqrt[3]{2}\zeta_3^i\right)/\mathbb{Q}$ sind nicht galoissch: Zum Beispiel liegen die beiden anderen Wurzeln von $x^3 - 2$ nicht in $\mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq \mathbb{R}$. Dagegen ist $A_3 \trianglelefteq S_3$ ein Normalteiler, und $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ ist galoissch mit Galoisgruppe $S_3/A_3 \cong \mathbb{Z}_2$. Abbildung 10 ist also genau die Situation des Hauptsatzes.

Außerdem kann man zeigen:

- Jede endliche separable Erweiterung L/K hat ein primitives Element, d.h. $L = K(\alpha)$ für ein $\alpha \in L$ (*Satz vom primitiven Element*). Insbesondere ist jede endliche Erweiterung von $\mathbb{Q}$ von der Form $\mathbb{Q}(\alpha)$.
- $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist galoissch mit zyklischer Galoisgruppe der Ordnung n, erzeugt von $a \mapsto a^p$. Die Teilkörper von $\mathbb{F}_{p^n}$ sind daher genau die $\mathbb{F}_{p^d}$ mit $d \mid n$.
- **Satz von Abel**: Für Polynome vom Grad 5 oder höher gibt es keine Lösungsformeln, die nur Körperoperationen und Wurzelziehen benutzen. Mit Galoistheorie sieht man das so: Ein Polynom ist genau dann durch Wurzelziehen lösbar, wenn seine Galoisgruppe eine bestimmte Eigenschaft (*auflösbar*) hat, und die Gruppe S_5, die als Galoisgruppe eines Polynoms vom Grad 5 auftritt, hat diese Eigenschaft nicht.

© 2026 Thomas Kahle

Wer mehr über Galoistheorie lernen möchte, dem sei das Buch *Galois Theory* von Joseph Rotman empfohlen.

Stichwortverzeichnis

A

Abelsche Gruppe 7
Additive Gruppe 10
Adjunktion 100
Algebraisch abgeschlossen 119
Algebraische Erweiterung 103
Algebraische Zahl 103
Algebraischer Abschluss 119
Algebraisches Element 103
Assoziativität 7
Assoziiert 85
Automorphismengruppe einer Erweiterung 124
Automorphismus 28

C

Charakteristik 94

D

Diamantensatz 62
Diedergruppe 11
Direktes Produkt 8
Disjunkte Zykel 17
Divisionsring 67

E

Einfache Gruppe 65
Einfache Körpererweiterung 100
Einheit 69
Einheitengruppe 69
Einheitswurzel 117
Einheitswurzel, primitive 118
Eins 67
Einsetzhomomorphismus 78
Eisensteinkriterium 92
Elliptische Kurve 5
Endlich erzeugte Erweiterung 107
Endlich erzeugtes Ideal 79
Endliche Körpererweiterung 97
Endlicher Körper 123
Erweiterungskörper 96
Erzeuger 14, 35
Erzeugte Untergruppe 39
Erzeugtes Ideal 79
Euklidischer Ring 88
Eulersche ϕ-Funktion 54, 118

F

Faktorabbildung 52
Faktorgruppe 50
Faktorieller Ring 87
Faser 43
Fermat, großer Satz von 5
Fermat, kleiner Satz von 54
Fermatsche Primzahl 113
Fixkörper 124
Formale Ableitung 121
Fundamentalsatz der Algebra 120

G

Galoiserweiterung 125
Galoisgruppe 125
Grad einer Körpererweiterung 97
Grad eines algebraischen Elements 104
Grad eines Polynoms 72
Gradformel 105
Gruppe 7
Gruppenring 73
Gruppenwirkung 25

H

Hasse-Diagramm 41
Hauptideal 79
Hauptidealring 80
Homomorphismus 21
Hölderprogramm 66

I

Ideal 77
Index 53
Inhalt eines Polynoms 91
Integritätsbereich 70
Inverses 7
Irreduzibel 85
Isomorph 21
Isomorphieklasse 22
Isomorphiesatz, dritter 63
Isomorphiesatz, erster 59
Isomorphiesatz, vierter 64
Isomorphiesatz, zweiter 62
Isomorphismus 21
Isomorphismus von Ringen 74

© 2026 Thomas Kahle

K

Kanonische Projektion 48
Kern 29
Kern einer Wirkung 34
Kern eines Ringhomomorphismus 74
Klassifikation der endlichen einfachen Gruppen 65
Kleinsche Vierergruppe 15
Kommutativer Ring 67
Kompositionsreihe 66
Konjugation 28, 49
Konjugiert 49
Konjugierte Untergruppe 49
Konstruierbare Zahl 110
Korrespondenzsatz 64
Kreisteilungskörper 118
Kreisteilungspolynom 93, 118
Körper 67
Körpererweiterung 96

L

Leitkoeffizient 72
Lemma von Bézout 8
Linksideal 77
Linksnebenklasse 46

M

Maximales Ideal 82
Minimalpolynom 104
Monisches Polynom 103
Monoid 74

N

Natürliche Projektion 77
Nebenklasse 46
Neusis 113
Neutrales Element 7
Norm 86
Normalisator 32
Normalisieren 49
Normalteiler 49
Nullring 67
Nullteiler 69

O

Ordnung einer Gruppe 15
Ordnung eines Elements 11

P

P-Gruppe 57
Permutation 17
Permutationsdarstellung 26
Polynom 72
Polynomring 72
Potenz 10
Potenz eines Ideals 80
Primelement 86
Primideal 84
Primitives Element 100
Primitives Polynom 91
Primkörper 95
Produkt von Idealen 80
Präsentation 14

Q

Quadratische Erweiterung 70, 105
Quadratur des Kreises 110
Quaternionen 68
Quotientengruppe 45, 50
Quotientenring 77

R

Rechtsideal 77
Rechtsnebenklasse 46
Reduzibel 85
Reguläre Wirkung 27
Restklassen 8
Restklassenring 69
Ring 67
Ringhomomorphismus 74

S

Satz vom primitiven Element 126
Satz von Abel 126
Satz von Cauchy 56
Satz von Cayley 28
Satz von Jordan–Hölder 66
Satz von Lagrange 52
Separabel 121
Stabilisator 34
Summe von Idealen 80
Sylow, Sätze von 57
Sylowgruppe 57

Symmetrische Gruppe 17

T

Teiler 85
Teilkörper 95
Teilring 71
Transposition 18
Transzendentes Element 103
Treue Wirkung 26
Triviale Untergruppe 29
Triviale Wirkung 26
Trivialer Teiler 85

U

Untergruppe 29
Untergruppenkriterium 30
Untergruppenverband 41

V

Verband 41
Vollständiges Urbild 52, 64

W

Winkeldreiteilung 110
Wirkung 25
Würfelverdopplung 109

Z

Zentralisator 31
Zentrum 32
Zerfällungskörper 114
Zornsches Lemma 82
Zweizeilige Notation 18
Zykel 17
Zyklische Gruppe 35

© 2026 Thomas Kahle