Inkrementelles Skript **Version 28. Juni 2018**

Grundlagen der Algebra

Goethe–Universität Frankfurt — Sommersemester 2017

für Bachelor und L3

JAKOB STIX

Zusammenfassung. — Die Vorlesung behandelt grundlegended die Theorie zu den algebraischen Grundbegriffen Gruppe, Ring und Körper.

Das Skript wird fortlaufend aktualisiert und es werden weiterhin Fehler korrigiert. Sie lesen daher das Skript **auf eigene Gefahr!** Bitte teilen Sie mir Korrekturvorschläge per Email mit.

Inhaltsverzeichnis

Danksagung. Ich möchte mich gerne bei allen bedanken, insbesondere bei Frau Salzmann für diverse Zeichnungen, und bei den Studierenden Adrian Baumann, Sebastian Groß, Julia Huth, Simone Jablonski, Theresa Kumpitsch, Denise Melchin, Carolin Müller, Phuong Bao Pham, Timofej Velesko und Julia Weber, die dazu beigetragen haben, das Skript von kleineren und größeren Eseleien zu befreien, auch wenn dies ein Kampf gegen die Windmühlen und die Rechtschreibreform ist. So mag ich beispielsweise beim besten Willen manches Mal nicht auf das "ß" verzichten.

Einführung

Wir motivieren zunächst aus der Arithmetik der Zahlen verschiedene algebraische Strukturen. Ich gehe davon aus, daß aus der Linearen Algebra 1 die Grundbegriffe Gruppe, Ring und Körper bereits mit Definition und ersten Beispielen bekannt sind.

Ein Panorama algebraischer Strukturen. Entsprechend des zeitlichen Ablaufs des Erwerbs arithmetischer Fähigkeiten bei Kindern beobachten wir eine Hierarchie algebraischer Strukturen, mit der wir eine Menge ausstatten können.

Halbgruppe. Zunächst lernen wir die **natürlichen Zahlen**

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

zum Zählen und Abzählen kennen. Diese versehen wir mit der Addition und erhalten, was wir eine **Halbgruppe** nennen.

Genaugenommen ziehen wir uns hier wie Münchhausen am eigenen Schopf aus dem Sumpf. Was die natürlichen Zahlen genau sind, erfordert zum Beispiel die Peano-Axiome, deren Modell die natürlichen Zahlen sind. Die Peano-Axiome sind bereits so kompliziert, daß Kurt Gödel[1] mit seinem Unvollständigkeitssatz zeigen konnte, daß die Widerspruchsfreiheit der darauf basierenden Arithmetik nicht innerhalb dieser Arithmetik gezeigt werden kann.

Beispielsweise beruht das Prinzip der vollständigen Induktion auf einem Axiom der Peano-Axiome[2], ist also ein mathematisches Schlußfolgerungsprinzip, das nicht bewiesen werden kann, sondern das in die Grundlagen der Arithmetik der natürlichen Zahlen hineindefiniert wird.

Monoid. Dann erfindet man die **Null** 0, mit der Eigenschaft, daß für alle $n \in \mathbb{N}$ gilt

$$0 + n = n = n + 0.$$

Die neue Menge

$$\mathbb{N}_0 = \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

mit Addition und dem ausgezeichneten Element $0 \in \mathbb{N}_0$ bildet die Struktur eines **Monoids**.

Gruppe. In dem Bestreben, die Addition in jedem Fall umkehren zu können, erweitert man $\mathbb{N}_0$ zu den **ganzen Zahlen**

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

Die ganzen Zahlen mit der Addition bilden eine **Gruppe**. Das ausgezeichnete Element 0 ist nun durch die verlangten Eigenschaften eindeutig bestimmt.

Ring. Jetzt kommt eine echte Innovation. Mit der Multiplikation betritt eine zweite Verknüpfung die Bühne. Dieselbe Menge $\mathbb{Z}$, jetzt aber mit Addition und Multiplikation, die sich wie gewohnt nach dem Distributivgesetz vertragen, bildet einen **Ring**. Von einem Ring verlangen wir sofort, daß er eine **Eins** 1 hat mit der Eigenschaft, daß für alle Zahlen n gilt

$$1 \cdot n = n = n \cdot 1.$$

Weitere Beispiele von Ringen sind gegeben durch Funktionen auf Mengen mit punktweiser Addition und Multiplikation. Der moderne Standpunkt identifiziert alle (kommutativen) Ringe als Ringe von strukturerhaltenden Funktionen auf strukturierten Mengen. Beispielsweise gibt es in der Funktionalanalysis das Theorem von Gelfand über C*-Algebren, das jede solche C*-Algebra A mit dem Ring der stetigen Funktionen auf dem Spektrum von A identifiziert.

---

[1] Kurt Gödel, 1906–1978, österreichischer Mathematiker.

[2] Das Prinzip der vollständigen Induktion: Eine Menge M natürlicher Zahlen, welche die 1 und mit jeder Zahl n deren Nachfolger $n + 1$ enthält, besteht aus allen natürlichen Zahlen, also $M = \mathbb{N}$.

In der algebraischen Geometrie definiert man ganz abstrakt das Spektrum $\operatorname{Spec}(R)$ eines Rings R. Dies liefert einen Raumbegriff, so daß genau R der Ring der Funktionen auf dem Spektrum wird. Für $\mathbb{Z}$ ist dies die Menge der Primzahlen und 0

$$\operatorname{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), \ldots, (p), \ldots\},$$

wobei die Klammern die entsprechenden Primideale bezeichnen.

Wie ist nun eine natürliche Zahl eine Funktion auf Primzahlen aufzufassen? Der Wert von $n \in \mathbb{Z}$ bei der Primzahl p ist definiert als $n \pmod p$. Beispiel: 32 hat den Wert 4 bei 7. Und was ist der Wert von n bei (0)? Das ist nichts anderes als n aufgefaßt als rationale Zahl!

Körper. Genauso, wie man die Addition mittels Subtraktion umkehren möchte, soll nun auch die Multiplikation umkehrbar sein. Dieser Schritt ist schon komplizierter und gelingt nur partiell. Man kann nur durch eine Zahl a dividieren, welche die Kürzungsregel befolgt:

$$ax = ay \quad \Longrightarrow \quad x = y.$$

Für $a = 0$ schlägt dies fehl. Wenn man für $\mathbb{Z}$ die Multiplikation mit allen Zahlen $a \in \mathbb{Z} \setminus \{0\}$ umkehrbar macht, gelangt man zu den Brüchen, also dem Körper $\mathbb{Q}$ der **rationalen Zahlen**. Als Besonderheit der Konstruktion von Brüchen können mehrere Symbole die gleiche Zahl beschreiben: etwa $22/7 = 66/21$. Außerdem muß man argumentieren, daß der Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ die bereits eingeführte Ringstruktur nicht zerstört. Ein Körper soll einfach nur ein Ring sein, bei dem für alle von 0 verschiedenen Zahlen die Multiplikation mit diesen umkehrbar ist.

Vollständiger Körper. Jetzt kommt ein nicht-algebraischer Schritt, der Übergang von $\mathbb{Q}$ nach den **reellen Zahlen** $\mathbb{R}$ durch Vervollständigung bezüglich Cauchy–Folgen bezüglich des reellen Absolutbetrags

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

wie in der Analysis üblich. Dies ist aber nicht der einzige sinnvolle Abstandsbegriff auf der Menge der rationalen Zahlen. Zu jeder Primzahl p gibt es einen solchen, für den man $\mathbb{Q}$ zu den p-adischen Zahlen vervollständigen kann.

Algebraisch abgeschlossener Körper. Über den reellen Zahlen zeigt der Zwischenwertsatz der Analysis, daß jedes Polynom ungeraden Grades eine reelle Nullstelle haben muß. Sei etwa das Polynom

$$f(X) = X^n + a_1 X^{n-1} + \ldots + a_n$$

mit $n \in \mathbb{N}$ ungerade und $a_i \in \mathbb{R}$ für alle $1 \leq i \leq n$ gegeben. Dann dominiert X^n in $f(x)$ für große $|x| \gg 0$, womit $f(x)$ mal positive und mal negative Werte annimmt. Der Zwischenwertsatz besagt, daß dann $f(x)$ auch alle Werte dazwischen annimmt, so zum Beispiel die 0.

Quadratische Gleichungen wie etwa

$$X^2 + 1 = 0$$

haben keine reelle Lösung. Hier stellt der Absolutbetrag auf $\mathbb{R}$ Bedingungen, die der Gleichung zuwiderlaufen: der Ausdruck $X^2 + 1$ ist stets positiv.

Eine Lösung erhält man wieder dadurch, daß man den Rechenbereich von $\mathbb{R}$ nach den **komplexen Zahlen** $\mathbb{C}$ durch Hinzufügen einer neuen Zahl i erweitert. Dabei erfüllt die neue Zahl i definitionsgemäß die zu lösende Gleichung und fügt sich ansonsten dahingehend ein, daß die erweiterte Struktur eine Körpererweiterung von $\mathbb{R}$ wird, und zwar minimal mit der Eigenschaft, auch i zu enthalten.

Jetzt geschieht ein Wunder. Durch Hinzunahme einer einzigen Zahl i und dem Abschließen unter Körperoperationen (dazu reichen $\mathbb{R}$-Linearkombinationen von 1 und i) wird aus $\mathbb{R}$ ein Körper $\mathbb{C} = \mathbb{R} \oplus \mathbb{R} \cdot i$, der immer noch vollständig bezüglich Cauchy–Folgen zum natürlich erweiterten Abstandsbegriff

$$|(a + bi) - (c + di)|^2 = |a - c|^2 + |b - d|^2$$

ist und in dem jede Polynomgleichung (sogar mit Koeffizienten aus $\mathbb{C}$) lösbar ist (Fundamentalsatz der Algebra). Man sagt, $\mathbb{C}$ ist vollständig und algebraisch abgeschlossen.

Nicht-kommutative Strukturen. Die in den vorherigen Abschnitten skizzierten algebraischen Strukturen sind sämtlich kommutativ: es kommt auf die Reihenfolge der Addition oder Multiplikation nicht an. Dies ist für einige Anwendungen zu einfach. Schon in der Linearen Algebra 1 trifft man nicht-kommutative Beispiele:

Symmetrische Gruppe. Zu $n \in \mathbb{N}$ gibt es die **symmetrische Gruppe** S_n aller Permutationen der Menge $\{1, 2, \ldots, n\}$, welche für $n \geq 3$ nicht-kommutativ ist.

Allgemeine lineare Gruppe. Zu einem Vektorraum V über einem Körper K gibt es die Gruppe der invertierbaren linearen Selbstabbildungen $V \to V$, auch **allgemeine lineare Gruppe von** V genannt und mit $\mathrm{GL}(V)$ bezeichnet. Ist $\dim(V) = n$, so kann man nach Wahl einer Basis $\mathscr{B}$ und der damit einhergehenden Koordinatenwahl

$$\kappa_{\mathscr{B}} : V \xrightarrow{\sim} K^n$$

jede invertierbare lineare Selbstabbildung $f \in \mathrm{GL}(V)$ durch eine $n \times n$-Matrix $M^{\mathscr{B}}_{\mathscr{B}}(f) \in \mathrm{M}_n(K)$ mit Einträgen aus K beschreiben. Die Zuordnung

$$M^{\mathscr{B}}_{\mathscr{B}} : \mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(K)$$

ist bijektiv zu Matrizen mit invertierbarer (von 0 verschiedener) Determinante und übersetzt die Komposition linearer Abbildungen in Matrizenmultiplikation.

Die Symmetrie des Quadrats. Wir betrachten in der Ebene $\mathbb{R}^2$ das durch die Ecken $\binom{\pm 1}{\pm 1}$ definierte Quadrat $\square$. Welche linearen Selbstabbildungen des $\mathbb{R}^2$ führen $\square$ in sich über? Sicherlich die Drehung um $\pi/2$, die Matrixmultiplikation mit

$$D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

und die Spiegelung an der x-Achse, die Matrixmultiplikation mit

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

Damit führen auch beliebig iterierte Kompositionen (also Matrixmultiplikationen) von D und S das Quadrat $\square$ in sich über. Alle diese bilden eine Gruppe von Matrizen in $\mathrm{GL}_2(\mathbb{R})$, die Diedergruppe D_4 aus 8 Elementen (das muß man sich und werden wir uns überlegen). In dieser Beschreibung kommt die Gruppe natürlich mit einer Interpretation als lineare Transformationen eines Vektorraumes daher. Das nennt man eine lineare Darstellung der Gruppe.

Die D_4 ist nicht kommutativ, wie man schon an

$$DS = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = SD$$

sieht. (Man überlege sich zur Übung, welche Transformationen des Quadrats durch DS und durch SD gegeben sind.)

Matrizenring. Sei $n \in \mathbb{N}$ und K ein Körper. Die Menge aller quadratischen Matrizen $\mathrm{M}_n(K) = \mathrm{M}_{n\times n}(K)$ mit Einträgen aus einem Körper K ist eine abelsche Gruppe bezüglich der Addition. Es ist $\mathrm{M}_n(K)$ sogar ein K-Vektorraum, aber das soll uns hier einmal nicht interessieren. Die Matrizenmultiplikation definiert eine weitere Verknüpfung, die bezüglich der Addition distributiv ist und aus $\mathrm{M}_n(K)$ einen Ring macht. Für $n \geq 2$ ist die Multiplikation dieses Rings nicht kommutativ.

Operationen. Die Beispiele im vorherigen Abschnitt haben die folgende Gemeinsamkeit. Die algebraische Struktur tritt nicht solitär abstrakt auf, sondern als Gruppe/Ring strukturerhaltender Selbstabbildungen eines einfacheren Objekts:

- S_n permutiert die *Menge* $\{1, 2, \ldots, n\}$,
- $\mathrm{GL}(V)$ permutiert den Vektorraum V, und zwar K-linear,
- $\mathrm{M}_n(K)$ umfaßt alle K-linearen Selbstabbildungen des K-Vektorraums K^n.

Diese Beziehung wird in beide Richtungen ausgenutzt. Durch die Operation auf einem einfacheren Objekt versteht man sowohl die Gruppe oder den Ring als auch das einfachere Objekt besser.

Die folgenden Lehrbücher werden für die Vorlesung empfohlen.

Literatur

[Ar93] Michael Artin, *Algebra*, Übersetzung des englischen Originals von 1991 durch Annette A'Campo, Birkhäuser Advanced Texts: Basler Lehrbücher, Birkhäuser Verlag, Basel, 1993, xiv+705 Seiten.

[Bo08] Siegfried Bosch, *Lineare Algebra*, Springer-Lehrbuch, 4. überarbeitete Auflage, 2008, x+297 Seiten.

[MK13] Kurt Meyberg und Christian Karpfinger, *Algebra: Gruppen âĂŞ Ringe âĂŞ KÃűrper*, Springer Spektrum, 2013, xi+386 Seiten.

Teil 1. Gruppen und Gruppenoperationen

1. Gruppen und Homomorphismen

1.1. **Definition und erste Beispiele.** Wir beginnnen mit der grundlegenden Definition.

Definition 1.1. Eine **Gruppe** ist ein Paar $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung

$$\circ : \ G \times G \to G,$$

geschrieben als $(g, h) \mapsto g \circ h$, mit den folgenden Eigenschaften.

(i) Die Verknüpfung ist **assoziativ**: für alle $g, h, k \in G$ gilt:

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

Die Klammerung legt die Reihenfolge fest, in der die Verknüpfungen auszuführen sind.

(ii) Es gibt ein Element $e \in G$, **neutrales Element** genannt, so daß für alle $g \in G$

$$g \circ e = g = e \circ g.$$

(iii) Zu jedem $g \in G$ gibt es ein $h \in G$, **inverses Element** oder das **Inverse** genannt, so daß

$$g \circ h = e = h \circ g.$$

Notation 1.2. Wir vereinfachen sofort die Notation und unsere Vorstellung, was eine Gruppe ist.

(1) Bei einer Gruppe $(G, \circ)$ denkt man zuerst an die zugrundeliegende Menge G und sodann an die auf G definierte Verknüpfung. Um die Notation zu verkürzen und damit knapp und übersichtlicher zu halten, sagen wir *„Sei G eine Gruppe ...“*, wenn wir in Wahrheit die Menge zusammen mit der Verknüpfung meinen. In der Regel ist die gemeinte Verknüpfung die offensichtliche Verknüpfung und es entstehen keine Mißverständnisse.

(2) Um die Verknüpfung zweier Gruppenelemente g und h zu bezeichenen, sind verschiedenste Notationen gebräuchlich, etwa

$$gh, \ g + h, \ g * h, \ g \circ h, \ \ldots$$

Bemerkung 1.3. (1) Die Assoziativität sorgt dafür, daß für $g_1, \ldots, g_r \in G$ das Element

$$g_1 g_2 \ldots g_r \in G$$

als Ergebnis von $r-1$ Verknüpfungen benachbarter Elemente unabhängig von der vorhandenen Wahl ist. Das ist unmittelbar klar, muß aber, wie alle Dinge die *offensichtlich* sind, bewiesen werden. Das gelingt durch vollständige Induktion nach der Länge r, aber damit wollen wir uns nicht aufhalten und überlassen das als Übungsaufgabe.

(2) Man kann die Axiome einer Gruppe abschwächen und zu einem äquivalenten Begriff kommen, wenn man nur die Existenz eines linksneutralen Elements und eines Linksinversen zu verlangen. Die Liste der Eigenschaften in Definition 1.1 ist aber diejenige, die man mit einer Gruppe verbinden sollte, und daher sprechen wir die Definition derart aus.

Beispiel 1.4. Beispiele für Gruppen sind bereits bekannt. Die wichtigsten in der linearen Algebra aufgetretenen Gruppen sind die folgenden.

(1) Die ganzen Zahlen $\mathbb{Z}$ mit Addition bilden eine Gruppe.

(2) Sei $n \geq 1$ eine natürliche Zahl. Die symmetrische Gruppe

$$S_n$$

ist die Menge aller Permutationen (bijektiven Selbstabbildungen) der Menge $\{1, \ldots, n\}$ mit der Komposition von Permutationen als Verknüpfung. Die symmetrische Gruppe ist nichts weiter als die volle Gruppe der Symmetrien der unstrukturierten Menge von n Elementen.

(3) Sei K ein Körper und V ein K-Vektorraum. Dann ist die Menge
$$\mathrm{GL}(V)$$
der bijektiven linearen Abbildungen $f : V \to V$ die **allgemeine**[3] **lineare Gruppe** von V. Die Gruppenverknüpfung hier ist wieder die Komposition und $\mathrm{GL}(V)$ ist die volle Gruppe der Symmetrien der Menge V, welche die K-lineare Vektorraumstruktur erhalten.
Speziell für $V = K^n$ setzen wir
$$\mathrm{GL}_n(K) = \mathrm{GL}(K^n) = \{A \in \mathrm{M}_n(K) \ ; \ \det(A) \neq 0\},$$
beschrieben durch invertierbare $n \times n$-Matrizen mit Einträgen aus K.

(4) Sei K ein Körper. Die **multiplikative Gruppe** von K ist die Teilmenge
$$K^\times = K \setminus \{0\}$$
mit der Multiplikation als Verknüpfung. Es ist geradezu die Definition eines Körpers: ein Ring K, für den $(K \setminus \{0\}, \cdot)$ eine Gruppe bildet.

(5) Die kleinste Gruppe ist $G = \{e\}$ mit der einzig möglichen Verknüpfung $ee = e$. Diese Gruppe nennt man die **triviale Gruppe**.

Bemerkung 1.5. Man sollte der Versuchung widerstehen, eine (endliche) Gruppe durch ihre Verknüpfungstafel, also eine Tabelle, welche die Werte gh mit $g, h \in G$ angibt, verstehen zu wollen. Zum Beispiel für eine Gruppe mit zwei Elementen $G = \{e, g\}$:

	e	g
e	e	g
g	g	e

Die dargestellte Information ist vollständig, aber auch vollständig nutzlos zum Verständnis. Wenigstens kann man sich mit diesem Beispiel leicht davon überzeugen, daß es im Wesentlichen (bis auf Bezeichnungen) nur eine Gruppe mit zwei Elementen gibt. Eine nützliche Beschreibung dieser Gruppe bekommt man als Gruppe
$$\{1, -1\}$$
etwa als Teilmenge von $\mathbb{R}$ mit der Multiplikation als Verknüpfung. Dabei ist $e = 1$ und $g = -1$.

Definition 1.6. Zwei Elemente g, h einer Gruppe G **kommutieren (miteinander)**, wenn
$$gh = hg.$$
Kommutieren in einer Gruppe alle Elemente miteinander, dann spricht man von einer **kommutativen** oder **abelschen**[4] Gruppe.

Beispiel 1.7. Auch Beispiele abelscher Gruppen sind bereits bekannt.

(1) Die ganzen Zahlen $(\mathbb{Z}, +)$ sind eine abelsche Gruppe.

(2) Sei $n \in \mathbb{Z}$. Wir erinnern daran, daß wir für $a, b \in \mathbb{Z}$ sagen „*a ist kongruent zu b modulo n*“ mit Notation $a \equiv b \pmod{n}$, wenn es ein $k \in \mathbb{Z}$ gibt mit $a - b = kn$. Die Relation *kongruent modulo n* ist eine Äquivalenzrelation auf $\mathbb{Z}$. Die Restklassen modulo n bilden mit der auf Vertretern der Restklassen definierten Addition eine abelsche Gruppe
$$\mathbb{Z}/n\mathbb{Z}.$$
Darin bezeichnen wir mit $[a]$ die Restklasse $a + n\mathbb{Z}$ zum Vertreter $a \in \mathbb{Z}$.

(3) Sei K ein Körper und sei V ein K-Vektorraum. Dann ist V mit der Addition aus der Vektorraumstruktur eine abelsche Gruppe.

[3] Englisch: general linear group, daher GL.

[4] Niels Henrik Abel, 1802–1829, norwegischer Mathematiker.

Bemerkung 1.8. (1) Die Kommutativität sorgt dafür, daß in einer kommutativen Gruppe G für $g_1, \ldots, g_n \in G$ das Element

$$g_1 g_2 \ldots g_n \in G$$

unabhängig von der Reihenfolge ist: Für jede Permutation $\sigma \in S_n$ gilt

$$g_1 g_2 \ldots g_r = g_{\sigma(1)} g_{\sigma(2)} \cdots g_{\sigma(n)}.$$

(2) Es gibt einen Struktursatz für endlich erzeugte abelsche Gruppen. Dieser benutzt weniger Methoden der Gruppentheorie, sondern solche der kommutativen Algebra, wie sie im Kapitel über Ringe und Moduln behandelt werden, und wird daher erst später behandelt.

Definition 1.9. (1) Das **direkte Produkt** zweier Gruppen G_1 und G_2 ist die Gruppe

$$G_1 \times G_2 = \{(g_1, g_2) \ ; \ g_1 \in G_1, g_2 \in G_2\}$$

mit komponentenweiser Komposition als Verknüpfung.

(2) Das **direkte Produkt** einer Menge G_i von Gruppen für $i \in I$ ist die Gruppe

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I} \ ; \ g_i \in G_i \text{ für alle } i \in I\}$$

mit komponentenweiser Komposition als Verknüpfung.

Bemerkung 1.10. Das direkte Produkt zweier Gruppen ist ein Spezialfall der allgemeinen Konstruktion für $I = \{1, 2\}$. Das neutrale Element in $\prod_{i \in I} G_i$ ist

$$(e_i)_{i \in I}$$

wobei $e_i \in G_i$ das neutrale Element ist. Die Komposition zweier Elemente ist

$$(g_i)_{i \in I} (h_i)_{i \in I} = (g_i h_i)_{i \in I}.$$

Das Inverse von $(g_i)_{i \in I}$ ist

$$(g_i)_{i \in I}^{-1} = (g_i^{-1})_{i \in I}.$$

1.2. **Elementare Folgerungen.** Die Definition einer Gruppe hat einige unmittelbare Konsequenzen für neutrale und inverse Elemente.

Proposition 1.11. *In jeder Gruppe ist das neutrale Element eindeutig.*

Beweis. Seien e und e' neutrale Elemente einer Gruppe G. Dann gilt

$$e = ee' = e'.$$ □

Notation 1.12. Das nach Proposition 1.11 eindeutige neutrale Element $e \in G$ wird oft mit 1 oder 0 bezeichnet je nachdem, ob man bei der Verknüpfung an eine Multiplikation oder eine Addition denkt. Beispielsweise ist $1 \in \mathrm{GL}_n(K)$ eine Kurznotation für die Einheitsmatrix. Dies ist nur eine Sprechweise und bedeutet sonst nichts.

Proposition 1.13. *In jeder Gruppe ist das Inverse eines Elements eindeutig.*
Genauer: sei $g \in G$ ein Element einer Gruppe G und $h \in G$ mit

$$hg = e,$$

dann ist h das Inverse von g. Hier bezeichnet e das neutrale Element von G.

Beweis. Sei k ein Inverses zu g. Dies existiert nach den Gruppenaxiomen. Dann gilt

$$h = he = h(gk) = (hg)k = ek = k.$$

Also ist $h = k$ ein Inverses.

Dasselbe Argument zeigt auch die Eindeutigkeit: sind h und k Inverse zu g, dann gilt $hg = e$, man kann k wie im obigen Argument wählen und schließt auf $h = k$. □

Notation 1.14. Das nach Proposition 1.13 eindeutige Inverse zu einem Element $g \in G$ wird mit

$$g^{-1}$$

bezeichnet, sofern die Verknüpfung multiplikativ geschrieben wird. Wird die Verknüpfung additiv geschrieben, wie das bei abelschen Gruppen üblich ist, so verwenden wir für das Inverse zu g die Notation $-g$.

Proposition 1.15. *Für Elemente g, h einer Gruppe gilt*

(1) $(gh)^{-1} = h^{-1}g^{-1}$,

(2) $(g^{-1})^{-1} = g$.

Beweis. (1) Wir berechnen

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}h = e.$$

und schließen nach Proposition 1.13, daß $h^{-1}g^{-1}$ das Inverse zu gh ist.

(2) Es gilt $g(g^{-1}) = e$, somit ist g Inverses zu g^{-1}. Die Eindeutigkeit des Inversen nach Proposition 1.13 zeigt $g = (g^{-1})^{-1}$. □

1.3. **Gruppenhomomorphismen.** Um Gruppen besser zu verstehen, braucht man einen Begriffsapparat für den Vergleich von Gruppen: strukturerhaltende Abbildungen.

Definition 1.16. Ein **Gruppenhomomorphismus** (oder **Homomorphismus von Gruppen**) ist eine Abbildung

$$f : G \to H$$

von einer Gruppe G nach einer Gruppe H mit der Eigenschaft, daß für alle $a, b \in G$ gilt:

$$f(ab) = f(a)f(b).$$

Beispiel 1.17. Auch für Gruppenhomomorphismen kenne wir bereits einige Beispiele.

(1) Die Determinante ist ein Gruppenhomomorphismus

$$\det : \mathrm{GL}_n(K) \to K^\times.$$

(2) Das aus der linearen Algebra bekannte Signum einer Permutation ist ein Gruppenhomomorphismus

$$\mathrm{sign} : S_n \to \{\pm 1\}.$$

Das Signum einer Transposition $\tau \in S_n$ ist $\mathrm{sign}(\tau) = -1$. Weil jede Permutation $\sigma \in S_n$ als Komposition von Transpositionen τ_i geschrieben werden kann, etwa

$$\sigma = \tau_1 \cdots \tau_s,$$

legt die Homomorphie das Signum dadurch eindeutig fest:

$$\mathrm{sign}(\sigma) = \mathrm{sign}(\tau_1) \cdots \mathrm{sign}(\tau_s) = (-1)^s.$$

Es gibt somit höchstens einen Homomorphismus $\mathrm{sign} : S_n \to \{\pm 1\}$ mit dem Wert -1 auf den Transpositionen.

Die Existenz des Signum ist eine nichttriviale Sache: Die Anzahl an Transpositionen, die man für eine Permutation braucht, ist modulo 2 unabhängig von der Wahl der Transpositionen.

Am einfachsten[5] sieht man die Existenz des Signum über die Determinante der Permutationsmatrizen ein. Sei $\sigma \in S_n$. Dann ist $P_\sigma \in \mathrm{GL}_n(\mathbb{Q})$ die Matrix, deren j-te Spalte $e_{\sigma(j)}$ ist. Es gilt also

$$P_\sigma(e_j) = e_{\sigma(j)},$$

[5]Hier droht ein Zirkelschluß, denn oft wird die Existenz der Determinate durch eine Formel bewiesen, die das Signum der Permutationen benötigt.

die Permutationsmatrix permutiert die Standardbasis wie dies σ vorschreibt. Daher gilt für $\sigma, \pi \in S_n$:

$$P_{\sigma\pi} = P_\sigma P_\pi,$$

denn für alle $j = 1, \ldots, n$ gilt

$$P_{\sigma\pi}(e_j) = e_{\sigma\pi(j)} = e_{\sigma(\pi(j))} = P_\sigma(e_{\pi(j)}) = P_\sigma(P_\pi(e_j)) = (P_\sigma \circ P_\pi)(e_j).$$

Die Zuordnung $\rho(\sigma) = P_\sigma$ ist ein Gruppenhomomorphismus

$$\rho : S_n \to \mathrm{GL}_n(\mathbb{Q}),$$

den wir die **Permutationsdarstellung** von S_n nennen.

Das Signum bekommen wir nun als Komposition

$$\mathrm{sign}(\sigma) = \det(\rho(\sigma)).$$

In der Tat ist dies ein Gruppenhomomorphismus und nimmt auf Transpositionen nach Eigenschaft der Determinante den Wert -1 an.

(3) Sei $n \in \mathbb{Z}$. Die Addition auf $\mathbb{Z}/n\mathbb{Z}$ ist gerade so gemacht, daß die Restklassenabbildung

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto a + n\mathbb{Z}$$

ein Gruppenhomomorphismus ist.

(4) Sei $f : V \to W$ eine lineare Abbildung von K-Vektorräumen. Dann ist f ein Gruppenhomomorphismus der zugrundeliegenden abelschen Gruppen $(V, +)$ und $(W, +)$.

(5) Sei I eine Menge und sei G_i eine Gruppe für $i \in I$. Sei $n \in I$ ein Element. Die Projektion auf die n-te Koordinate des Produkts

$$p_n : \prod_{i \in I} G_i \to G_n$$

ist der Gruppenhomomorphismus mit $p_n((g_i)_{i\in I}) = g_n$. Die Homomorphieeigenschaft folgt sofort aus der Definition des Produkts, weil die Gruppenverknüpfung im Produkt komponentenweise erklärt ist.

Lemma 1.18. *Sei G eine Gruppe. Das neutrale Element von G ist das einzige Element $g \in G$ mit $gg = g$.*

Beweis. Sei $e \in G$ das neutrale Element. Dann gilt $ee = e$. Für die umgekehrte Richtung betrachten wir ein $g \in G$ mit $gg = g$. Dann ist

$$e = g^{-1}g = g^{-1}(gg) = (g^{-1}g)g = eg = g.$$ □

Lemma 1.19. *Sei $f : G \to H$ ein Gruppenhomomorphismus.*

(1) Es gilt

$$f(e_G) = e_H,$$

wobei e_G das neutrale Element in G und e_H das in H bezeichne.

(2) Für alle $g \in G$ gilt

$$f(g^{-1}) = f(g)^{-1}.$$

Beweis. (1) Aus $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$ folgt durch $f(e_G) = e_H$ nach Lemma 1.18.

(2) Sei nun wieder $e \in G$ das neutrale Element. Wegen (1) gilt für $g \in G$

$$f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e.$$

Daraus folgt mit Proposition 1.13 die Behauptung. □

Definition 1.20. Ein **Isomorphismus** (von Gruppen) ist ein bijektiver Gruppenhomomorphismus, und ein **Automorphismus** (von Gruppen) ist ein Isomorphismus $G \to G$.

Zwei Gruppen G und H heißen **isomorph**, wenn es einen Isomorphismus $G \to H$ zwischen ihnen gibt. Als Notation verwenden wir $G \simeq H$.

Beispiel 1.21. Die positiven reellen Zahlen $\mathbb{R}_{>0} \subseteq \mathbb{R}^\times$ bilden mit Multiplikation eine Gruppe. Die Exponentialfunktion nimmt nur Werte in $\mathbb{R}_{>0}$ an und liefert einen Gruppenhomomorphismus

$$\exp : \mathbb{R} \to \mathbb{R}_{>0},$$

denn für alle $x, y \in \mathbb{R}$ gilt

$$\exp(x + y) = \exp(x) \exp(y).$$

Dies ist sogar ein Isomorphismus. Die Umkehrabbildung ist der natürliche Logarithmus.

Proposition 1.22. *Es gilt:*

(1) Die Komposition von Gruppenhomomorphismen ist wieder ein Gruppenhomomorphismus.
(2) Die Identität ist ein Gruppenhomomorphismus.
(3) Ein bijektiver Gruppenhomomorphismus hat eine links- und rechtsinverse Abbildung bezüglich der Komposition, welche selbst Gruppenhomomorphismus ist.

Beweis. (1) Seien $g : G \to H$ und $f : H \to K$ Gruppenhomomorphismen. Dann gilt für alle $a, b \in G$ für $h = f \circ g$, daß

$$h(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = h(a)h(b),$$

und damit ist h auch ein Gruppenhomomorphismus.

Aussage (2) ist trivial.

(3) Sei $f : G \to H$ bijektiver Gruppenhomomorphismus. Dann gibt es $f^{-1} : H \to G$ als Mengenabbildung mit der Eigenschaft $f \circ f^{-1} = \mathrm{id}_H$ und $f^{-1} \circ f = \mathrm{id}_G$. Es bleibt zu zeigen, daß f^{-1} ein Gruppenhomomorphismus ist. Dazu benutzen wir die Bijektivität von f und beschreiben zwei beliebige Elemente $x, y \in H$ durch $a, b \in G$ als $x = f(a)$, $y = f(b)$. Wir rechnen nun

$$f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y),$$

und dies weist f^{-1} als Gruppenhomomorphismus aus. □

Korollar 1.23. *Die Menge* $\mathrm{Aut}(G)$ *aller Automorphismen einer Gruppe* G *ist bezüglich der Komposition eine Gruppe.* □

Beispiel 1.24. Sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. Sei n eine natürliche Zahl. Die Skalarmultiplikation auf dem $\mathbb{F}_p$-Vektorraum $\mathbb{F}_p^n$ wird schon durch die Addition der zugrundeliegenden abelschen Gruppe erklärt. Genauer, sei $v \in \mathbb{F}_p^n$ ein Vektor, und sei der Skalar $\alpha \in \mathbb{F}_p$ repräsentiert durch $a \in \mathbb{N}$, dann ist αv durch

$$\alpha v = \underbrace{v + \ldots + v}_{a\text{-mal}}$$

erklärt. Dies hat zur Folge, daß $\mathbb{F}_p$-lineare Abbildungen von $\mathbb{F}_p$-Vektorräumen dasselbe sind wie Gruppenhomomorphismen der zugrundeliegenden abelschen Gruppen. Die Verträglichkeit mit der Skalarmultiplikation ist automatisch. Daraus folgt

$$\mathrm{Aut}(\mathbb{F}_p^n) = \mathrm{GL}_n(\mathbb{F}_p).$$

Übungsaufgaben zu §1

Übungsaufgabe 1.1. Zeigen Sie, daß in einer Gruppe G für Elemente $g_1, \ldots, g_r \in G$ die Verknüpfung

$$g_1 \ldots g_r$$

von der konkret gewählten Klammerung unabhängig ist.

Übungsaufgabe 1.2. Seien $g_1, \ldots, g_n$ Elemente einer kommutative Gruppe G. Zeigen Sie, daß für jede Permutation $\sigma \in S_n$ gilt:

$$g_1 g_2 \ldots g_r = g_{\sigma(1)} g_{\sigma(2)} \ldots g_{\sigma(n)}.$$

Übungsaufgabe 1.3. Sei $G = \{e, g\}$ eine Gruppe mit genau zwei Elementen: mit neutralem Element e und $g \neq e$.

(a) Zeigen Sie, daß dann $gg = e$ gelten muß.
(b) Finden Sie einen Isomorphismus $G \simeq \mathbb{Z}/2\mathbb{Z}$.

Bemerkung: Sie zeigen hier, daß es bis auf Isomorphismus genau eine Gruppe mit zwei Elementen gibt. Darüberhinaus ist selbst der Isomorphismus zwischen zwei Gruppen der Ordnung 2 eindeutig.

Übungsaufgabe 1.4. In der Regel gilt für Elemente $g, h \in G$ und $n \in \mathbb{Z}$ nicht

$$(gh)^n = g^n h^n.$$

Finden Sie ein Beispiel. Zeigen Sie, wenn dies für $n = -1$ und g, h gilt, dann kommutieren g, h, und dann gilt die Gleichung bereits für alle $n \in \mathbb{Z}$.

Übungsaufgabe 1.5. Sei G eine Gruppe und $\mu : G \times G \to G$ die Komposition. Zeigen Sie, daß μ denau dann ein Gruppenhomomorphismus ist, wenn G abelsch ist.

Übungsaufgabe 1.6. Sei G eine endliche Gruppe. Zeigen Sie, daß dann auch $\mathrm{Aut}(G)$ eine endliche Gruppe ist.

2. Untergruppen

In diesem Kapitel betrachten wir Potenzen eines Gruppenelements. Dies führt zum Begriff der Ordnung, der vom Element erzeugten Untergruppe, und damit allgemeiner zu Untergruppen.

2.1. **Die Potenzen eines Elements.** In multiplikativer Schreibweise kann man Gruppenelemente potenzieren.

Definition 2.1. Sei $g \in G$ ein Element einer Gruppe G mit neutralem Element 1. Wir setzen $g^0 = 1$ und dann für $n \geq 1$ rekursiv

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

Die Notation g^{-1} ist doppelt, aber konsistent definiert. Für $n \geq 1$ ergibt sich

$$g^n = \underbrace{g \cdot \ldots \cdot g}_{n\text{-mal}}.$$

Lemma 2.2. *Sei $g \in G$ ein Gruppenelement. Für alle $n \in \mathbb{N}$ gilt*

$$g^{n+1} = g^n \cdot g.$$

Beweis. Für $n \geq 0$ gilt dies per Definition. Für $n < 0$ setzen wir $n = -m$ mit $m > 0$ und rechnen

$$g^{n+1} = g^{-(m-1)} = g^{-(m-1)} \cdot (g^{-1} \cdot g) = \left(g^{-(m-1)} \cdot g^{-1}\right) \cdot g = g^{-m} \cdot g = g^n \cdot g. \qquad \square$$

Die üblichen Potenzregeln mit fester Basis gelten, denn diese spiegeln nur die Abzählkombinatorik von Faktoren wider.

Proposition 2.3 (Potenzgesetze)**.** *Sei $g \in G$ ein Gruppenelement und $n, m \in \mathbb{Z}$. Dann gelten*

(1) $g^0 = 1$ *und* $g^1 = g$,
(2) $g^n \cdot g^m = g^{n+m}$,
(3) $g^{-n} = (g^n)^{-1}$,
(4) $(g^n)^m = g^{nm}$.

Beweis. Das ist trivial. Formal gelingt der Beweis am besten durch Fallunterscheidung nach den Vorzeichen von n und m sowie durch vollständige Induktion. Die Aussage (1) folgt direkt aus der Definition.

Wir beweisen (2) per Induktion nach $|m|$. Der Induktionsanfang hat $m = 0$ und gilt trivialerweise: $g^n \cdot g^0 = g^n \cdot 1 = g^n = g^{n+0}$. Wir nehmen nun an, daß (2) in allen Fällen mit kleinerem $|m|$ gilt. Es gibt nun zwei Fälle je nach Vorzeichen von m:

- $m \geq 1$. Wir verwenden die Induktionsannahme für n und $m-1$:
$$g^n \cdot g^{m-1} = g^{n+m-1}$$
Dann rechnen wir mit Lemma 2.2
$$g^n \cdot g^m = g^n \cdot (g^{m-1} \cdot g) = (g^n \cdot g^{m-1}) \cdot g = g^{n+m-1} \cdot g = g^{n+m}.$$
- $m \leq -1$. Wir verwenden die Induktionsannahme für n und $m+1$:
$$g^n \cdot g^{m+1} = g^{n+m+1}$$
Dann rechnen wir mit Lemma 2.2
$$(g^n \cdot g^m) \cdot g = g^n \cdot (g^m \cdot g) = g^n \cdot g^{m+1} = g^{n+m+1} = g^{n+m} \cdot g.$$
Durch Multiplikation mit g^{-1} von rechts ergibt sich die Behauptung.

Jetzt beweisen wir (3). Nach Proposition 1.13 reicht die Rechnung (mittels (2))
$$g^{-n} \cdot g^n = g^{-n+n} = g^0 = 1.$$

Aussage (4) beweisen wir zunächst per Induktion nach m für $m \geq 0$. Der Fall $m = 0$ ist trivial und die Rechnung
$$(g^n)^{m+1} = (g^n)^m \cdot g^n = g^{nm} \cdot g^n = g^{nm+n} = g^{n(m+1)}$$
zeigt den Induktionsschritt.

Der Fall $m < 0$ wird durch zweimaliges Anwenden von (3) auf den Fall $m > 0$ zurückgeführt:
$$(g^n)^m = \big((g^n)^{-m}\big)^{-1} = \big(g^{-nm}\big)^{-1} = g^{nm}.$$ □

Korollar 2.4. *Sei G eine Gruppe und $g \in G$ ein Element. Die Abbildung*
$$\varphi : \mathbb{Z} \to G, \qquad \varphi(a) = g^a$$
ist ein Gruppenhomomorphismus.

Beweis. Das folgt sofort aus Proposition 2.3 (2). □

Bemerkung 2.5. Man beachte hingegen, daß in der Regel für $g, h \in G$ und $n \in \mathbb{Z}$
$$(gh)^n \neq g^n h^n.$$

Bemerkung 2.6. In einer abelschen Gruppe A verwenden wir anstelle der Potenzschreibweise das Folgende. Sei $a \in A$ ein Element. Wir setzen $0 \cdot a = 0$ und dann für $n \in \mathbb{Z}$ rekursiv
$$n \cdot a = (n-1) \cdot a + a.$$
Damit ist
$$n \cdot a = \underbrace{a + \ldots + a}_{n\text{-mal}}.$$
Für $n \in \mathbb{N}$, definieren wir allgemeiner
$$(-n) \cdot a = n \cdot (-a) = \underbrace{(-a) + \ldots + (-a)}_{n\text{-mal}}.$$
Damit ist $n \cdot a$, kurz na für alle $a \in A$ und $n \in \mathbb{Z}$ definiert. In der Notation halten wir uns an Punkt- vor Strichrechnung und sparen so Klammern.

Proposition 2.3 übersetzt sich in die erwarteten Assoziativ- und Distributivgesetze: für alle $a, b \in A$ und $n, m \in \mathbb{Z}$ gilt

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

Da A kommutativ ist, gilt zudem auch noch das andere Distributivgesetz

$$n \cdot (a + b) = n \cdot a + n \cdot b.$$

2.2. **Die Ordnung.**

Notation 2.7. Sei G eine Gruppe und $g \in G$ ein Element. Das Bild der Abbildung $\varphi(a) = g^a$ aus Korollar 2.4 bezeichnen wir mit

$$\langle g \rangle := \mathrm{im}(\varphi) = \{g^a \ ; \ a \in \mathbb{Z}\}.$$

Dies ist die Teilmenge der Potenzen von g in G.

Definition 2.8. Die **Ordnung** eines Elements g einer Gruppe G ist

$$\mathrm{ord}(g) := \min\{n \in \mathbb{N}, n > 0 \ ; \ g^n = 1\},$$

sofern diese Menge nicht leer ist und damit ein Minimum hat. Andernfalls sagen wir g hat **unendliche Ordnung** und schreiben $\mathrm{ord}(g) = \infty$.

Beispiel 2.9. (1) Betrachten wir das Element $1 \in \mathbb{Z}$. Dann ist für $n \in \mathbb{Z}$

$$n \cdot 1 = n,$$

also hat 1 unendliche Ordnung: $\mathrm{ord}(1) = \infty$.

(2) Betrachten wir das Element $[1] \in \mathbb{Z}/n\mathbb{Z}$. Dann ist für alle $m \in \mathbb{Z}$

$$m \cdot [1] = [m],$$

also $\mathrm{ord}([1]) = n$.

(3) Betrachten wir das Element $\sigma \in S_n$, das die Elemente $1, 2, \ldots, n$ zyklisch permutiert:

$$\sigma(i) \equiv i + 1 \pmod{n},$$

oder als Permutation in Form einer Wertetabelle:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}.$$

Dann gilt für alle $i \in \{1, \ldots, n\}$

$$\sigma^r(i) \equiv i + r \pmod{n}$$

und somit $\mathrm{ord}(\sigma) = n$.

(4) Für $\varphi \in \mathbb{R}$ betrachte die Matrix

$$D_\varphi = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{R})$, welche eine Drehung um den Winkel φ beschreibt. Die Additionstheoreme für Sinus und Cosinus sind gerade äquivalent zur Matrixgleichung

$$D_\varphi D_\psi = D_{\varphi+\psi}.$$

Die Zuordnung $\varphi \mapsto D_\varphi$ beschreibt daher einen Gruppenhomomorphismus

$$(\mathbb{R}, +) \to \mathrm{GL}_2(\mathbb{R}).$$

Sei $n \in \mathbb{N}$ und speziell $\varphi = \frac{2\pi}{n}$. Dann ist in $\mathrm{GL}_2(\mathbb{R})$

$$(D_{2\pi/n})^n = D_{2\pi} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

aber $(D_{2\pi/n})^m = D_{2\pi m/n} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ für alle $0 < m < n$. Das Element $D_{2\pi/n}$ hat also die Ordnung n.

(5) Sei K ein Körper und $A \in \mathrm{GL}_n(K)$ die Matrix (der Rest wird mit 0 aufgefüllt)

$$A = \begin{pmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

Dies beschreibt die lineare Abbildung, welche auf der Standardbasis $(e_1, \ldots, e_n)$ durch

$$Ae_i = e_{i+1}$$

(mit dem Index modulo n) wirkt. Es gilt

$$\mathrm{ord}(A) = n,$$

wie man aus $A^r e_i = e_{i+r}$ (mit dem Index modulo n) sofort sieht.

Definition 2.10. Die **Ordnung** einer Gruppe G ist die Mächtigkeit (die Anzahl der Elemente)

$$|G|$$

der zugrundeliegenden Menge G.

Beispiel 2.11. (1) Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ hat die Ordnung

$$|\mathbb{Z}/n\mathbb{Z}| = n,$$

denn durch $\{0, \ldots, n-1\}$ wird ein vollständiges Vertretersystem für die Äquivalenzklassen modulo n beschrieben.

(2) Sind G und H endliche Gruppen, so ist $G \times H$ endlich und $|G \times H| = |G| \cdot |H|$.

Proposition 2.12 (Zwei Bedeutungen von Ordnung)**.** *Sei G eine Gruppe und $g \in G$ ein Element. Dann ist $\langle g \rangle$ mit der von G geerbten Verknüpfung eine Gruppe.*

(1) Sei $\mathrm{ord}(g) = n$ *endlich. Dann gilt*

$$\langle g \rangle = \{g^0 = 1, g, g^2, \ldots, g^{n-1}\},$$

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

(2) Sei $\mathrm{ord}(g) = \infty$ *unendlich. Dann gilt für alle $a, b \in \mathbb{Z}$, daß aus $g^a = g^b$ bereits $a = b$ folgt, und* $|\langle g \rangle| = \mathrm{ord}(g)$ *ist unendlich.*

Beweis. Daß es sich bei $\langle g \rangle$ um eine Gruppe handelt, folgt sofort aus Proposition 2.3: es gibt ein neutrales Element g^0, und g^{-n} ist ein inverses Element zu g^n, denn für alle $a, b \in \mathbb{Z}$ gilt $g^a g^b = g^{a+b}$. Assoziativität erbt $\langle g \rangle$ sofort von G.

(1) Sei nun $\mathrm{ord}(g) = n$ endlich. Mittels Division mit Rest kann man jede ganze Zahl a als $a = qn + r$ mit $0 \leq r < n$ schreiben. Dann ist

$$g^a = g^{qn+r} = (g^n)^q \cdot g^r = g^r.$$

Damit hat $\langle g \rangle$ die angegebenen Elemente. Es bleibt zu zeigen, daß keine zwei g^a und g^b mit $0 \leq a < b \leq n-1$ gleich sind. Aber aus $g^a = g^b$ folgt

$$1 = g^b \cdot (g^a)^{-1} = g^b \cdot g^{-a} = g^{b-a}.$$

Dies ist ein Widerspruch zur Minimalität von $n = \mathrm{ord}(g)$ aus der Definition der Ordnung, denn $0 < b - a < n$, aber trotzdem $g^{b-a} = 1$.

(2) Angenommen $g^a = g^b$ mit ganzen Zahlen $a \neq b$. Dann ist oBdA $b > a$ und damit $g^{b-a} = 1$ im Widerspruch zur Definition von $\mathrm{ord}(g) = \infty$. □

2.3. **Untergruppen.** Ein erstes Verständnis einer Gruppe erlangt man durch das Studium ihrer inneren Struktur, etwa ihrer Untergruppen.

Definition 2.13. Eine **Untergruppe** einer Gruppe G ist eine Teilmenge $U \subseteq G$, so daß für alle $g, h \in U$ auch $gh \in U$ und U mit der Einschränkung

$$U \times U \to U$$
$$(g, h) \mapsto gh$$

der Verknüpfung von G selbst eine Gruppe ist.

Bemerkung 2.14. Der zweite Teil der Definition ist nur aufgrund des ersten Teils wohldefiniert: die Einschränkung der Verknüpfung auf $U \times U \subseteq G \times G$ ist nur dann eine Verknüpfung auf U, also mit Werten in U, wenn man dies zuerst gefordert hat.

Notation 2.15. Wir werden eine Untergruppe U einer Gruppe G oft durch $U < G$ oder $U \leq G$ bezeichnen. Diese Notation ist aber nicht allgemeingültiger Standard.

Beispiel 2.16. (1) Die positiven reellen Zahlen mit Multiplikation bilden eine Untergruppe

$$\mathbb{R}_{>0} \subseteq \mathbb{R}^\times.$$

(2) Sei $n \in \mathbb{Z}$. Die Menge $n\mathbb{Z}$ der durch n teilbaren ganzen Zahlen ist eine Untergruppe

$$n\mathbb{Z} = \{a \in \mathbb{Z} \ ; \ a = nx \text{ für ein } x \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

(3) In jeder Gruppe G sind die triviale Gruppe $\{e\}$ und die ganze Gruppe G Untergruppen.

(4) Die Teilmenge

$$\{\pm 1\} \subset \mathbb{Q}^\times$$

ist eine Untergruppe (das ist gerade $\mathbb{Z}^\times$, vgl Kapitel §7).

(5) Die rationalen Matrizen $\mathrm{GL}_n(\mathbb{Q}) \subseteq \mathrm{GL}_n(\mathbb{R})$ sind eine Untergruppe. Allgemeiner haben wir für eine beliebige Körpererweiterung $K \subseteq L$ die Untergruppe

$$\mathrm{GL}_n(K) \subseteq \mathrm{GL}_n(L).$$

(6) Die Menge $\mathrm{Aff}^1(K) = K^\times \times K$ kann man als invertierbare affin-lineare Transformationen des 1-dimensionalen Vektorraums K begreifen. Ein $(a, b) \in \mathrm{Aff}^1(K)$ beschreibt

$$x \mapsto ax + b.$$

Die Komposition von Abbildungen definiert eine Verknüpfung auf $\mathrm{Aff}^1(K)$:

$$(ax + b) \circ (cx + d) = (a(cx + d) + b) = acx + ad + b,$$

also

$$(a, b)(c, d) := (ac, ad + b).$$

Dies ist die affin-lineare Gruppe in Dimension 1 (Übung!). Die Teilmengen

$$U = \{(a, 0) \ ; \ a \in K^\times\}$$

ist eine Untergruppe isomorph zu $K^\times$ und

$$V = \{(0, b) \ ; \ b \in K\}$$

ist eine Untergruppe isomorph zu $(K, +)$.

(7) Seien G eine beliebige Gruppe und $g \in G$ ein Element. Dann ist $\langle g \rangle \subseteq G$ eine Untergruppe nach Proposition 2.12.

Lemma 2.17. *Sei $U \leq G$ eine Untergruppe.*

(1) Das neutrale Element von G ist auch das neutrale Element von U.

(2) *Sei $u \in U$ und u^{-1} das zu u in G inverse Element. Dann ist $u^{-1} \in U$ und in U das zu u inverse Element.*

Beweis. (1) Sei $\varepsilon \in U$ neutrales Element für die Gruppe U. Aus $\varepsilon\varepsilon = \varepsilon$ in U folgt mit Lemma 1.18, daß ε auch neutrales Element von G ist.

(2) Sei $u \in U$ beliebig, u^{-1} das inverse Element in G und $v \in U$ das inverse Element in U. Dann gilt (mit (1))

$$u^{-1} = u^{-1}e = u^{-1}(uv) = (u^{-1}u)v = ev = v \in U. \qquad \square$$

Notation 2.18. Für Teilmengen $A, B \subseteq G$ einer Gruppe G und ein Element $g \in G$ vereinbaren wir die Notationen

$$\begin{aligned} AB &:= \{ab \ ; \ a \in A, b \in B\}, \\ gA &:= \{ga \ ; \ a \in A\}, \\ Ag &:= \{ag \ ; \ a \in A\}, \\ A^{-1} &:= \{a^{-1} \ ; \ a \in A\}. \end{aligned}$$

Ein Kriterium zum Nachweis, ob eine Teilmenge eine Untergruppe ist, besteht wie folgt.

Proposition 2.19 (Untergruppenkriterium)**.** *Sei U eine Teilmenge einer Gruppe G. Dann sind äquivalent:*

(a) *U ist Untergruppe.*
(b) *U ist nicht leer, $UU \subseteq U$ und $U^{-1} \subseteq U$.*
(c) *U ist nicht leer und für alle $u, v \in U$ folgt $uv^{-1} \in U$.*

Beweis. Wir zeigen im Ringschluß (a) $\implies$ (b) $\implies$ (c) $\implies$ (a).

(a) $\implies$ (b): Es gelte Aussage (a). Dann enthält U ein neutrales Element, ist also nicht leer, und per Defintion gilt $UU \subseteq U$. Nach Lemma 2.17 sind das Inverse in G und das Inverse in U für $u \in U$ dasselbe. Also folgt, daß auch $U^{-1} \subseteq U$.

(b) $\implies$ (c): Es gelte Aussage (b). Für beliebige u, v schließen wir dann

$$uv^{-1} \in uU^{-1} \subseteq uU \subseteq UU \subseteq U,$$

also gilt Aussage (c).

(c) $\implies$ (a): Es gelte Aussage (c). Da U nicht leer ist, gibt es ein $u \in U$. Damit auch

$$e = uu^{-1} \in U.$$

Für ein beliebiges $v \in U$ gilt dann

$$v^{-1} = ev^{-1} \in U,$$

somit $U^{-1} \subseteq U$. Damit folgt für beliebige $u, v \in U$, daß

$$uv = u(v^{-1})^{-1} \in U.$$

Die nun wohldefinierte Einschränkung $U \times U \to U$ der Verknüpfung $G \times G \to G$ ist weiterhin assoziativ, besitzt ein neutrales Element, da wir schon $e \in U$ gelernt haben, und jedes $u \in U$ hat Inverse in U, da wir $U^{-1} \subseteq U$ verifiziert haben. Damit ist U eine Untergruppe. $\square$

Für die Gruppe $(\mathbb{Z}, +)$ haben wir einen vollständigen Überblick über alle Untergruppen.

Satz 2.20 (Die Untergruppen von $\mathbb{Z}$)**.** *Jede Untergruppe von $\mathbb{Z}$ ist von der Form*

$$n\mathbb{Z} = \{na \ ; \ a \in \mathbb{Z}\}$$

für ein eindeutiges $n \in \mathbb{N}_0$.

Beweis. Die Teilmengen $n\mathbb{Z}$ erfüllen das Kriterium aus Proposition 2.19, denn mit $na, nb \in n\mathbb{Z}$ ist auch

$$na + (-nb) = n(a - b) \in n\mathbb{Z}.$$

Daher ist $n\mathbb{Z}$ Untergruppe.

Sei also umgekehrt $U \subseteq \mathbb{Z}$ eine Untergruppe. Wir betrachten die positiven Elemente in U:

$$P = \{g \in U \ ; \ g > 0\}.$$

Dann gilt $U = P \cup \{0\} \cup -P$, wobei $-P$ die additiven Inversen zu den Elementen aus P enthält. Entweder gilt $P = \emptyset$, und dann ist $U = \{0\} = 0\mathbb{Z}$. Oder es gilt $P \neq \emptyset$, und dann gibt[6] es ein minimales Element in P

$$n = \min P.$$

Mit $n \in U$ ist auch $n + n = 2n, n + n + n = 3n, \ldots \in U$, insgesamt gilt sicher

$$n\mathbb{Z} \subseteq U.$$

Wir zeigen nun die umgekehrte Inklusion. Sei dazu $g \in U$ beliebig. Division mit Rest von g durch n liefert $q, r \in \mathbb{Z}$ mit $0 \leq r < n$ und

$$g = qn + r.$$

Mit g ist auch $r = g - nq \in U$. Wenn $r > 0$ gelten würde, dann wäre $r \in P$, was der Konstruktion von n als Minimum von P widerspricht. Daher muß $r = 0$ und damit $g = nq \in n\mathbb{Z}$ gelten. Dies zeigt $U \subseteq n\mathbb{Z}$ und damit $U = n\mathbb{Z}$. □

Lemma–Definition 2.21. *Das **Zentrum** einer Gruppe G ist die Untergruppe*

$$Z(G) = \{g \in G \ ; \ \text{für alle } h \in G \text{ gilt } gh = hg\}$$

derjenigen Elemente, die mit allen Gruppenelementen kommutieren.

Beweis. Wir müssen zeigen, daß $Z(G)$ eine Untergruppe ist. Dies folgt sofort aus dem Untergruppenkriterium Proposition 2.19.

Wegen $1 \in Z(G)$ ist das Zentrum nicht leer. Wenn $a, b \in Z(G)$, dann gilt für alle $x \in G$:

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab),$$

also auch $ab \in Z(G)$. Weiter gilt auch $a^{-1} \in Z(G)$, denn

$$a^{-1}x = a^{-1}x(aa^{-1}) = a^{-1}(xa)a^{-1} = a^{-1}(ax)a^{-1} = (a^{-1}a)xa^{-1} = xa^{-1}.$$ □

Beispiel 2.22. (1) Das Zentrum einer abelschen Gruppe A ist $Z(A) = A$.

(2) Sei $n \geq 3$. Dann ist das Zentrum der symmetrischen Gruppe $Z(S_n) = 1$ die triviale Gruppe. Das ist hier eine Übungsaufgabe und wird später als Korollar bewiesen.

(3) Sei K ein Körper. Das Zentrum von $\mathrm{GL}_n(K)$ besteht genau aus den Diagonalmatrizen mit konstanter Diagonale aus $K^\times$. Als Gruppe ist das Zentrum isomorph zu $K^\times$ via $K^\times \to Z(\mathrm{GL}_n(K))$, $\lambda \mapsto \lambda \cdot \mathbf{1}_n$.

[6] Das ist nicht so trivial, wie es scheint. Die Existenz eines minimalen Elements in einer nichtleeren Teilmenge von $\mathbb{N}$ nennt man Eigenschaft der *Wohlordnung*. Dies ist eine Eigenschaft der natürlichen Zahlen, die aus den Axiomen folgt und äquivalent zum Axiom der vollständigen Induktion ist.

2.4. **Homomorphismen und Untergruppen.**

Proposition 2.23. *Sei $f : G \to H$ ein Gruppenhomomorphismus und $U \subseteq G$ und $V \subseteq H$ Untergruppen. Dann sind $f^{-1}(V) \subseteq G$ und $f(U) \subseteq H$ Untergruppen.*

Beweis. Dies folgt sofort aus dem Untergruppenkriterium Proposition 2.19. Wir behandeln zuerst $f^{-1}(V)$. Aus $f(1) = 1 \in V$ folgt $1 \in f^{-1}(V)$ ist nicht leer. Aus $a, b \in f^{-1}(V)$ folgen

$$f(ab) = f(a)f(b) \in V,$$
$$f(a^{-1}) = f(a)^{-1} \in V,$$

also $ab, a^{-1} \in f^{-1}(V)$. Damit ist $f^{-1}(V)$ eine Untergruppe von G.

Nun behandeln wir $f(U)$. Zu $a, b \in f(U)$ gibt es $x, y \in U$ mit $a = f(x), b = f(y)$. Dann gelten

$$ab = f(x)f(y) = f(xy) \in f(U)$$
$$a^{-1} = f(x)^{-1} = f(x^{-1}) \in f(U),$$

so daß $f(U)$ eine Untergruppe in H ist. □

Definition 2.24. Sei $f : G \to H$ ein Gruppenhomomorphismus.

(1) Der **Kern** von f ist die Untergruppe von G

$$\ker(f) = \{g \in G \ ; \ f(g) = 1\} = f^{-1}(1).$$

(2) Das **Bild** von f ist die Untergruppe von H

$$\mathrm{im}(f) = \{h \in H \ ; \ \text{ es gibt ein } g \in G \text{ mit } f(g) = h\} = f(G).$$

Beispiel 2.25. (1) Der **Einheitskreis** $\mathrm{S}^1 = \{z \in \mathbb{C}^\times \ ; \ |z| = 1\} \subseteq \mathbb{C}^\times$ ist der Kern des Betragshomomorphismus

$$|\ | : \mathbb{C}^\times \to \mathbb{R}^\times, \qquad z \mapsto |z|$$

und damit eine Untergruppe. Das Bild ist die Gruppe $\mathbb{R}_{>0}$ der positiven reellen Zahlen mit Multiplikation.

(2) Sei $n \geq 1$ eine natürliche Zahl. Die **alternierende Gruppe**

$$A_n = \{\sigma \in S_n \ ; \ \mathrm{sign}(\sigma) = 1\}$$

ist der Kern des Signum-Homomorphismus und damit eine Untergruppe von S_n.

(3) Sei $n \in \mathbb{N}$ und sei K ein Körper. Die **spezielle lineare Gruppe** der Dimension n

$$\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) \ ; \ \det(A) = 1\}$$

ist der Kern des Homomorphismus Determinante $\det : \mathrm{GL}_n(K) \to K^\times$. Aus

$$\det \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} = \lambda$$

folgt $\mathrm{im}(\det) = K^\times$.

Die folgende Proposition ist analog zu einer Aussage über lineare Abbildungen.

Proposition 2.26. *Der Gruppenhomomorphismus $f : G \to H$ ist injektiv genau dann, wenn*

$$\ker(f) = \{1\}.$$

Beweis. Wenn f injektiv ist, dann folgt aus $g \in \ker(f)$, also $f(g) = 1 = f(1)$ bereits $g = 1$. Somit gilt $\ker(f) = \{1\}$.

Sei umgekehrt $\ker(f) = \{1\}$. Seien $a, b \in G$ mit $f(a) = f(b)$. Dann ist $ab^{-1} \in \ker(f)$, weil $f(ab^{-1}) = f(a)f(b)^{-1} = 1$. Damit folgt $ab^{-1} = 1$, also $a = b$ und f ist injektiv. □

Proposition 2.27. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Die Abbildungen $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$ sind zueinander inverse Bijektionen der Mengen von Untergruppen*

$$\{U \subseteq G \ ; \ \ker(f) \subseteq U\} \overset{\sim}{\leftrightarrow} \{V \subseteq H \ ; \ V \subseteq f(G)\}.$$

Beweis. Nach Proposition 2.23 sind $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$ wohldefiniert, d.h., die Bild- bzw. Urbildmenge ist eine Untergruppe der geforderten Form.

Sei $V \subseteq f(G)$ eine Untergruppe von H. Dann ist

$$f(f^{-1}(V)) = V,$$

weil dies bereits für eine Teilmenge von $f(G)$ gilt. Die Bedingung $V \subseteq f(G)$ sorgt dafür, daß jedes Element von V auch im Bild von $f^{-1}(V)$ enthalten ist.

Sei $U \subseteq G$ eine Untergruppe mit $\ker(f) \subseteq U$. Dann ist per Definition

$$U \subseteq f^{-1}(f(U)).$$

Es bleibt zu zeigen, daß jedes $x \in f^{-1}(f(U))$ aus U kommt. Wegen $f(x) \in f(U)$ gibt es $a \in U$ mit $f(x) = f(a)$. Dann ist $xa^{-1} \in \ker(f)$ und somit wegen $\ker(f) \subseteq U$ auch

$$x = (xa^{-1})a \in U. \qquad \square$$

Bemerkung 2.28. Der Gruppenhomomorphismus $f : G \to H$ bildet G nach H wie im Diagramm

$$\begin{array}{ccccccc} \{e\} & \subseteq & \ker(f) & \subseteq & G & & \\ & & \vdots & & \vdots & \searrow^{f} & \\ & & \{e\} & \subseteq & \mathrm{im}(f) & \subseteq & H \end{array}$$

ab. Dabei zeigt Proposition 2.26, daß bezüglich Untergruppen zwischen $\ker(f)$ und G das „gleiche“ passiert, wie zwischen $\{e\}$ und $\mathrm{im}(f)$.

2.5. **Zyklische Gruppen.** Die arithmetisch einfachsten Gruppen sind die zyklischen Gruppen.

Definition 2.29. Eine **zyklische Gruppe** ist eine Gruppe G, für die es ein Element $g \in G$ gibt mit

$$G = \langle g \rangle.$$

Man sagt, g ist ein **Erzeuger** und G wird von g erzeugt.

Beispiel 2.30. Die wichtigsten Beispiele von Erzeugern in Gruppen sind die folgenden.

(1) Die Gruppe $\mathbb{Z}$ wird von $1 \in \mathbb{Z}$ erzeugt und ist somit zyklisch. Auch $-1 \in \mathbb{Z}$ ist ein Erzeuger, und es gibt keinen weiteren Erzeuger für $\mathbb{Z}$.

(2) Sei n eine natürliche Zahl. Dann ist die Restklasse von 1 in $\mathbb{Z}/n\mathbb{Z}$ ein Erzeuger. Zum Beispiel überlege man sich, daß 1 ein Erzeuger von $\mathbb{Z}$ ist, und wegen des surjektiven Gruppenhomomorphismus $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ auch das Bild ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$. Damit ist

$$\mathbb{Z}/n\mathbb{Z}$$

eine zyklische Gruppe, und zwar der Ordnung n.

(3) Verschiedene Elemente einer Gruppe können diese erzeugen. Zum Beispiel wird $\mathbb{Z}/3\mathbb{Z}$ sowohl von der Restklasse [1] als auch von [2] erzeugt.

(4) In der Gruppe $G = \mathbb{R}_{>0}$ der positiven reellen Zahlen mit der Multiplikation als Verknüpfung ist für jedes feste $a \neq 1$ jedes $x \in G$ von der Form $x = a^t$ für ein geeignetes t. Trotzdem ist $\mathbb{R}_{>0}$ nicht zyklisch, denn wir benötigen $t = \log(x)/\log(a)$ und das ist in der Regel nur in $\mathbb{R}$ und nicht in $\mathbb{Z}$. Die Untergruppe $\langle a \rangle$ enthält nur die ganzzahligen Potenzen a^n mit $n \in \mathbb{Z}$. Also ist $\langle a \rangle \neq \mathbb{R}_{>0}$.

Satz 2.31 (Struktursatz für zyklische Gruppen)**.** *Sei G eine zyklische Gruppe. Wenn G unendliche Ordnung hat, dann ist*

$$G \simeq \mathbb{Z},$$

und wenn G die endliche Ordnung n hat, dann ist

$$G \simeq \mathbb{Z}/n\mathbb{Z}.$$

Beweis. Dies folgt sofort aus Satz 2.32, denn in der Notation des Beweises ist $\langle g\rangle = G$, wenn wir für g einen Erzeuger von G wählen. Einen Erzeuger gibt es, weil G als zyklische Gruppe vorausgesetzt wird. □

Satz 2.32 (Babyversion des Homomorphiesatzes)**.** *Sei G eine Gruppe und $g \in G$ ein Element. Der Gruppenhomomorphismus*

$$\varphi : \mathbb{Z} \to G, \qquad \varphi(a) = g^a$$

hat als Bild die Untergruppe $\langle g\rangle$ aller Potenzen von g, und es gilt:

(1) *Sei* $\operatorname{ord}(g) = n$ *endlich. Dann gilt*
  - *(a)* $\ker(\varphi) = n\mathbb{Z}$.
  - *(b)* *φ induziert einen Isomorphismus*

$$\bar\varphi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g\rangle, \qquad \bar\varphi([a]) = g^a.$$

(2) *Sei* $\operatorname{ord}(g) = \infty$ *unendlich. Dann gilt*
  - *(a)* $\ker(\varphi) = 0$, *d.h., φ ist injektiv.*
  - *(b)* *$\varphi : \mathbb{Z} \to \langle g\rangle$ ist ein Isomorphismus.*

Beweis. Proposition 2.12 beschreibt das Bild von φ und seine Ordnung.

(1) Sei $\operatorname{ord}(g) = n < \infty$. Dann ist per Definition der Ordnung $n \in \ker(\varphi) = \{m \in \mathbb{Z}\,;\, g^m = 1\}$ das kleinste positive Element. Nach dem Beweis des Struktursatzes über Untergruppen von $\mathbb{Z}$, Satz 2.20, folgt

$$\ker(\varphi) = n\mathbb{Z}.$$

Wenn $a \equiv b \pmod n$, dann gibt es ein $k \in \mathbb{Z}$ mit $a = b + kn$. Dann folgt

$$g^a = g^{b+kn} = g^b \cdot (g^n)^k = g^b \cdot 1^k = g^b.$$

Die Abbildung $[a] \mapsto g^a$ ist daher wohldefiniert. Die Homomorphieeigenschaft von $\bar\varphi$ berechnet sich wie die von φ aus Proposition 2.3. Nach Proposition 2.12 ist $\bar\varphi$ bijektiv.

(2) Sei $\operatorname{ord}(g) = \infty$. Dann gibt es in der Untergruppe $\ker(\varphi)$ kein kleinstes positives Element. Nach dem Beweis von Satz 2.20 folgt

$$\ker(\varphi) = 0\mathbb{Z} = 0.$$

Aus Proposition 2.26 schließen wir, daß φ injektiv ist. Damit ist die Einschränkung von φ auf sein Bild als Wertebereich

$$\varphi : \mathbb{Z} \to \langle g\rangle$$

ein bijektiver Gruppenhomomorphismus und damit ist alles gezeigt. □

Korollar 2.33. *Sei $g \in G$ und $m \in \mathbb{Z}$ mit $g^m = 1$. Dann ist $m = 0$, wenn $\operatorname{ord}(g) = \infty$, oder ein Vielfaches der Ordnung $\operatorname{ord}(g)$, wenn g endliche Ordnung hat.*

Beweis. Das folgt sofort aus der Beschreibung von $\ker(\varphi)$ im Beweis von Satz 2.32. □

Korollar 2.34. *Sei $g \in G$. Dann gilt*

$$g^a = g^b \quad \Longleftrightarrow \quad a \equiv b \pmod{\operatorname{ord}(g)},$$

wobei dies für $\operatorname{ord}(g) = \infty$ bedeuten soll, daß $a = b$.

Beweis. Das folgt sofort aus dem Beweis von Satz 2.32. □

Bemerkung 2.35. Satz 2.32 kann man später leichter als Anwendung des Homomorphiesatz, Satz 6.7 bekommen.

Wenn man sich in einer Gruppe nur für die Potenzen eines Elements g interessiert, dann besagt Satz 2.32, daß man so tun kann, als ob man in einer der beiden Fälle ist: $\mathbb{Z}$ mit $g = 1$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n > 0$ und $g = [1]$.

2.6. **Schnitt, Vereinigung und Erzeuger.** Untergruppen vertragen sich mit Schnitten.

Lemma 2.36. *Sei G eine Gruppe, I eine Menge und für jedes $i \in I$ eine Untergruppe $U_i \leq G$ gegeben. Dann ist der Schnitt eine Untergruppe von G:*

$$U = \bigcap_{i \in I} U_i.$$

Beweis. Wir weisen Proposition 2.19(c) nach. Für $u, v \in U$ gilt $u, v \in U_i$ für alle i. Damit nach Proposition 2.19(c) auch $uv^{-1} \in U_i$, und somit $uv^{-1} \in U$. (Hier ist wesentlich, daß das Inverse v^{-1} in allen Untergruppen U_i dasselbe Element ist, denn es stimmt mit dem Inversen aus G überein.) □

Bei der Vereinigung ist die Situation spezieller.

Lemma 2.37. *Sei G eine Gruppe, und für jedes $i \in \mathbb{N}$ eine Untergruppe $U_i \leq G$ gegeben, so daß diese eine aufsteigende Kette*

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots \subseteq U_i \subseteq U_{i+1} \subseteq \ldots$$

bilden. Dann ist die Vereinigung eine Untergruppe von G:

$$U = \bigcup_{i \in \mathbb{N}} U_i.$$

Beweis. Wir weisen Proposition 2.19(c) nach. Zuerst ist U nicht leer, denn das neutrale Element von G ist in U_i (sogar für jedes i).

Für $u, v \in U$ gibt es $i, j \in \mathbb{N}$ mit $u \in U_i$ und $v \in U_j$. Wenn $k \geq \max\{i, j\}$, dann ist $u, v \in U_k$, also $u + v \in U_k \subseteq U$ und $u^{-1} \in U_k \subseteq U$. □

Definition 2.38. Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Die **von S erzeugte Untergruppe** $\langle S \rangle \subseteq G$ ist definiert über die folgenden zwei Eigenschaften:

(i) $\langle S \rangle \subseteq G$ ist eine Untergruppe von G, die S enthält,
(ii) jede Untergruppe $U \subseteq G$ mit $S \subseteq U$, enthält auch $\langle S \rangle$.

Die Elemente von S heißen **Erzeuger** von $\langle S \rangle$.

Proposition 2.39. *Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Dann ist $\langle S \rangle$ wohldefiniert und hat die folgenden zwei Beschreibungen (mit $T = S \cup S^{-1}$):*

$$\langle S \rangle = \bigcap_{S \subseteq U,\ U \subseteq G \text{ Untergrp.}} U = \bigcup_{n \geq 0} T^n.$$

Unter T^0 verstehen wir in jedem Fall $\{1\}$, auch wenn $T = \emptyset$.

Beweis. Wir müssen zeigen, daß es eine Untergruppe $\langle S \rangle$ mit den in der Definition geforderten Eigenschaften gibt. Sei

$$H = \bigcap_{S \subseteq U,\ U \subseteq G \text{ Untergrp.}} U.$$

Der Schnitt ist nicht leer, denn mindestens $U = G$ gibt es, also ist H nach Lemma 2.36 eine Untergruppe. Offensichtlich gilt $S \subseteq H$. Es ist über jede Untergruppe U, die S enthält, zu schneiden, also gilt $H \subseteq U$. Damit erfüllt H die Forderungen für $\langle S \rangle$.

Angenommen, H und H' erfüllen die Forderungen aus Definition 2.38. Dann ist $S \subseteq H$ wegen (i), und somit folgt aus (ii) auch $H' \subseteq H$. Gleiches gilt mit vertauschten Rollen, also $H = H'$. Die Gruppe $\langle S \rangle$ ist somit eindeutig durch (i) und (ii) beschrieben.

Wir zeigen nun die zweite Beschreibung. Die Menge

$$H = \bigcup_{n \geq 0} \underbrace{T \cdot \ldots \cdot T}_{n\text{-mal}}$$

ist nicht leer (wegen der Konvention für T^0) und abgeschlossen unter der Gruppenverknüpfung

$$T^n \cdot T^m = T^{n+m}.$$

Da $T = T^{-1}$ und

$$(g_1 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_1^{-1}$$

ist H auch abgeschlossen unter Inversenbildung. Damit ist H nach Proposition 2.19 eine Untergruppe. Die Forderungen (i) und (ii) aus Definition 2.38 sind von H offensichtlich erfüllt. Aufgrund der Eindeutigkeit gilt dann auch $H = \langle S \rangle$. □

Definition 2.40. Ein **Erzeugendensystem** für eine Gruppe G ist eine Teilmenge $S \subseteq G$ mit

$$\langle S \rangle = G.$$

Kann man für G eine endliche Menge S finden mit $G = \langle S \rangle$, dann nennt man G endlich erzeugt.

Bemerkung 2.41. (1) Jede Gruppe G hat ein Erzeugendensystem, denn

$$G = \langle G \rangle.$$

Interessanter sind natürlich sparsamere Erzeugendensysteme.

(2) Für $g \in G$ haben wir bereits mit $\langle g \rangle$ die Untergruppe der Potenzen von g in G bezeichnet. Dies ist kein Konflikt, wie die zweite Beschreibung in Proposition 2.39 zeigt.

Beispiel 2.42. (1) Sei $n \in \mathbb{Z}$. Dann ist $\langle n \rangle = n\mathbb{Z}$.

(2) Wir betrachten nun die Menge $S = \{15, 21\}$ in der Gruppe $\mathbb{Z}$. Die Gruppe $\langle 15, 21 \rangle$ enthält auch

$$6 = 21 - 15$$

und daher

$$3 = 15 - 6 - 6.$$

Wegen $3 \in \langle 15, 21 \rangle$ folgt

$$3\mathbb{Z} = \langle 3 \rangle \subseteq \langle 15, 21 \rangle \subseteq 3\mathbb{Z},$$

also Gleichheit $\langle 15, 21 \rangle = 3\mathbb{Z}$. Die vorgeführte Rechnung ist nichts anderes als der euklidische Algorithmus, siehe Kapitel 11.2.

(3) Allgemeiner gibt es zu $a_1, \ldots, a_n \in \mathbb{Z}$ nach Satz 2.20 ein eindeutiges $d \geq 0$ mit

$$\langle a_1, \ldots, a_n \rangle = d\mathbb{Z}.$$

Dieses d ist der größte gemeinsame Teiler der $a_1, \ldots, a_n$, siehe Kapitel 11.1.

(4) In der Theorie der Determinante nutzt man aus, daß die Antisymmetrie bezüglich Vertauschung von Spalten zur allgemeinen Symmetrie mit Vorzeichen durch $\operatorname{sign}(\sigma)$ für beliebige Elemente $\sigma \in S_n$ der symmetrischen Gruppe führt. Das begründet man damit, daß man jede Permutation als Komposition von Zweiervertauschungen (Transpositionen) schreiben kann (man denke an den Sortieralgorithmus Bubblesort). Die Menge der Transpositionen in S_n ist ein Erzeugendensystem von S_n.

Bemerkung 2.43. Ist zu einer Gruppe G ein Erzeugendensystem $S \subseteq G$ gegeben, dann stellt sich als nächstes die Frage nach einer vollständigen Liste von **Relationen**, das ist eine ausreichende Liste von Wörtern aus $T = S \cup S^{-1}$, die in G alle zum neutralen Element verknüpfen und erklären können, wenn zwei Wörter in G zum gleichen Element komponieren.

Hier treffen wir auf das Wortproblem, das da fragt, ob ein Wort im Alphabet $T = S \cup S^{-1}$ mittels einer Liste von Relationen R als zum trivialen Element in G komponierend erkannt werden kann. Im Jahr 1952 wurde von Nowikow[7] (und unabhängig davon von Boone) bewiesen, daß das Wortproblem keine algorithmische Lösung erlaubt.

Das Verständnis von Gruppen muß also auf einem anderen Wege angestrebt werden.

Proposition 2.44. *Sei $f : G \to H$ ein Gruppenhomorphismus und $S \subseteq G$ eine Teilmenge. Dann ist*

$$f(\langle S\rangle) = \langle f(S)\rangle.$$

Beweis. Das ist trivial in der Beschreibung $\langle S\rangle = \bigcup_{n\geq 0} T^n$ mit $T = S \cup S^{-1}$:

$$f(T) = f(S) \cup f(S)^{-1}, \qquad f(T^n) = \big(f(T)\big)^n. \qquad \square$$

Übungsaufgaben zu §2

Übungsaufgabe 2.1 (Quaternionen). Sei $\mathbb{H} \subseteq \mathrm{M}_2(\mathbb{C})$ die Menge der Matrizen

$$\begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix}$$

mit $z, w \in \mathbb{C}$ beliebig. Zeigen Sie, daß $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$ eine Untergruppe von $\mathrm{GL}_2(\mathbb{C})$ ist.

Übungsaufgabe 2.2 (Quaternionengruppe). Wir betrachten die Teilmenge $\mathbb{Q}_8 \subseteq \mathbb{H}^\times$ derjenigen Quaternionen

$$\begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix}$$

mit $z = 0$ und $w \in \{\pm 1, \pm i\}$ oder $w = 0$ und $z \in \{\pm 1, \pm i\}$. Zeigen Sie, daß Q_8 eine Untergruppe aus 8 Elementen ist, die von Elementen

$$i := \begin{pmatrix} i & \\ & -i \end{pmatrix}, \quad j := \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \quad k := \begin{pmatrix} & i \\ i & \end{pmatrix}.$$

erzeugt wird, wobei

$$i^2 = j^2 = k^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$$

und

$$ij = k.$$

Bestimmen Sie die Ordnung der Elemente von Q_8.

Übungsaufgabe 2.3. Zeigen Sie: eine Gruppe in der jedes nichttriviale Element die Ordnung 2 hat, ist eine abelsche Gruppe.

Übungsaufgabe 2.4. Sei g ein Gruppenelement der Ordnung n und $m \in \mathbb{Z}$. Bestimmen Sie die Ordnung von g^m.

Übungsaufgabe 2.5. Wir betrachten das Quadrat im $\mathbb{R}^2$ mit den Ecken $\binom{\pm 1}{\pm 1}$. Bestimmen sie die Ordnung der Symmetriegruppe des Quadrats als Untergruppe von $\mathrm{GL}_2(\mathbb{R})$.

Übungsaufgabe 2.6. Sei $G = G_1 \times G_2$ das Produkt zweier Gruppen G_1 und G_2. Zeigen Sie, daß

$$Z(G) = Z(G_1) \times Z(G_2).$$

[7] Pjotr Sergejewitsch Nowikow, 1901–1975, russischer Mathematiker.

Übungsaufgabe 2.7. Sei $n \geq 1$ eine natürliche Zahl und K ein Körper. Bestimmen Sie das Zentrum von $\mathrm{GL}_n(K)$.

Übungsaufgabe 2.8. Wir definieren die Abbildung $(-)^\dagger : \mathrm{GL}_n(K) \to \mathrm{GL}_n(K)$ durch

$$A^\dagger := (A^{-1})^t.$$

Zeigen Sie, daß es sich um einen Automorphismus von $\mathrm{GL}_n(K)$ handelt und bestimmen Sie seine Ordnung als Element von $\mathrm{Aut}(\mathrm{GL}_n(K))$.

Übungsaufgabe 2.9. Sei G eine Gruppe und $[n] : G \to G$ für $n \in \mathbb{Z}$ die Abbildung

$$[n](g) = g^n$$

für alle $g \in G$. Zeigen Sie, daß $[n]$ für alle $n \in \mathbb{Z}$ ein Gruppenhomomorphismus ist genau dann, wenn G abelsch ist.

Übungsaufgabe 2.10. Unter $\mathrm{SL}_2(\mathbb{Z})$ verstehen wir die Teilmenge von $\mathrm{SL}_2(\mathbb{R})$ bestehend aus Matrizen mit Einträgen aus $\mathbb{Z}$:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;;\; \det(A) = 1,\ a, b, c, d \in \mathbb{Z} \right\}.$$

Zeigen Sie, daß $\mathrm{SL}_2(\mathbb{Z})$ eine Untergruppe ist und von den beiden Matrizen

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

erzeugt wird.

3. Gruppenoperationen

Gruppen werden am besten als **Gruppen von Symmetrie**transformationen verstanden. Dies ist die Menge der strukturerhaltenden bijektiven Selbstabbildungen einer Struktur. Der daraus abstrahierte Begriff ist derjenige der Gruppenoperation auf einer Menge.

3.1. Definition und erste Beispiele.

Definition 3.1. Eine **Gruppenoperation** (oder **Gruppenwirkung**, genauer **Linksoperationen** oder **Operation von links**) einer Gruppe G auf einer Menge X ist eine Abbildung

$$G \times X \to X$$
$$(g, x) \mapsto g.x$$

mit den folgenden Eigenschaften.

(i) Die Verknüpfung ist **assoziativ**: für alle $g, h \in G$ und $x \in X$ gilt:

$$g.(h.x) = (gh).x,$$

wobei die Klammerung die Reihenfolge der Verknüpfung festlegt.

(ii) Das neutrale Element $e \in G$ operiert wie die Identität, d.h. für alle $x \in X$ gilt:

$$e.x = x.$$

Wir nennen X eine G-**Menge**.

Es folgen einige natürliche Beispiele.

Beispiel 3.2. (1) Sei K ein Körper. Die Gruppe $\mathrm{GL}_n(K)$ operiert auf K^n vermöge Matrixmultiplikation von Matrix und Vektor.

(2) Die symmetrische Gruppe operiert auf $\{1, \ldots, n\}$ qua Definition.

(3) Die ganzen Zahlen $\mathbb{Z}$ operieren auf $\mathbb{R}$ durch Translation:

$$\mathbb{Z} \times \mathbb{R} \to \mathbb{R}$$
$$(n, x) \mapsto n + x.$$

(4) Die Gruppe S^1 operiert auf $\mathbb{C} \simeq \mathbb{R}^2$ durch Multiplikation komplexer Zahlen.
(5) Die 3-dimensionale Drehgruppe $\mathrm{SO}(3)$ operiert auf der 2-Sphäre

$$\mathrm{S}^2 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \; ; \; x_1^2 + x_2^2 + x_3^2 = 1 \right\} \subseteq \mathbb{R}^3.$$

Diese Operation wird genauer in der Vorlesung Geometrie behandelt.
(6) Man vergleiche die formale Ähnlichkeit von Definition 3.1 mit der Definition einer Gruppe. Insbesondere operiert G auf $X = G$ vermöge der Gruppenmultiplikation.

Zum besseren Verständnis, wie man über eine Gruppenoperation denken soll, beweisen wir die folgende Proposition. Deren Gehalt besagt, daß die Operation einer Gruppe G auf einer Menge X bedeutet, daß jedes $g \in G$ zu einer Symmetrie von X gehört, die homomorph von g abhängt.

Proposition 3.3. *Sei G eine Gruppe und X eine Menge.*

(1) Sei $G \times X \to X$ eine Gruppenoperation. Dann ist zu jedem $g \in G$ die Abbildung

$$\psi_g : X \to X, \qquad \psi_g(x) = g.x$$

eine Bijektion. Die Zuordnung $g \mapsto \psi_g$ ist ein Gruppenhomomorphismus $G \to \mathrm{Aut}(X)$, wobei $\mathrm{Aut}(X)$ die Gruppe der bijektiven Abbildungen $X \to X$ bezeichnet.

(2) Sei $\rho : G \to \mathrm{Aut}(X)$ ein Gruppenhomomorphismus. Durch

$$g.x := \rho(g)(x) \quad \text{für alle } g \in G \text{ und } x \in X$$

wird eine Gruppenoperation $G \times X \to X$ definiert.

Die Konstruktionen in (1) und (2) sind invers zueinander.

Beweis. (1) Die Assoziativität der Gruppenoperation besagt gerade, daß für alle $g, h \in G$ und $x \in X$ gilt

$$\psi_{gh}(x) = (gh).x = g.(h.x) = \psi_g(\psi_h(x)) = (\psi_g \circ \psi_h)(x).$$

Weil das neutrale Element $e \in G$ wie die Identität operiert, gilt für alle $x \in X$

$$\psi_e(x) = e.x = x,$$

also $\psi_e = \mathrm{id}$. Aus beiden Überlegungen folgt, daß $\psi_{g^{-1}}$ das Inverse zu ψ_g ist, und auch, daß die Zuordnung $g \mapsto \psi_g$ ein Gruppenhomomorphismus ist.

(2) Die Homomorphie von ρ zeigt für alle $g, h \in G$ und $x \in X$

$$(gh).x = \rho(gh)(x) = (\rho(g) \circ \rho(h))(x) = \rho(g)\big(\rho(h)(x)\big) = g.(h.x).$$

Aus $\rho(e) = \mathrm{id}$ folgt $e.x = \rho(e)(x) = \mathrm{id}(x) = x$ für alle $x \in X$.

Offensichtlich sind die Konstruktionen in (1) und (2) zueinander invers. □

Definition 3.4. Sei G eine Gruppe. Eine **G-äquivariante Abbildung** von G-Mengen ist eine Abbildung $f : X \to Y$ von G-Mengen X und Y, so daß für alle $x \in X$ und $g \in G$ gilt

$$f(g.x) = g.f(x).$$

Beispiel 3.5. In diesem Beispiel ist G die Gruppe $\{\pm 1\}$ und die Operation ist auf einer Gruppe X: zu $\varepsilon \in \{\pm 1\}$ und $x \in X$ (eine Gruppe!) sei

$$\varepsilon.x = x^\varepsilon.$$

Damit ist jeder Gruppenhomomorphismus $f : X \to Y$ eine $\{\pm 1\}$-äquivariante Abbildung, denn für alle $x \in X$ und $\varepsilon \in \{\pm 1\}$ gilt

$$f(x^\varepsilon) = f(x)^\varepsilon.$$

3.2. **Stabilisator und Orbit.** Die Begriffe Stabilisator und Orbit beschreiben das Verhalten eines Elements der Menge, auf der eine Gruppe operiert.

Satz–Definition 3.6. *Sei $G \times X \to X$ eine Operation der Gruppe G auf der Menge X. Der **Stabilisator** eines Elements $x \in X$ ist die Untergruppe*

$$G_x := \mathrm{Stab}_G(x) := \{g \in G \;;\; g.x = x\} \subseteq G.$$

Beweis. Wir müssen zeigen, daß G_x eine Untergruppe ist. Wegen $e.x = x$ ist $e \in G_x$ und somit G_x nicht leer. Mit $u, v \in G_x$ ist

$$(uv).x = u.(v.x) = u.x = x,$$

also auch $uv \in G_x$, und

$$u^{-1}.x = u^{-1}.(u.x) = (u^{-1}u).x = e.x = x,$$

also auch $u^{-1} \in G_x$. Wir schließen aus Proposition 2.19, daß $G_x \subseteq G$ eine Untergruppe ist. □

Beispiel 3.7. (1) Der Stabilisator von $e_1 \in K^n$ unter der Operation von $GL_n(K)$ besteht aus allen Matrizen $A \in \mathrm{GL}_n(K)$ mit $Ae_1 = e_1$, also allen Matrizen der Blockform

$$A = \begin{pmatrix} 1 & * \\ 0 & B \end{pmatrix}$$

mit $B \in \mathrm{GL}_{n-1}(K)$.

(2) Der Stabilisator $\mathrm{Stab}_{S_n}(x)$ des Elements x für die definierende Operation von S_n auf $X = \{1, \ldots, n\}$ besteht aus den Permutationen $\sigma \in S_n$ mit $\sigma(x) = x$. Ein solches σ wird eindeutig durch seine Einschränkung auf $X \setminus \{x\}$ bestimmt. Wir benutzen eine Bijektion

$$\varphi : \{1, \ldots, x-1, x+1, \ldots, n\} \xrightarrow{\sim} \{1, 2, \ldots, n-1\}$$

etwa

$$\varphi(i) = \begin{cases} i & \text{für } i < x, \\ i-1 & \text{für } i > x. \end{cases}$$

Als Übungsaufgabe überzeugen Sie sich, daß die Abbildung

$$\mathrm{Stab}_{S_n}(x) \to S_{n-1}, \qquad \sigma \mapsto \varphi \circ \sigma|_{X \setminus x} \circ \varphi^{-1}$$

wohldefiniert, ein Gruppenhomomorphismus und bijektiv, also ein Isomorphismus ist. Der Stabilisator ist isomorph zu S_{n-1}. Am einfachsten sieht man dies im Fall $x = n$: der Stabilisator von n besteht aus den Permutationen von $\{1, \ldots, n-1\}$, also S_{n-1}.

(3) Die Operation von $G = \mathrm{S}^1$ auf $\mathbb{C}$ hat für alle $z \in \mathbb{C}$ mit $z \neq 0$ trivialen Stabilisator, also $G_z = \{1\}$. Hingegen wird $z = 0$ von jedem Element von S^1 fixiert: $G_0 = \mathrm{S}^1$.

Beispiel 3.8 (Obere Dreiecksmatrizen). Sei K ein Körper und $n \in \mathbb{N}$. Wir definieren[8]

$$B_n(K) \subseteq \mathrm{GL}_n(K)$$

als die Menge der oberen Dreiecksmatrizen

$$\begin{pmatrix} * & \cdots & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & * \end{pmatrix},$$

wobei die Einträge auf der Diagonalen aus $K^\times$ und die übrigen $*$-Einträge beliebig aus K sind.

[8]Die Notation $B_n(K)$ wurde gewählt, um dem Begriff der Borel'schen Untergruppe linearer algebraischer Gruppen Genüge zu tun, dessen prominentestes Beispiel $B(K)$ ist.

Am besten verifiziert man, daß $B_n(K)$ eine Untergruppe ist, indem man die folgende Charakterisierung verwendet. Man betrachte die vollständige Fahne in K^n, also die aufsteigende Folge von K-Untervektorräumen

$$0 = W_0 \subset W_1 \subset \ldots \subset W_{n-1} \subset W_n = K^n,$$

wobei für $0 \leq i \leq n$

$$W_i = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \; ; \; x_j = 0 \text{ für alle } j > i \right\} \subseteq K^n.$$

Dann gilt für $A \in \mathrm{GL}_n(K)$ nämlich $A \in B_n(K)$ genau dann, wenn für alle $i = 0, \ldots, n$ gilt

$$AW_i = W_i.$$

Sei $\mathrm{VF}_n(K)$ die Menge der vollständigen Fahnen für K^n. Ein linearer Automorphismus von K^n transportiert eine vollständige Fahne in K^n wieder in eine vollständige Fahne (Inklusion und Dimension von Unterräumen bleiben erhalten). Klarerweise erhalten wir eine Operation

$$\mathrm{GL}_n(K) \times \mathrm{VF}_n(K) \to \mathrm{VF}_n(K)$$

von $\mathrm{GL}_n(K)$ auf der Menge der vollständigen Fahnen von K^n. Der Stabilisator der Fahne der W_i ist nichts anderes als $B_n(K)$, was damit eine Untergruppe ist.

Der Fahnensatz der linearen Algebra (über die Existenz von vollständigen Fahnen bestehend aus invarianten Unterräumen) beschreibt die Vereinigung der Stabilisatoren aller vollständigen Fahnen als Menge der Matrizen $A \in \mathrm{GL}_n(K)$ mit über K zerfallendem Minimalpolynom.

Definition 3.9. Sei $G \times X \to X$ eine Operation der Gruppe G auf der Menge X.

(1) Die **Bahn** (oder **Orbit**, oder G-**Orbit**) eines Elements $x \in X$ ist die Teilmenge

$$G.x = \{y \in X \; ; \;\; \text{es gibt } g \in G \text{ mit } y = g.x\}.$$

(2) Der **Bahnenraum** (oder **Orbitraum**, oder **Raum der Orbits**) der Gruppenoperation ist die Menge

$$G\backslash X = \{B \; ; \; B \subseteq X \text{ und es gibt ein } x \in X \text{ mit } B = G.x\}$$

von Teilmengen von X.

Beispiel 3.10. (1) Die Bahnen der S^1-Operation auf $\mathbb{C}$ durch Multiplikation sind genau die Kreise

$$\{z \in \mathbb{C} \; ; \; |z| = r\}$$

für $r \in \mathbb{R}$, $r > 0$, und der ‚degenerierte Kreis' mit $r = 0$: die Menge $\{0\}$. Der Orbitraum ist durch den Parameter r bijektiv zur Menge $\mathbb{R}_{\geq 0}$ der reellen Zahlen ≥ 0.

(2) Die Bahnen der Translation von $\mathbb{Z}$ auf $\mathbb{R}$ werden durch den Nachkommaanteil parametrisiert, etwa durch ein Element des halboffenen Intervalls $[0, 1)$.

(3) Sei K ein Körper und sei $n \in \mathbb{N}$. Die Operation von $\mathrm{GL}_n(K)$ auf K^n durch Matrixmultiplikation hat zwei Bahnen, nämlich 0 und $K^n \setminus \{0\}$.

Für jedes $A \in \mathrm{GL}_n(K)$ ist $A0 = 0$. Also besteht der Orbit des Nullvektors nur aus dem Nullvektor.

Wir berechnen nun die Bahn eines beliebigen $v \in K^n \setminus \{0\}$. Es gilt nie $Av = 0$, weil A invertierbar ist. Sei $w \in K^n \setminus \{0\}$ ein weitere beliebiger Vektor. Nach dem Basisergänzungssatz gibt es Basen

$$(v_1 = v, v_2, \ldots, v_n) \qquad (w_1 = w, w_2, \ldots, w_n)$$

von K^n. Die Lineare Abbildung $K^n \to K^n$, welche $v_i \mapsto w_i$ abbildet, wird durch Multiplikation mit einer invertierbare Matrix A beschrieben. Es gilt dann

$$Av = w,$$

somit besteht die Bahn von v aus ganz $K^n \setminus \{0\}$.

Satz 3.11. *Sei $G \times X \to X$ eine Operation der Gruppe G auf der Menge X.*

(1) Die Relation
$$x \sim y \iff \text{es gibt ein } g \in G \text{ mit } x = g.y$$
ist eine Äquivalenzrelation $\sim$ auf X.

(2) Die Äquivalenzklassen von $\sim$ sind die Orbits der Operation von G auf X.

(3) Je zwei G-Orbits in X sind entweder disjunkt oder identisch.

Beweis. (1) Wir müssen zeigen, daß $\sim$ reflexiv, symmetrisch und transitiv ist.

- reflexiv: für alle $x \in X$ gilt $e.x = x$ mit dem neutralen Element $e \in G$.
- symmetrisch: wenn $x \sim y$ für $x, y \in X$, dann gibt es $g \in G$ mit $x = g.y$. Daraus folgt
$$g^{-1}.x = g^{-1}.(g.y) = (g^{-1}g).y = e.y = y,$$
und das zeigt $y \sim x$.
- transitiv: wenn $x \sim y$ und $y \sim z$ für $x, y, z \in X$, dann gibt es $g, h \in G$ mit $x = g.y$ und $y = h.z$. Daraus folgt $x = g.y = g.(h.z) = (gh).z$, also $x \sim z$.

Aussage (2) ist trivial, und (3) ist eine allgemeine Eigenschaft von Äquivalenzklassen. □

Beispiel 3.12. Sei $n \in \mathbb{N}$ und sei K ein Körper. Die multiplikative Gruppe $K^\times = K \setminus \{0\}$ operiert durch Skalarmultiplikation auf K^{n+1}. Die Bahn von $0 \neq v \in K^{n+1}$ ist
$$\begin{aligned} K^\times.v &= \{\lambda v \ ; \ \lambda \in K^\times\} = \langle v \rangle_K \setminus \{0\} \\ &= \text{die Vektoren auf der } \textbf{Ursprungsgerade durch } v \text{ ohne } 0. \end{aligned}$$
Die Bahn von 0 besteht nur aus der 0. Die eingeschränkte Operation
$$\begin{aligned} K^\times \times (K^{n+1} \setminus \{0\}) &\to K^{n+1} \setminus \{0\} \\ (\lambda, v) &\mapsto \lambda v \end{aligned}$$
ist wohldefiniert, denn $\lambda v = 0 \iff \lambda = 0$ oder $v = 0$, und alle Stabilisatoren sind trivial. Der zugehörige Bahnenraum
$$\mathbb{P}^n(K) = K^\times \backslash (K^{n+1} \setminus \{0\})$$
wird der **projektive Raum** der Dimension n über dem Körper K genannt. Die Punkte von $\mathbb{P}^n(K)$ interpretiert man als die eindimensionalen Unterräume von K^{n+1}, die Ursprungsgeraden. Die Bahn des Vektors
$$v = \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$$
bezeichnet man mit
$$[x_0 : \ldots : x_n]$$
und nennt die x_i **homogene Koordinaten** (die nur bis auf Skalieren mit λ bestimmt sind).

Für $n = 1$ hat man die folgende Parametrisierung von $\mathbb{P}^1(K)$:
$$\begin{aligned} K \cup \{\infty\} &\xrightarrow{\sim} \mathbb{P}^1(K) \\ t \in K &\mapsto [t : 1] \\ \infty &\mapsto [1 : 0]. \end{aligned}$$

Definition 3.13. Sei $G \times X \to X$ eine Gruppenoperation auf einer Menge X, und sei $e \in G$ das neutrale Element.

(1) Die Operation heißt **transitiv**, wenn es nur eine Bahn gibt: für alle $x, y \in X$ existiert $g \in G$ mit $g.x = y$.

(2) Die Operation heißt **frei**, wenn für alle $x \in X$ der Stabilisator $G_x = \{e\}$ die triviale Gruppe ist: aus $g.x = x$ für ein $x \in X$ und $g \in G$ folgt $g = e$.
(3) Die Operation heißt **treu**, wenn für alle $g \in G$, $g \neq e$ ein $x \in X$ existiert mit $g.x \neq x$.

Bemerkung 3.14. Die Bahnen $B \subseteq X$ einer G-Operation auf der Menge X sind genau diejenigen Teilmengen, auf denen durch Einschränkung eine transitive G-Operation gegeben ist.

3.3. **Die Bahnenformel und Anwendungen.** Bahn und Stabilisator sind nicht unabhängig: wenn viele Gruppenelemente nichts tun, dann kann die Bahn nicht mehr so lang werden.

Satz 3.15 (Bahnenformel oder Orbit–Stabilisatorformel)**.** *Sei G eine Gruppe und*

$$G \times X \to X$$

eine Operation auf einer Menge X.

(1) Sei $x \in X$ ein Element. Die Gruppe G hat endliche Ordnung $|G|$ genau dann, wenn $|G_x|$ und $|G.x|$ endlich sind, und dann gilt die ***Orbit–Stabilisatorformel***

$$|G| = |G_x| \cdot |G.x|.$$

(2) Sind X und G endlich, so gilt die ***Bilanzgleichung***

$$|X| = \sum_{B \in G\backslash X} \frac{|G|}{|G_{x(B)}|},$$

wobei die Summe über die Bahnen jeweils die Wahl eines Elements $x(B) \in B$ aus der Bahn B benötigt (aber der Summand $\frac{|G|}{|G_{x(B)}|}$ davon unabhängig ist).

Beweis. (1) Die Abbildung $f : G \to X$ definiert durch

$$f(g) = g.x$$

hat per Definition als Bild die Bahn $G.x$ von x. Die Faser (Urbild) von f in y ist

$$f^{-1}(y) = \{g \in G \ ; \ g.x = y\},$$

also speziell $f^{-1}(x) = G_x$ ist der Stabilisator von x.

Zu jedem $y \in f(G) = G.x$ gibt es ein $g \in f^{-1}(y)$ und mit diesem ist die Multiplikation mit g eine bijektive Abbildung

$$\begin{aligned} g\cdot : G_x &\to f^{-1}(y) \\ h &\mapsto gh. \end{aligned}$$

- In der Tat, für $h \in G_x$ ist $(gh).x = g.(h.x) = g.x = y$, also die Abbildung wohldefiniert.
- Wenn für $h, h' \in G_x$ gilt $gh = gh'$, dann folgt aus Multiplikation mit g^{-1} von links schon $h = h'$. Dies zeigt die Injektivität.
- Zur Surjektivität nehmen wir $k \in f^{-1}(y)$ und rechnen (e ist das neutrale Element in G)

$$(g^{-1}k).x = g^{-1}.(k.x) = g^{-1}.y = g^{-1}.(g.x) = (g^{-1}g).x = e.x = x.$$

Daher ist $h = g^{-1}k \in G_x$ und $gh = g(g^{-1}k) = k$.

Die Inklusion $G_x \subseteq$G und die Surjektion $f : G \twoheadrightarrow G.x$ zeigen, daß mit $|G|$ auch $|G_x|$ und $|G.x|$ endlich sind.

Umgekehrt, wenn $|G_x|$ und $|G.x|$ endlich sind, dann ist G durch die endlich vielen $f^{-1}(y)$ mit $y \in G.x$ überdeckt, und jede dieser Mengen $f^{-1}(y)$ ist selbst endlich, da in Bijektion mit G_x. Daher ist G dann auch endlich. Genauer folgt dann

$$|G| = \sum_{y \in G.x} |f^{-1}(y)| = \sum_{y \in G.x} |G_x| = |G.x| \cdot |G_x|. \tag{3.1}$$

Für Aussage (2) zerlegen wir X nach Satz 3.11 disjunkt in Bahnen und berechnen nach (1) die Größe einer jeden Bahn:

$$|X| = \sum_{B \in G\backslash X} |B| = \sum_{B \in G\backslash X} \frac{|G|}{|G_{x(B)}|}.$$

Der Summand zu B ist von der Wahl des Elements $x(B) \in B$ unabhängig, weil der Quotient nach (1) gerade gleich $|B|$ ist. □

Korollar 3.16. *Wenn eine endliche Gruppe G auf einer Menge X operiert, dann sind die Ordnungen der Stabilisatoren und die Länge der Orbits Teiler der Gruppenordnung.*

Beweis. Das folgt sofort aus Satz 3.15. □

Anwendung 3.17. In Beispiel 3.7 (2) haben wir gesehen, daß der Stabilisator von $n \in \{1, \ldots, n\}$ unter der definierenden Permutationsoperation von S_n natürlich mit S_{n-1} zu identifizieren ist. Die Operation hat nur eine Bahn der Länge n. Es folgt

$$|S_n| = n \cdot |S_{n-1}|$$

und per Induktion nach n die bekannte Formel $|S_n| = n!$.

Anwendung 3.18. Sei $n \geq 1$ eine natürliche Zahl und Δ_n ein regelmäßiges n-Eck. Die **Diedergruppe** D_n ist definiert als die Automorphismengruppe von Δ_n, also derjenigen Selbstabbildungen, die Ecken auf Ecken und Kanten auf Kanten abbilden. Dies ist eine Gruppe mit Komposition von Abbildungen als Verknüpfung.

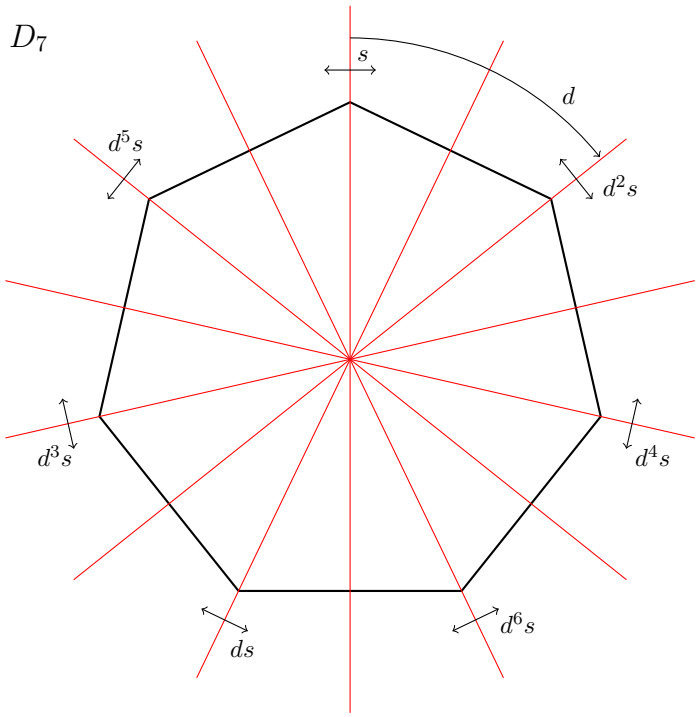


Abbildung 1. Geometrie der Diedergruppe D_7.

Die Gruppe D_n ist zusammen mit einer Operation auf Δ_n definiert. Dies induziert eine Operation auf den Ecken von Δ_n. Die Drehung um den Winkel $\frac{2\pi}{n}$ beschreibt ein Element

$$d \in D_n.$$

Durch Anwendung von Potenzen von d sehen wir, daß D_n transitiv auf der Menge der Ecken operiert. Der Stabilisator einer Ecke v (Vertex, daher v) besteht nur noch aus der Identität und der Spiegelung s an der Geraden durch den Mittelpunkt von Δ_n und der gegebenen Ecke v.

Aus der Bahnenformel folgt nun

$$|D_n| = |\text{alle Ecken}| \cdot |\text{Stabilisator einer Ecke}| = 2n.$$

Genauer kann man aus dieser Überlegung (und dem Beweis der Bahnenformel folgern), daß D_n aus den $2n$-Elementen

$$D_n = \{1, d, d^2, \ldots, d^{n-1}, s, ds, d^2s, \ldots, d^{n-1}s\}$$

besteht. Damit wird D_n von d und s erzeugt.

Bemerkung 3.19. Für die folgenden Anwendungen sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Solche gibt es, etwa für jede Primzahl p den Körper $\mathbb{F}_p$ mit p Elementen, der aus den Restklassen $\mathbb{Z}/p\mathbb{Z}$ mit der von $\mathbb{Z}$ geerbten Addition und Multiplikation besteht, vgl. Lineare Algebra 1. In der Vorlesung Algebra lernt man, daß q eine Primzahlpotenz sein muß und daß es für jede Primzahlpotenz q bis auf Isomorphie genau einen Körper mit q Elementen gibt.

Anwendung 3.20. Sei $\mathbb{F}$ ein endlicher Körper aus q Elementen. Dann hat $\mathbb{P}^n(\mathbb{F})$ die Mächtigkeit

$$|\mathbb{P}^n(\mathbb{F})| = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + q + 1.$$

In der Tat handelt es sich um den Orbitraum der Gruppe $\mathbb{F}^\times$ der Ordnung $q-1$ auf der Menge $\mathbb{F}^{n+1}\setminus\{0\}$ der Mächtigkeit $q^{n+1}-1$. Da alle Stabilisatoren trivial sind, folgt aus der Bahnenformel, daß alle Orbits die gleiche Größe $q-1$ haben und

$$|\mathbb{P}^n(\mathbb{F})| = |\,\mathbb{F}^\times \Big\backslash (\mathbb{F}^{n+1} \setminus \{0\})\,| = \frac{|\mathbb{F}^{n+1}\setminus\{0\}|}{|\mathbb{F}^\times|} = \frac{q^{n+1}-1}{q-1}.$$

Anwendung 3.21. Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Wir bestimmen die Ordnung von $\mathrm{GL}_n(\mathbb{F})$ mittels der Operation auf der Menge der vollständigen Fahnen $\mathrm{VF}_n(\mathbb{F})$. Aus der Linearen Algebra 1 wissen wir, daß jede vollständige Fahne

$$W_\bullet: \quad 0 = W_0 \subseteq W_1 \subseteq \ldots \subseteq W_n = \mathbb{F}^n$$

mittels einer Basis $(v_1, \ldots, v_n)$ von $\mathbb{F}^n$ durch

$$W_i = \langle v_1, \ldots, v_i\rangle_{\mathbb{F}}$$

beschrieben werden kann. Sei $0 = V_0 \subseteq V_1 \subseteq \ldots \subseteq V_n = \mathbb{F}^n$ mit

$$V_i = \langle e_1, \ldots, e_i\rangle_{\mathbb{F}}$$

die Standardfahne. Die Matrix

$$A = [v_1, \ldots, v_n]$$

mit den Basisvektoren v_i als Spalten ist in $\mathrm{GL}_n(\mathbb{F})$ und

$$AV_i = A\langle e_1, \ldots, e_i\rangle_{\mathbb{F}} = \langle Ae_1, \ldots, Ae_i\rangle_{\mathbb{F}} = \langle v_1, \ldots, v_i\rangle_{\mathbb{F}} = W_i.$$

Dies zeigt, daß die Operation von $\mathrm{GL}_n(\mathbb{F})$ auf $\mathrm{VF}_n(\mathbb{F})$ transitiv ist. Aus Satz 3.15 folgt

$$|\mathrm{GL}_n(\mathbb{F})| = |B_n(\mathbb{F})| \cdot |\mathrm{VF}_n(\mathbb{F})|.$$

Die Borelsche Untergruppe $B_n(\mathbb{F})$ enthält alle invertierbaren oberen Dreiecksmatrizen. Die Diagonaleinträge sind beliebig aus $\mathbb{F}^\times$ und die Einträge oberhalb der Diagonale beliebig aus $\mathbb{F}$. Daher gilt

$$|B_n(\mathbb{F})| = (q-1)^n \cdot q^{n(n-1)/2}.$$

Es bleibt, die Anzahl der vollständigen Fahnen in $\mathbb{F}^n$ zu bestimmen. Dies gelingt induktiv nach n. Der eindimensionale Raum W_1 einer Fahne $W_\bullet$ in $\mathbb{F}^n$ ist ein Punkt

$$W_1 \in \mathbb{P}^{n-1}(\mathbb{F}).$$

Jeder solche Unterraum W_1 kann genau durch die Urbilder von vollständigen Fahnen im Faktorraum $\mathbb{F}^n/W_1 \simeq \mathbb{F}^{n-1}$ zu einer vollständigen Fahne von $\mathbb{F}^n$ ergänzt werden. Daher gilt

$$|\mathrm{VF}_n(\mathbb{F})| = |\mathbb{P}^{n-1}(\mathbb{F})| \cdot |\mathrm{VF}_{n-1}(\mathbb{F})|,$$

und somit per Induktion, Anwendung 3.20 und $|\mathrm{VF}_1(\mathbb{F})| = 1$

$$|\mathrm{VF}_n(\mathbb{F})| = |\mathrm{VF}_1(\mathbb{F})| \cdot \prod_{m=1}^{n-1} |\mathbb{P}^m(\mathbb{F})| = \prod_{m=1}^{n-1} \frac{q^{m+1}-1}{q-1} = \prod_{m=1}^{n} \frac{q^m-1}{q-1}.$$

Daraus resultiert die folgende Formel für die Ordnung von $\mathrm{GL}_n(\mathbb{F})$:

$$\begin{aligned} |\mathrm{GL}_n(\mathbb{F})| &= (q-1)^n \cdot q^{n(n-1)/2} \cdot \prod_{m=1}^{n} \frac{q^m-1}{q-1} \\ &= q^{\sum_{m=1}^n (n-m)} \cdot \prod_{m=1}^{n} (q^m-1) = \prod_{m=1}^{n} q^{n-m}(q^m-1) = \prod_{m=0}^{n-1} (q^n - q^m). \end{aligned}$$

Übungsaufgaben zu §3

Übungsaufgabe 3.1. Sei G eine Gruppe und X eine Menge mit einer G-Operation auf X.

Zeigen Sie, daß die Bahnen $B \subseteq X$ genau diejenigen Teilmengen von X sind, auf denen die G-Operation zu einer transitiven G-Operation $G \times B \to B$ einschränkt.

Übungsaufgabe 3.2. Sei G eine endliche Gruppe der Ordnung $|G| = 2n$ mit $n \in \mathbb{Z}$. Zeigen Sie die folgenden Aussagen:

(1) Es gibt ein $g \in G$ verschieden von 1 mit $g^2 = 1$.
(2) Für alle $g \in G$ gibt es ein $h \neq g^{-1}$ mit $hgh = g^{-1}$.

Tipp: Verwenden Sie die Bahnenformel für die Abbildung $g \mapsto g^{-1}$, die man als Operation der Gruppe $\{\pm 1\}$ auf G verstehen kann. Formulieren Sie, was es für ein Element bedeutet, wenn sein Orbit die Länge 1 hat.

Übungsaufgabe 3.3. Bestimmen Sie die Orbits der Operation von $\mathrm{GL}_n(K)$ auf K^n durch Matrixmultiplikation.

Übungsaufgabe 3.4. Sei M eine Menge und $f : M \to M$ eine Involution, d.h. es gilt $f \circ f = \mathrm{id}_M$.

(1) Konstruieren Sie eine Gruppenoperation von $\mathbb{Z}/2\mathbb{Z}$ auf M, bei der für alle $x \in M$ gilt: $[1].x = f(x)$.
(2) Sei nun M eine endliche Menge und f habe genau einen Fixpunkt. Zeigen Sie, daß M ungerade viele Elemente hat.
(3) Gilt auch die Umkehrung von (b)? Was kann man über die Fixpunkte von f sagen, wenn $\#M$ ungerade ist?

Übungsaufgabe 3.5. Die Elemente von $\mathbb{P}^n(K)$ sind Geraden $L = Kv \subseteq K^{n+1}$ für $0 \neq v \in K^{n+1}$. Für eine Matrix $A \in \mathrm{GL}_{n+1}(K)$ ist

$$AL = \{Aw \ ; \ w \in L\}$$

ebenfalls eine Gerade in K^{n+1}. Zeigen Sie, daß

$$\begin{aligned} \mathrm{GL}_{n+1}(K) \times \mathbb{P}^n(K) &\to \mathbb{P}^n(K) \\ (A, L) &\mapsto AL \end{aligned}$$

eine Operation von $\mathrm{GL}_{n+1}(K)$ auf $\mathbb{P}^n(K)$ definiert.

Übungsaufgabe 3.6. In dieser Aufgabe analysieren wir die Operation von $G = \mathrm{GL}_2(K)$ auf $\mathbb{P}^1(K)$ aus Aufgabe 3.5.

(1) Beschreiben Sie den Stabilisator G_x eines geschickt gewählten Punktes $x \in \mathbb{P}^1(K)$.

(2) Bestimmen Sie für zwei verschiedene (geschickt gewählte) Punkte $x, y \in \mathbb{P}^1(K)$ den Stabilisator des Paares (x, y):

$$G_{x,y} = \{g \in G \ ; \ g.x = x \text{ und } g.y = y\}.$$

Zeigen Sie, daß $G_{x,y} = G_x \cap G_y$ gilt.

(3) Bestimmen Sie den Stabilisator des ungeordneten Paares $\{x, y\}$, also

$$G_{\{x,y\}} = \big\{g \in G \ ; \ \{g.x, g.y\} = \{x, y\}\big\},$$

für die in (2) gewählten Punkte x, y.

Übungsaufgabe 3.7. Sei G eine Gruppe, $G \neq 1$. Zeigen Sie, daß die Abbildung $\mathbb{Z} \times G \to G$ gegeben für $n \in \mathbb{Z}$ und $g \in G$ durch $(n, g) \mapsto g^n$ keine Gruppenoperation ist.

4. Operationen von Gruppen auf Gruppen

Bemerkung 4.1. Man kann auch analog eine **Operation von rechts** definieren als eine Abbildung

$$X \times G \to X,$$
$$(x, g) \mapsto x.g$$

mit den entsprechenden Eigenschaften. Man kann zwischen Links- und Rechtsoperationen übersetzen, indem man ein ‚Vorzeichen spendiert' siehe Aufgabe 4.1.

4.1. **Translation.** Im Folgenden verwenden wir Gruppenoperationen zum abstrakten Studium von Gruppen. Das erste gruppentheoretische Beispiel einer Operationen ist die Translationsoperation einer Untergruppe.

Definition 4.2. Sei $U \subseteq G$ eine Untergruppe.

(1) Die Untergruppe U operiert auf G von links durch **Translation (von links, oder Linkstranslation)** wie folgt:

$$U \times G \to G$$
$$(u, g) \mapsto ug.$$

Die Orbits der Translationsoperation von links werden **Nebenklassen**, oder genauer **Rechtsnebenklassen**, genannt und sind von der Form

$$Ug = \{h \in G \ ; \ \text{ es gibt ein } u \in U \text{ mit } h = ug\}.$$

(2) Die Untergruppe U operiert auf G von rechts durch **Translation** wie folgt:

$$G \times U \to G$$
$$(g, u) \mapsto gu.$$

Die Orbits der Translationsoperation von rechts werden **Nebenklassen**, oder genauer **Linksnebenklassen**, genannt und sind von der Form

$$gU = \{h \in G \ ; \ \text{ es gibt ein } u \in U \text{ mit } h = gu\}.$$

Die Eigenschaften einer Operation erfüllen die Translationsoperationen offensichtlich.

Lemma 4.3. *Die Translationsoperation einer Untergruppe ist frei.*

Beweis. Sei $u \in U$ im Stabilisator von $g \in G$ bezüglich der Operation durch Linkstranslation der Untergruppe U der Gruppe G (für die Rechtstranslation geht der Beweis analog). Dann gilt

$$ug = g,$$

und nach Multiplikation mit g^{-1} von rechts wird daraus $u = e$, das neutrale Element in G. □

Beispiel 4.4. Die Bahn des neutralen Elements $e \in G$ unter der Translation mit der Untergruppe U (von links oder rechts!) ist gerade U selbst.

Beispiel 4.5. Wir betrachten als Beispiel die Diedergruppe D_n erzeugt von einer Drehung d um $2\pi/n$ und einer Spiegelung s. Als Untergruppe nehmen wir zunächst $U = \langle d \rangle$. Dann gibt es die zwei Rechtsnebenklassen

$$\begin{aligned} U = Ue &= \{1, d, d^2, \dots, d^{n-1}\}, \\ Us &= \{s, ds, d^2s, \dots, d^{n-1}s\}. \end{aligned}$$

Man mache sich klar, daß jedes Element in Us eine Spiegelung des regelmäßigen n-Ecks ist, und damit die Ordnung 2 hat. Dazu berechnet man, daß in D_n

$$sds = d^{-1}$$

gilt. Damit ist für alle $i \geq 0$ (und dann auch für alle $i \in \mathbb{Z}$)

$$sd^i = \underbrace{(sds)\dots(sds)}_{i\text{-mal}}s = d^{-i}s = d^{n-i}s.$$

Daraus folgt

$$(sd^i)^2 = sd^i(sd^i) = sd^id^{-i}s = ss = 1.$$

Bezüglich der Untergruppe $V = \langle s \rangle$ gibt es n Rechtsnebenklassen, für jedes $0 \leq i \leq n-1$ eine:

$$Vd^i = \{d^i, sd^i\} = \{d^i, d^{n-i}s\}.$$

Wir beobachten, daß zwar

$$Us = sU,$$

aber für $i \in \mathbb{Z}$ im Allgemeinen gilt:

$$\{d^i, sd^i = d^{n-i}s\} = Vd^i \neq d^iV = \{d^i, d^is\}.$$

Satz–Definition 4.6. *Sei U eine Untergruppe von G. Dann gibt es eine Bijektion*

$$U\backslash G \xrightarrow{\sim} G/U$$

der Menge der Rechts- mit der Menge der Linksnebenklassen.

*Wenn $|G/U|$ endlich ist, dann definieren wir den **Index** $(G : U)$ von U in G als*

$$(G : U) = |U\backslash G| = |G/U|.$$

Beweis. Eine Bijektion $U\backslash G \to G/U$ ist gegeben durch $Ug \mapsto (Ug)^{-1} = g^{-1}U$ mit inverser Abbildung definiert durch $gU \mapsto (gU)^{-1} = Ug^{-1}$. □

Bemerkung 4.7. Falls G endlich ist, so folgt Satz-Definition 4.6 unmittelbar aus der Bahnenformel für die Translationsoperation von U auf G:

$$|U\backslash G| = \frac{|G|}{|U|} = |G/U|,$$

denn sowohl Links- als auch Rechtstranslation sind freie Operationen, die Bahnen also alle der Länge $|U|$.

Beispiel 4.8. (1) In der Notation von Beispiel 4.5 hat die Untergruppe $\langle d \rangle \subseteq D_n$ den Index 2 und $\langle s \rangle \subseteq D_n$ den Index n.

(2) Die alternierende Gruppe A_n der geraden Permutationen ist eine Untergruppe der symmetrischen Gruppe S_n vom Index 2. Die Bahnen σA_n für $\sigma \in S_n$ sind die Teilmengen von S_n mit konstantem Signum.

Beispiel 4.9. Sei U eine Untergruppe von G. Auf dem Raum der Linksnebenklassen von U operiert G durch Translation von links:

$$G \times G/U \to G/U$$
$$(g, xU) \mapsto gxU.$$

Nur für die Wohldefiniertheit muß man kurz überlegen: wenn $xU = yU$ für $x, y \in G$, dann ist für alle $g \in G$:

$$g.(xU) = gxU = g(xU) = g(yU) = g.(yU).$$

Diese Operation ist offensichtlich transitiv und der Stabilisator der Nebenklasse $1U = U$ ist

$$\{g \in G \ ; \ gU = U\} = U.$$

Satz 4.10. *Sei U eine Untergruppe der Gruppe G. Wenn G transitiv auf einer Menge X operiert und $U = G_x$ der Stabilisator eines Elements $x \in X$ ist, dann gibt es eine Bijektion von G-Mengen*

$$G/U \xrightarrow{\sim} X,$$

die den Bahnenraum der (Rechts-)Translationsoperation durch U mit X identifiziert. Insbesondere gilt:

$$(G : U) = |X|,$$

sofern eine der beiden Größen endlich ist.

Beweis. Wir betrachten die Abbildung $f : G/U \to X$ definiert durch

$$f(gU) = g.x$$

Die Abbildung f ist wohldefiniert: zu $g, h \in G$ mit $gU = hU$ gibt es $u \in U$ mit $g = hu$ und

$$f(hU) = h.x = h.(u.x) = (hu).x = g.x = f(gU).$$

Die Abbildung ist surjektiv, weil die Operation auf X transitiv ist. Und die Abbildung ist injektiv, weil aus $g.x = h.x$ bereits (e ist das neutrale Element in G)

$$(h^{-1}g).x = h^{-1}.(g.x) = h^{-1}.(h.x) = (h^{-1}h).x = e.x = x,$$

also $h^{-1}g \in U$ und damit (nach Multiplikation mit h) auch $g \in hU$ also $gU = hU$ folgt.

Außerdem ist f mit den G-Operationen auf beiden Seiten verträglich: für alle $g, h \in G$ gilt

$$f(g.(hU)) = f(ghU) = (gh).x = g.(h.x) = g.f(hU). \qquad \square$$

Bemerkung 4.11. Die Beweise von Satz 4.10 und der Bahnenformel aus Satz 3.15 sind sehr ähnlich. Die Abbildung $G \to X$ aus dem Beweis von Satz 3.15 ist die Komposition von $G \to G/U$, $g \mapsto gU$ mit der Abbildung $f : G/U \to X$ aus dem Beweis von Satz 4.10. Im Gegensatz zur Bahnenformel braucht man aber für Satz 4.10 nicht, daß G eine endliche Gruppe ist. Nur X und $(G : U)$ sollten endlich sein, damit ein nützlicher Anzahlvergleich besteht.

Ist darüberhinaus $|G|$ endlich, so zeigt die Bahnenformel angewandt auf die Linkstranslation von G auf G/U, daß

$$(G : U) = |G/U| = |G|/|U|.$$

Die Notation $(G : U)$ für den Index der Untergruppe $U \subseteq G$ ist suggestiv für diesen Quotienten.

Beispiel 4.12. Sei K ein Körper. Die Gruppe $\mathrm{GL}_2(K)$ operiert auf dem projektiven Raum $\mathbb{P}^1(K)$ durch **Möbiustransformationen**

$$\mathrm{GL}_2(K) \times \mathbb{P}^1(K) \to \mathbb{P}^1(K)$$
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, [x : y] \right) \mapsto [ax + by : cx + dy]$$

Klassisch schreibt man diese Operation mit einem Parameter $t = \frac{x}{y}$, der die Werte $K \cup \{\infty\}$ durchläuft ($[t:1] = [x:y]$ außer für $y = 0$ bzw. $t = \infty$, das $[1:0]$ entspricht) als

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.t = \frac{at+b}{ct+d}.$$

Dies ist wirklich eine Operation, weil

$$\begin{aligned}
\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} . \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} .[x:y] \right) &= \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} .[ax+by : cx+dy] \\
&= [\alpha(ax+by)+\beta(cx+dy) : \gamma(ax+by)+\delta(cx+dy)] \\
&= [(\alpha a+\beta c)x + (\alpha b+\beta d)y : (\gamma a+\delta c)x + (\gamma b+\delta d)y] \\
&= \begin{pmatrix} \alpha a+\beta c & \alpha b+\beta d \\ \gamma a+\delta c & \gamma b+\delta d \end{pmatrix} .[x:y] \\
&= \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) .[x:y].
\end{aligned}$$

Der Stabilisator des Punktes $[1:0]$ besteht aus allen $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit

$$[1:0] = [a:c],$$

also mit $c = 0$. Dies ist die Untergruppe der oberen Dreiecksmatrizen

$$B = \left\{ \begin{pmatrix} \lambda & x \\ 0 & \mu \end{pmatrix} \;;\; \lambda, \mu, x \in K, \lambda, \mu \neq 0 \right\}.$$

Wie in Satz 4.10 sind die Linksnebenklassen gB die Fasern der Abbildung

$$\begin{aligned}
f &: \mathrm{GL}_2(K) \to \mathbb{P}^1(K) \\
f(&\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} .[1:0] = [a:c].
\end{aligned}$$

Die Abbildung f ist surjektiv, weil jedes $\begin{pmatrix} a \\ c \end{pmatrix} \neq 0$ zu einer Basis von K^2 ergänzt werden kann und damit als erste Spalte einer Matrix aus $\mathrm{GL}_2(K)$ auftritt.

Die Linksnebenklasse gB für $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ hat demnach die Form

$$gB = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K) \;;\; \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \text{ und } \begin{pmatrix} a \\ c \end{pmatrix} K\text{-linear abhängig} \right\} \tag{4.1}$$

und besteht aus allen Elementen von $\mathrm{GL}_2(K)$, deren erste Spalte die gleiche Gerade in K^2 aufspannen. Der Raum der Linksnebenklassen entspricht also bijektiv über die von der ersten Spalte aufgespannten Gerade dem projektiven Raum $\mathbb{P}^1(K)$ der Dimension 1 über K. In homogenen Koordinaten erhalten wir eine Bijektion

$$\begin{aligned}
\mathrm{GL}_2(K)/B &\xrightarrow{\sim} \mathbb{P}^1(K) \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix} B &\mapsto [a:c]
\end{aligned}$$

Satz 4.13 (Satz von Lagrange)**.** *Sei U eine Untergruppe der Gruppe G. Dann ist G von endlicher Ordnung genau dann, wenn U von endlicher Ordnung ist und endlichen Index $(G:U)$ in G hat. In diesem Fall gilt*

$$|G| = (G:U) \cdot |U|.$$

Beweis. Dies folgt sofort aus Satz 3.15 (1) angewandt auf die Operation von G auf G/U: der Stabilisator von U ist U und der Index $(G:U)$ ist die Länge der Bahn. □

Beispiel 4.14. Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Dann hat die Gruppe der oberen Dreiecksmatrizen $B_2(\mathbb{F})$, also der Matrizen

$$\begin{pmatrix} \lambda & x \\ 0 & \mu \end{pmatrix}$$

mit $x \in \mathbb{F}$ und $\lambda, \mu \in \mathbb{F}^\times$ genau $q(q-1)^2$ Elemente. Da der Raum der Linksnebenklassen bijektiv (siehe Beispiel 4.12) ist zu $\mathbb{P}^1(\mathbb{F})$ mit $|\mathbb{P}^1(\mathbb{F})| = q+1$ Elementen (siehe Anwendung 3.20), folgt aus dem Satz von Lagrange erneut

$$|\operatorname{GL}_2(\mathbb{F})| = |B| \cdot |\mathbb{P}^1(\mathbb{F})| = q(q-1)^2 \cdot (q+1) = (q^2-1)(q^2-q).$$

Beispielsweise ist die Ordnung von $\operatorname{GL}_2(\mathbb{F}_7)$ gleich $48 \cdot 42 = 2016$.

Korollar 4.15. *Sei G eine endliche Gruppe und U eine Untergruppe. Dann ist $|U|$ ein Teiler von $|G|$.*

Beweis. Das folgt sofort aus Satz 4.13. □

Korollar 4.16. *Die Ordnung eines Elements einer endlichen Gruppe teilt die Gruppenordnung.*

Beweis. Sei G eine endliche Gruppe, $g \in G$ ein Element und $U = \langle g \rangle$. Die Behauptung folgt nun aus $\operatorname{ord}(g) = |U|$, siehe Satz 2.32, und Korollar 4.15. □

Korollar 4.17 (Kleiner Fermat, abstrakte Form)**.** *Sei G eine endliche Gruppe mit neutralem Element $e \in G$. Dann gilt*

$$g^{|G|} = e$$

für alle $g \in G$.

Beweis. Dies folgt sofort aus Korollar 4.16. □

Beispiel 4.18. Sei p eine Primzahl. Wir erinnern an den endlichen Körper $\mathbb{F}_p$ mit p Elementen, die Restklassen von ganzen Zahlen modulo p, mit Addition wie $\mathbb{Z}/p\mathbb{Z}$ und Multiplikation ebenfalls durch Multiplikation der Representanten:

$$[a] \cdot [b] = [ab].$$

Dies ist in der Tat ein Körper, weil erstens $[0] \neq [1]$ und zweitens jedes $[a] \neq 0$ invertierbar ist. Aus $[a] \cdot [x] = [a] \cdot [y]$ folgt $p \mid ax - ay = a(x-y)$. Weil p eine Primzahl ist und a nicht durch p teilbar ist, muß $x - y$ ein Vielfaches von p sein, ergo $[x] = [y]$. Damit ist die Abbildung $[x] \mapsto [a] \cdot [x]$ injektiv, damit bijektiv. Es existiert daher eine Restklasse $[x]$ mit $[a] \cdot [x] = [1]$. Dies ist das gesuchte Inverse.

Die multiplikative Gruppe des endlichen Körpers $\mathbb{F}_p$

$$\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$$

hat $p-1$ Elemente, die nicht durch p teilbaren Restklassen.

Satz 4.19 (Kleiner Fermat)**.** *Sei p eine Primzahl. Sei $a \in \mathbb{Z}$ nicht durch p teilbar. Dann gilt*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beweis. Die Behauptung besagt, daß die Ordnung von $[a]$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ ein Teiler von $p-1$ ist, siehe Korollar 2.33. Weil $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ folgt dies aus Korollar 4.17 angewandt auf $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Definition 4.20. Der **Exponent** $\exp(G)$ einer Gruppe G ist die kleinste natürliche Zahl $N \geq 1$, so daß

$$g^N = e$$

für alle $g \in G$ gilt (e ist wie üblich das neutrale Element in G), sofern so ein N existiert:

$$\exp(G) = \operatorname*{kgV}_{g \in G} \operatorname{ord}(g).$$

Bemerkung 4.21. Nach dem kleinen Fermat teilt $\exp(G)$ die Gruppenordnung $|G|$. Aber Gleichheit muß hier nicht gelten. Als Beispiel dient die S_4. Die Ordnungen von Elementen aus S_4 sind

$$1, 2, 3 \text{ oder } 4.$$

Somit gilt

$$\exp(S_4) = 12 \neq 24 = |S_4|.$$

Satz 4.22. *Sei p eine Primzahl. Jede Gruppe der Ordnung p ist zyklisch. Es gibt bis auf Isomorphie genau eine Gruppe der Ordnung p, und zwar $\mathbb{Z}/p\mathbb{Z}$.*

Beweis. Sei G eine Gruppe der Ordnung p und sei g ein Element in G, das nicht das neutrale Element ist. Insbesondere ist $\operatorname{ord}(g) > 1$. Nach Korollar 4.16 ist $\operatorname{ord}(g)$ ein Teiler von p, aber nicht 1. Da p Primzahl ist, muß $\operatorname{ord}(g) = p$ sein. Die Untergruppe

$$\langle g \rangle \subseteq G$$

hat dann $\operatorname{ord}(g) = p = |G|$-viele Elemente, also ist $G = \langle g \rangle$ und G zyklisch.

Alle zyklischen Gruppen der Ordnung p sind isomorph zu $\mathbb{Z}/p\mathbb{Z}$, siehe Satz 2.31. □

4.2. **Konjugation.** Wir lernen nun eine zweite gruppentheoretische Operation kennen.

Lemma–Definition 4.23. *Sei G eine Gruppe. Die Abbildung*

$$G \times G \to G$$
$$(g, h) \mapsto ghg^{-1}$$

*beschreibt die **Operation durch Konjugation** (oder **Konjugationsoperation**) von G auf G.*

Beweis. Das neutrale Element $e \in G$ operiert wie die Identität, denn $ehe^{-1} = h$ für alle $h \in G$. Und für $a, b \in G$ und $h \in G$ gilt Assoziativität:

$$(ab).h = (ab)h(ab)^{-1} = abhb^{-1}a^{-1} = a(bhb^{-1})a^{-1} = a.(b.h).$$ □

Definition 4.24. Sei G eine Gruppe und $g, h \in G$ Gruppenelemente. Man nennt

$$ghg^{-1}$$

das zu h (mittels g) **konjugierte Element**. Unter Gruppentheoretikern wird auch oft die Notation und Definition

$$x^g = g^{-1}xg$$

für das mittels $g \in G$ zu $x \in G$ konjugierte Elemente benutzt. Im Sinne dieses Skripts ist x^g dann das mittels g^{-1} zu x konjugierte Element.

Proposition 4.25. *Sei G eine Gruppe. Die Relation auf G definiert durch: für alle $a, b \in G$*

$$a \sim b \iff a \text{ ist konjugiert zu } b$$

ist eine Äquivalenzrelation, d.h für alle $a, b, c \in G$ gilt:

(i) *für alle a ist a konjugiert zu a,*
(ii) *wenn a konjugiert zu b ist, dann ist auch b konjugiert zu a,*
(iii) *wenn a konjugiert zu b und b konjugiert zu c sind, dann ist a konjugiert zu c.*

Beweis. Die Bahn von $g \in G$ unter der Konjugationsoperation besteht aus allen zu g konjugierten Elementen. Aus Satz 3.11 folgt, daß „konjugiert zu“ auf G eine Äquivalenzrelation ist. □

Proposition 4.26. *Die **Konjugation mit** $g \in G$ ist ein Gruppenautomorphismus*

$$\varphi_g : G \to G, \qquad \varphi_g(h) = ghg^{-1}.$$

Beweis. Für $a, b \in G$ gilt

$$\varphi_g(ab) = g(ab)g^{-1} = ga(g^{-1}g)bg^{-1} = (gag^{-1})(gbg^{-1}) = \varphi_g(a)\varphi_g(b).$$

Damit ist φ_g ein Gruppenhomomorphismus.

Mit $g, h \in G$ gilt $\varphi_g \circ \varphi_h = \varphi_{gh}$, denn für alle $a \in G$ gilt

$$\varphi_{gh}(a) = (gh)a(gh)^{-1} = g(h(a)h^{-1})g^{-1} = \varphi_g(\varphi_h(a)) = \varphi_g \circ \varphi_h(a).$$

Sei $e \in G$ das neutrale Element. Da $\varphi_e(a) = eae^{-1} = a$, also $\varphi_e = \mathrm{id}_G$, ist das Inverse zu φ_g gerade $\varphi_{g^{-1}}$. Daraus folgt, daß für alle $g \in G$ der Gruppenhomomorphismus φ_g bijektiv, also ein Automorphismus ist. □

Bemerkung 4.27. Die Rechnung in Proposition 4.26 zeigt einen Gruppenhomomorphismus

$$G \to \mathrm{Aut}(G)$$
$$g \mapsto \varphi_g = (x \mapsto gxg^{-1}).$$

Automorphismen der Form φ_g werden **innere Automorphismen** genannt.

Korollar 4.28. *Konjugierte Elemente haben die gleiche Ordnung.*

Beweis. Seien $g, h \in G$, und bezeichne $1 \in G$ das neutrale Element. Dann gilt für alle $n \in \mathbb{Z}$

$$h^n = 1 \iff \varphi_g(h^n) = \varphi_g(1) \iff \varphi_g(h)^n = 1 \iff (ghg^{-1})^n = 1.$$ □

Definition 4.29. Sei G eine Gruppe.

(1) Die Bahnen der Konjugationsoperation heißen **Konjugationsklassen** von G. Die Konjugationsklasse von $x \in G$ bezeichnen wir mit

$$C_x := \{gxg^{-1} \ ; \ g \in G\}.$$

Dies sind die Äquivalenzklassen der Äquivalenzrelation „konjugiert“ auf G.

(2) Die **Ordnung** einer Konjugationsklasse C_x ist die Ordnung $\mathrm{ord}(g)$ für jedes $g \in C_x$. Dies ist nach Korollar 4.28 wohldefiniert.

(3) Der **Zentralisator** eines Gruppenelements $x \in G$ ist der Stabilisator der Konjugationsoperation

$$Z_G(x) := \{g \in G \ ; \ gxg^{-1} = x\}.$$

Beispiel 4.30. (1) Der Zentralisator von $x \in G$ ist die Untergruppe von G bestehend aus allen Elementen $g \in G$, die mit x kommutieren, denn $gxg^{-1} = x$ ist äquivalent zu $gx = xg$. Insbesondere gilt stets

$$\langle x \rangle \subseteq Z_G(x).$$

(2) Die Mächtigkeit der Konjugationsklassse von $x \in G$ ist nach dem Bahnensatz, Satz 3.15,

$$|C_x| = (G : Z_G(x))$$

der Index des Zentralisators. Ist G eine endliche Gruppe, so folgt weiter aus dem Satz von Lagrange, Satz 4.13,

$$|G| = |Z_G(x)| \cdot |C_x|.$$

Insbesondere sind bei einer endlichen Gruppe G die $|C_x|$ für alle $x \in G$ ein Teiler der Gruppenordnung.

Die Bilanzgleichung der Bahnenformel angewandt auf die Konjugationsoperation einer Gruppe G auf sich selbst nennt man die **Klassengleichung**:

Korollar 4.31 (Klassengleichung)**.** *Sei G eine endliche Gruppe und $X \subseteq G$ ein Vertretersystem für die Konjugationsklassen der Elemente von G. Dann gilt die Gleichung*

$$|G| = \sum_{x \in X} |C_x| = \sum_{x \in X} \frac{|G|}{|Z_G(x)|}.$$

Beweis. Satz 3.15 angewandt auf die Konjugationsoperation. □

Beispiel 4.32. (1) Sei $n \geq 1$ eine natürliche Zahl. Sei D_n die Diedergruppe mit einer Drehung $d \in D_n$ um den Winkel $2\pi/n$ und einer Spiegelung $s \in D_n$. Wir bestimmen den Zentralisator von d. Es gilt $\mathrm{ord}(d) = n$, also

$$\langle d \rangle = \{1, d, d^2, \ldots, d^{n-1}\} \subseteq Z_{D_n}(d).$$

Der Zentralisator hat also Index 1 oder 2 in D_n:

$$(D_n : Z_{D_n}(d)) = |D_n|/|Z_{D_n}(d)| \leq |D_n|/|\langle d \rangle| = 2n/n = 2.$$

Dementsprechend bestehen die Konjugationsklassen aus einem oder zwei Elementen. Die Elemente von D_n haben die Form d^i oder sd^i mit $0 \leq i < n$. Wegen

$$\begin{aligned} d^i(d)d^{-i} &= d \\ (sd^i)d(sd^i)^{-1} &= s(d^i d d^{-i})s^{-1} = sds^{-1} = d^{-1} \end{aligned}$$

besteht die Konjugationsklasse von d aus

$$C_d = \{d, d^{-1}\}.$$

Dies ist 2-elementig, es sei denn $d = d^{-1}$, also $n = 1$ oder $n = 2$.

Für die Konjugationsklasse von s berechnen wir

$$dsd^{-1} = ds(sds) = ds^2ds = d^2s$$

und damit

$$d(d^j s)d^{-1} = \varphi_d(d^j s) = \varphi_d(d^j)\varphi_d(s) = d^j(d^2 s) = d^{j+2}s.$$

Konjugation mit d permutiert die Spiegelungen

$$\{s, ds, d^2s, \ldots, d^{n-1}s\}$$

zyklisch um 2 Positionen.

- Sei n ungerade. Damit sind alle $d^j s$ konjugiert (durch iteriertes Anwenden von d) und
$$|C_s| \geq n.$$
Andererseits enthält $Z_{D_n}(s)$ mindestens die zwei Elemente $1, s$, so daß die Konjugationsklasse C_s höchstens n Elemente haben kann. Folglich gilt
$$C_s = \{s, ds, d^2s, \ldots, d^{n-1}s\}$$
und $Z_{D_n}(s) = \langle s \rangle$.
- Sei $n = 2m$ gerade. Die Menge der Spiegelungen spaltet sich in zwei Konjugationsklassen auf: je nach Parität von j in $d^j s$, etwa
$$C_s = \{s, d^2s, d^4s, \ldots, d^{n-2}s\}.$$
Es gilt $|C_s| = n/2$. In diesem Fall ist die Punktspiegelung $d^m \in D_n$ ein weiteres Element im Zentralisator, der daher mit
$$Z_{D_n}(s) = \{1, s, d^m, d^m s\}$$
aus 4 Elementen besteht.
Geometrisch unterscheidet man die Konjugationsklassen von Spiegelungen wie folgt: die eine Konjugationsklasse besteht aus Spiegelungen an Achsen durch zwei Eckpunkte, die andere Konjugationsklasse besteht aus Spiegelungen an Achsen durch zwei Seitenmitten.

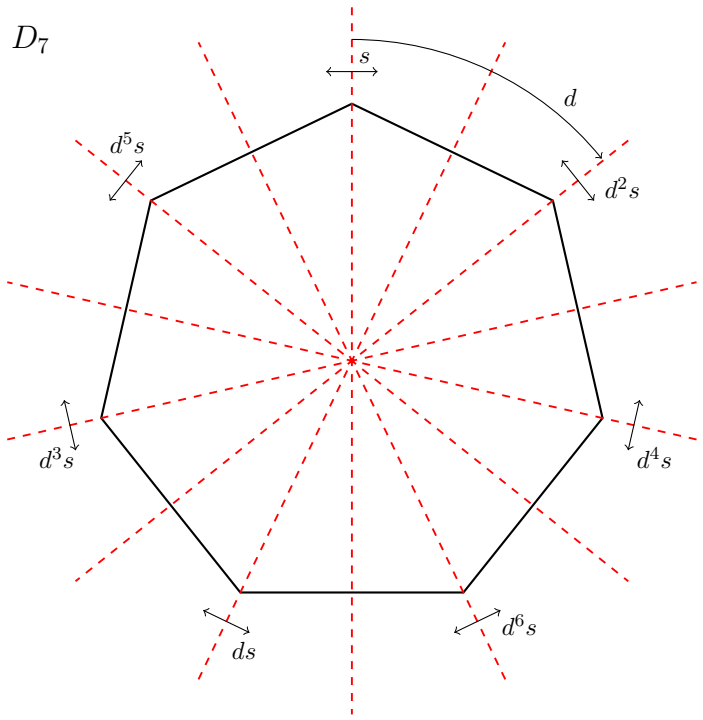


ABBILDUNG 2. Eine Konjugationsklasse von Spiegelungen in D_7.

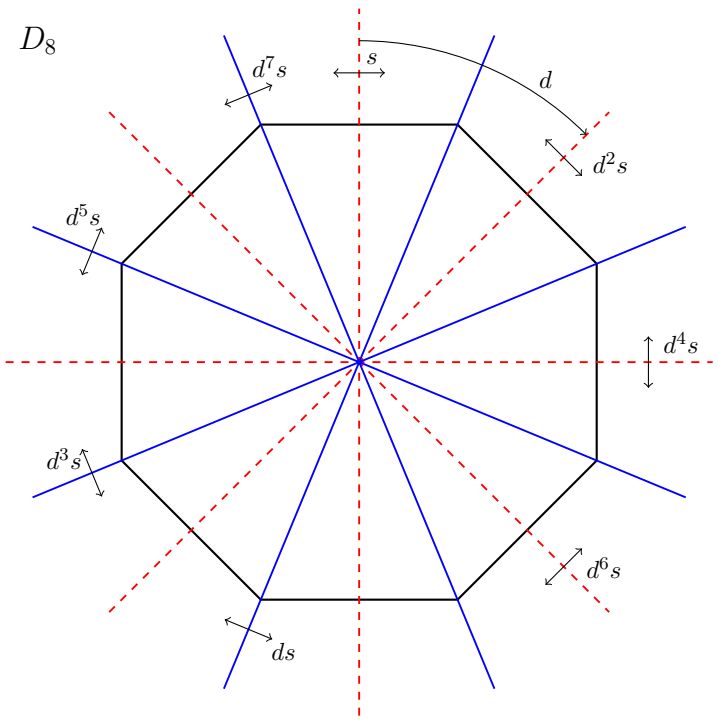


ABBILDUNG 3. Zwei Konjugationsklassen von Spiegelungen in D_8.

4.3. **Konjugation von Untergruppen.**

Definition 4.33. Konjugierte Untergruppen sind Untergruppen $U, V \subseteq G$ einer Gruppe G, so daß es ein Element $g \in G$ gibt mit $gUg^{-1} = V$.

Proposition 4.34. *Konjugierte Untergruppen sind isomorph zueinander.*

Beweis. Sind U und V konjugierte Untergruppen von G, dann gibt es $g \in G$ mit $V = gUg^{-1}$. Es gilt dann auch $U = g^{-1}Vg$. Die Einschränkung $\varphi_g|_U$ des inneren Automorphismus $\varphi_g = g(-)g^{-1}$ auf U ist ein Gruppenhomomorphismus $U \to V$, und sogar ein Isomorphismus, denn $\varphi_{g^{-1}}|_V : V \to U$ ist sein Inverses. □

Bemerkung 4.35. Eine Gruppe G operiert auf der Menge ihrer Untergruppen

$$\mathscr{U}_G = \{V \subseteq G \ ; \ \text{Untergruppe}\}$$

vermöge Konjugation:

$$G \times \mathscr{U}_G \to \mathscr{U}_G, \qquad g.V = gVg^{-1}.$$

In der Tat ist mit $g \in G$ für die Untergruppe $U \subseteq G$ die mit g konjugierte Untergruppe gerade $\varphi_g(U)$, das Bild unter einem Automorphismus, also nach Proposition 2.23 wieder eine Untergruppe. Die zu U konjugierten Untergruppen bilden die Bahn von U bezüglich dieser Operation. Damit ist 'konjugierte Untergruppe' eine Äquivalenzrelation auf der Menge der Untergruppen von G.

Definition 4.36. Sei U eine Untergruppe von G.

(1) Der Zentralisator von U in G ist die Untergruppe

$$Z_G(U) = \{g \in G \ ; \ gx = xg \text{ für alle } x \in U\}.$$

(2) Der Normalisator von U in G ist die Untergruppe

$$N_G(U) = \{g \in G \ ; \ gUg^{-1} = U\}.$$

Bemerkung 4.37. Der Zentralisator von U in G ist als Schnitt

$$Z_G(U) = \bigcap_{x \in U} Z_G(x)$$

von Untergruppen selbst eine Untergruppe. Der Normalisator von U in G ist der Stabilisator von U aufgefaßt als Element der Menge der Untergruppen $\mathscr{U}_G$ bezüglich der Operation von G durch Konjugation. Dies zeigt ohne Nachrechnen, daß der Normalisator eine Untergruppe ist.

Es gilt stets

$$Z(G) \subseteq Z_G(U) \subseteq N_G(U)$$

und $U \subseteq N_G(U)$.

Die Anzahl der zu U konjugierten Untergruppen ist nach dem Bahnensatz, Satz 3.15,

$$|\{V \ ; \ \exists g \in G : \ V = gUg^{-1}\}| = (G : N_G(U))$$

der Index des Normalisators. Ist G eine endliche Gruppe, so folgt weiter aus dem Satz von Lagrange, Satz 4.13,

$$|G| = |N_G(U)| \cdot |\{V \ ; \ \exists g \in G : \ V = gUg^{-1}\}|.$$

Konjugierte Untergruppen treten bei Gruppenoperationen in natürlicher Weise auf.

Satz 4.38. *Sei X eine Menge mit G-Operation und sei $B \subseteq X$ ein Orbit. Dann sind die Stabilisatoren G_x, G_y für $x, y \in B$ konjugiert zueinander.*

Beweis. Nach Voraussetzung gibt es ein $g \in G$ mit $g.x = y$. Dann gilt $gG_xg^{-1} = G_y$, denn

$$(gG_xg^{-1}).y = (gG_xg^{-1}).g.x = (gG_x).x = g.x = y$$

zeigt $gG_xg^{-1} \subseteq G_y$. Weiter folgt aus $g^{-1}.y = x$ wie eben $g^{-1}G_yg \subseteq G_x$. Darauf wenden wir φ_g an und erhalten die umgekehrte Inklusion $G_y \subseteq gG_xg^{-1}$. □

4.4. **Normalteiler und Faktorgruppen.** Kerne haben die bemerkenswerte Eigenschaft, als Untergruppe nur zu sich selbst konjugiert zu sein. Diese Eigenschaft bekommt einen Namen.

Definition 4.39. Ein **Normalteiler** ist eine Untergruppe N in einer Gruppe G, die nur zu sich selbst konjugiert ist: für alle $g \in G$ gilt

$$gNg^{-1} = N.$$

Notation 4.40. Eine Untergruppe $N \subseteq G$, die ein Normalteiler ist, wird auch mit $N \lhd G$ notiert.

Proposition 4.41. *Sei $N \subseteq G$ eine Untergruppe. Die folgenden Aussagen sind äquivalent:*

(a) *N ist Normalteiler: für alle $g \in G$ gilt*
$$gNg^{-1} = N.$$

(b) *Für alle $g \in G$ gilt*
$$gNg^{-1} \subseteq N.$$

(c) *Für alle $g \in G$ gilt*
$$N \subseteq gNg^{-1}.$$

(d) *Für alle $g \in G$ stimmen die von g repräsentierten Links- und Rechtsnebenklassen überein:*
$$gN = Ng.$$

Beweis. (a) $\Longrightarrow$ (b): trivial.

(b) $\Longrightarrow$ (c): Wendet man auf $g^{-1}Ng \subseteq N$, das ist (b) für g^{-1}, den inneren Automorphismus $\varphi_g(x) = gxg^{-1}$ an, so entsteht $N \subseteq gNg^{-1}$.

(c) $\Longrightarrow$ (d): Wir multiplizieren (c) für g mit g von rechts und erhalten

$$Ng \subseteq (gNg^{-1})g = gN(g^{-1}g) = gN.$$

Für die umgekehrte Inklusion nutzen wir (c) für g^{-1} und multiplizieren von links mit g:

$$gN \subseteq g\big(g^{-1}N(g^{-1})^{-1}\big) = (gg^{-1})Ng = Ng.$$

Dies zeigt (d), denn $g \in G$ war beliebig.

(d) $\Longrightarrow$ (a): aus $gN = Ng$ wird $gNg^{-1} = (gN)g^{-1} = (Ng)g^{-1} = N$. □

Proposition 4.42. *Der Kern eines Gruppenhomomorphismus ist ein Normalteiler.*

Beweis. Sei $f : G \to H$ ein Gruppenhomomorphismus, und sei $h \in N = \ker(f)$. Dann gilt für alle $g \in G$

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g)^{-1} = 1$$

und somit $ghg^{-1} \in N$. Dies zeigt $gNg^{-1} \subseteq N$. Wir schließen nun mit Proposition 4.41. □

Proposition 4.43. *Sei $U \subseteq G$ eine Untergruppe.*

(1) *U ist Normalteiler in $N_G(U)$.*

(2) *Der Normalisator $N_G(U)$ ist die bezüglich Inklusion größte Untergruppe von G, die U enthält und in der U ein Normalteiler ist.*

Beweis. (1) Daß U in $N_G(U)$ ein Normalteiler ist, folgt aus der Definition.

(2) Sei $g \in V$ in einer Untergruppe $U \subseteq V \subseteq G$ mit U Normalteiler in V. Dann ist $gUg^{-1} = U$, also $g \in N_G(U)$. Folglich ist $V \subseteq N_G(U)$. Da überdies der Normalisator selbst bereits eine Untergruppe der geforderten Art ist, folgt die Aussage. □

Beispiel 4.44. Hier sind einige Beispiele für Normalteiler und für eine Untergruppe, die kein Normalteiler ist.

(1) $\mathrm{SL}_n(K)$ ist ein Normalteiler in $\mathrm{GL}_n(K)$.
(2) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.
(3) Jede Gruppe G hat die trivialen Normalteiler G und 1.

(4) Seien K ein Körper und $B \subseteq \mathrm{GL}_2(K)$ die Untergruppe der oberen Dreiecksmatrizen. Dann ist B kein Normalteiler. Linksnebenklassen bestehen aus Matrizen deren erste Spalte die gleiche Gerade aufspannen (Beispiel 4.12), während Rechtsnebenklassen aus Matrizen bestehen, deren untere Zeile Vielfache voneinander sind.

Proposition 4.45. *Das Zentrum einer Gruppe ist ein Normalteiler und besteht genau aus den Fixpunkten der Konjugationsoperation.*

Beweis. Offenbar ist $g \in Z(G)$ genau dann, wenn für alle $h \in G$ gilt

$$ghg^{-1} = h,$$

also wenn der innere Automorphismus $\varphi_g \in \mathrm{Aut}(G)$ trivial ist. Das Zentrum $Z(G)$ ist also der Kern des Gruppenhomomorphismus $G \to \mathrm{Aut}(G)$ durch Konjugation. Daraus folgt alles. □

Proposition 4.46. *Eine Untergruppe vom Index 2 ist ein Normalteiler.*

Beweis. Sei U eine Untergruppe vom Index $(G : U) = 2$ in der Gruppe G. Wir müssen zeigen, daß Rechtsnebenklassen gU mit Linksnebenklassen Ug als Teilmengen von G übereinstimmen. Die Nebenklasse, welche das neutrale Element enthält, ist in beiden Fällen U.

Nach Voraussetzung an den Index gibt es genau eine weitere Nebenklasse. Diese ist in beiden Fällen das Komplement $G \setminus U$. □

Beispiel 4.47. Sei D_n die Diedergruppe, $d \in D_n$ eine Drehung um $2\pi/n$ und s eine Spiegelung. Dann ist $\langle d \rangle$ vom Index 2 und damit ein Normalteiler; aber für $n \geq 3$ ist die Untergruppe $\langle s \rangle$ kein Normalteiler.

Wir beschreiben nun die fundamentale Konstruktion, die nur mit einem Normalteiler und nicht mit einer beliebigen Untergruppe funktioniert.

Satz 4.48 (Faktorgruppe)**.** *Seien G eine Gruppe und $N \subseteq G$ ein Normalteiler.*

(1) Auf der Menge G/N der Nebenklassen definiert

$$G/N \times G/N \to G/N$$
$$(gN, hN) \mapsto ghN$$

eine Gruppenstruktur.

(2) Die Abbildung $p : G \to G/N$

$$p(g) = gN$$

ist ein surjektiver Gruppenhomomorphismus mit Kern $\ker(p) = N$.

Die Gruppe G/N heißt ***Faktorgruppe von G nach N***.

Beweis. (1) Die Abbildung ist wohldefiniert, denn die Verknüpfung auf G/N ist in der Tat das Produkt von Teilmengen von G:

$$(gN)(hN) = g(Nh)N = g(hN)N = ghN$$

und hängt damit nur von den Nebenklassen gN, hN und nicht von den Vertretern g, h ab.

Die Verknüpfung ist assoziativ, denn für $gN, hN, kN \in G/N$ gilt

$$(gNhN)kN = ghNkN = (gh)kN = g(hk)N = gNhkN = gN(hNkN).$$

Weiter gibt es ein neutrales Element $N \in G/N$ wegen $(gN)N = gN$ und

$$N(gN) = (Ng)N = (gN)N = gN.$$

Das inverse Element zu gN ist $g^{-1}N$, denn

$$gNg^{-1}N = (gg^{-1})N = N = (g^{-1}g)N = g^{-1}NgN.$$

(2) Für alle $g, h \in G$ gilt

$$p(gh) = ghN = (gN)(hN) = p(g)p(h),$$

so daß p ein Gruppenhomomorphismus ist. Wegen $gN = p(g)$ liegt jedes beliebige Element $gN \in G/N$ im Bild von p, und p ist surjektiv. Ein Element $g \in G$ liegt im Kern von p genau dann, wenn

$$g \in \ker(p) \iff p(g) = 1 \iff gN = N \iff g \in N. \qquad \square$$

Bemerkung 4.49. Satz 4.48 und Proposition 4.42 zeigen, daß Kerne von Gruppenhomomorphismen dasselbe sind wie Normalteiler.

Proposition 4.50. *Sei $f : G \to H$ ein Gruppenhomomorphismus.*

(1) Sei $N \subseteq H$ ein Normalteiler. Dann ist $f^{-1}(N)$ ein Normalteiler in G.
(2) Sei f surjektiv und $N \subseteq G$ ein Normalteiler. Dann ist $f(N)$ ein Normalteiler in H.

Beweis. (1) Das Urbild $f^{-1}(N)$ ist der Kern der Komposition $G \to H \to H/N$ und als Kern wieder ein Normalteiler.

(2) Wir müssen zeigen, daß $f(N)$ invariant ist unter Konjugation mit jedem $h \in H$. Da f surjektiv ist, gibt es ein $g \in G$ mit $f(g) = h$. Dann gilt

$$hf(N)h^{-1} = f(g)f(N)f(g)^{-1} = f(g)f(N)f(g^{-1}) = f(gNg^{-1}) = f(N),$$

weil N invariant ist unter Konjugation in G. $\square$

Bemerkung 4.51. Man kann in Proposition 4.50 (2) nicht auf die Annahme verzichten, daß der Gruppenhomomorphismus $f : G \to H$ surjektiv ist. Hier ist ein generisches Beispiel. Sei U eine Untergruppe in G, aber kein Normalteiler. Dann ist U ein Normalteiler von U, aber das Bild unter der Inklusion $U \hookrightarrow G$, also wieder U ist kein Normalteiler mehr. Nicht jede Untergruppe ist ein Normalteiler.

Als konkretes Beispiel betrachten wir die oberen Dreiecksmatrizen

$$B = \left\{ \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \; ; \; x \in K, a, b \in K^\times \right\}$$

und den durch die Inklusion gegebenen Gruppenhomomorphismus $i : B \hookrightarrow \mathrm{GL}_2(K)$, also

$$i(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}) = \begin{pmatrix} a & x \\ 0 & b \end{pmatrix}.$$

Weiter sei N die Untergruppe der unipotenten oberen Dreiecksmatrizen

$$N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \; ; \; x \in K \right\}.$$

Die Abbildung $\chi : B \to K^\times \times K^\times$ definiert durch

$$\chi(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}) = (a, b)$$

ist ein Gruppenhomomorphismus:

$$\chi(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix}) = \chi(\begin{pmatrix} a\alpha & a\gamma + x\beta \\ 0 & b\beta \end{pmatrix}) = (a\alpha, b\beta) = \chi(\begin{pmatrix} a & x \\ 0 & b \end{pmatrix})\chi(\begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix}).$$

Damit ist $N = \ker(\chi)$ ein Normalteiler in B. Aber $N = i(N)$ ist kein Normalteiler von $\mathrm{GL}_2(K)$, denn für $x \neq 0$ gilt

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \notin N.$$

4.5. **Das semi-direkte Produkt.** Wir verallgemeinern die Konstruktion des Produkts. Die Grundlegende Idee kann man in einer Gruppe G bezüglich einem Normalteiler N von G und einer Untergruppe $H \subseteq G$ beobachten, wenn man im Produkt hx mit $x \in N$ und $h \in H$ die Faktoren vertauschen möchte:

$$hx = h(x)h^{-1}h = yh$$

mit $y = hxh^{-1} \in N$. Um an einem Element vorbeizukommen, muß man konjugieren. Aufgrund der Normalteilereigenschaft bleibt der Faktor wenigstens im Normalteiler N. Dabei wirkt h über die Konjugation $h(-)h^{-1}$ auf dem Normalteiler N:

$$H \to \mathrm{Aut}(N), \qquad h \mapsto h(-)h^{-1}|_N.$$

Dies ist wohldefiniert, weil N ein Normalteiler ist.

Lemma–Definition 4.52. *Das* ***semi-direkte Produkt*** *einer Gruppe N mit einer Gruppe H bezüglich des Gruppenhomomorphismus $\alpha : H \to \mathrm{Aut}(N)$ ist die Gruppe $G = N \rtimes_\alpha H$ definiert als Menge durch*

$$G = N \times H$$

und mit der Verknüpfung definiert für $x, y \in N$ und $g, h \in H$ durch

$$(x, g)(y, h) := (x\alpha_g(y), gh),$$

wobei $\alpha_g(y)$ die Abkürzung für $\alpha(g)(y) \in N$ ist.

Beweis. Wr müssen zeigen, daß es in $N \rtimes_\alpha H$ ein neutrales Element gibt. Dies ist $e = (1, 1)$, denn für $x \in N$ und $h \in H$ gilt

$$(x, h)(1, 1) = (x\alpha_h(1), h) = (x, h) = (\alpha_1(x), h) = (1, 1)(x, h).$$

Weiter müssen wir zeigen, daß die Komposition ein Inverses besitzt. Für $x \in N$ und $h \in H$ ist

$$(x, h)(\alpha_{h^{-1}}(x^{-1}), h^{-1}) = (x\alpha_h(\alpha_{h^{-1}}(x^{-1})), hh^{-1}) = (x\alpha_1(x^{-1}), 1) = (xx^{-1}, 1) = (1, 1)$$

und

$$(\alpha_{h^{-1}}(x^{-1}), h^{-1})(x, h) = (\alpha_{h^{-1}}(x^{-1})\alpha_{h^{-1}}(x), h^{-1}h) = (\alpha_{h^{-1}}(x^{-1}x), 1) = (\alpha_{h^{-1}}(1), 1) = (1, 1).$$

Daher ist $(\alpha_{h^{-1}}(x^{-1}), h^{-1})$ ein Inverses zu (x, h).

Jetzt fehlt noch die Assoziativität: für $x, y, z \in N$ und $g, h, k \in H$ ist

$$\begin{aligned}\big((x, g)(y, h)\big)(z, k) &= (x\alpha_g(y), gh)(z, k) = (x\alpha_g(x)\alpha_{gh}(z), (gh)k) \\ &= (x\alpha_g(y\alpha_h(z)), g(hk)) = (x, g)(y\alpha_h(z), hk) = (x, g)\big((y, h)(z, k)\big). \qquad \square\end{aligned}$$

Notation 4.53. Wenn die Operation aus dem Kontext klar ist, wird das semi-direkte Produkt auch gerne als $N \rtimes H := N \rtimes_\alpha H$ notiert. Für die Verknüpfung bietet sich dann die Schreibweise

$$(x, g)(y, h) = (x\alpha_g(y), gh) = (x\ {}^g y, gh)$$

an, die auch ohne α auskommt: $\alpha_g(y) = {}^g y$.

Außerdem findet man auch die Notation $H \ltimes N$, wobei dann die Multiplikation als $(h, x)(g, y) = (hg, \alpha_{g^{-1}}(x)y)$ definiert werden muß.

Bemerkung 4.54. Produkte $H \times K$ sind spezielle Beispiele von semi-direkten Produkten, nämlich für den trivialen Gruppenhomomorphismus $\alpha : K \to \mathrm{Aut}(H)$, also $\alpha(k) = \mathrm{id}_H$ für alle $k \in K$.

Beispiel 4.55. Sei $n \in \mathbb{N}$. Die Gruppe $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$ operiert durch

$$\varepsilon.[a] = [\varepsilon a]$$

für alle $[a] \in \mathbb{Z}/n\mathbb{Z}$. Das semi-direkte Produkt mit dieser Operation ist isomorph zur Diedergruppe:

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Ein Isomorphismus ist gegeben durch $d \mapsto [1] \in \mathbb{Z}/n\mathbb{Z}$ und $s \mapsto -1 \in \{\pm 1\} = \mathbb{Z}/2\mathbb{Z}$.

Beispiel 4.56. Als Beispiel konstruieren wir das **Kranzprodukt** zweier Gruppen H und Γ als die Gruppe

$$G = H \wr \Gamma := (\prod_{\gamma\in\Gamma} H) \rtimes_\alpha \Gamma,$$

wobei die Operation $\alpha : \Gamma \to \mathrm{Aut}(N)$ auf $N = \prod_{\gamma\in\Gamma} H$ durch die folgende Permutation der Komponenten operiert. Für $g \in \Gamma$ und $x = (h_\gamma)_{\gamma\in\Gamma} \in N$ gilt

$$\alpha(g)(x) = (h_{\gamma g})_{\gamma\in\Gamma}.$$

In der Tat handelt es sich bei $\alpha(g) : N \to N$ um einen Automorphismus von N. Und die Zuordnung $g \mapsto \alpha_g := \alpha(g)$ is ein Gruppenhomomorphismus, denn für $g_1, g_2 \in G$ und $x = (h_\gamma)_{\gamma\in\Gamma} \in N$ gilt

$$\alpha_{g_1}\big(\alpha_{g_2}(x)\big) = \alpha_{g_1}\big((h_{\gamma g_2})_{\gamma\in\Gamma}\big) = (h_{\gamma g_1 g_2})_{\gamma\in\Gamma} = \alpha_{g_1 g_2}(x).$$

Man beachte die Reihenfolge der g_i. Es wird γ zu γg substituiert, also im zweiten Schritt γg_2 zu $(\gamma g_1)g_2$.

Beispiel 4.57. Wir definieren die Blockpermutationsgruppe zu einer disjunkten Zerlegung $\mathscr{B} = (B_1, \ldots, B_r)$

$$\{1, \ldots, n\} = B_1 \amalg \ldots \amalg B_r$$

in **Blöcke** B_i. Die Blockpermutationsgruppe ist in S_n die Untergruppe derjenigen Permutationen, welche Blöcke als ganzes in Blöcke permutieren:

$$S_{\mathscr{B}} = \{\sigma \in S_n \ ; \ \text{ es gibt } \tau \in S_r \text{ mit } \sigma(B_i) = B_{\tau(i)} \text{ für alle } 1 \le i \le r\}.$$

Wenn $n = kr$ und $|B_i| = k$ für alle $1 \le i \le r$, dann ist $S_{\mathscr{B}} = (S_k)^r \rtimes S_r$. Diese Gruppe kann man mit einer Verallgemeinerung des Kranzprodukts beschreiben.

Proposition 4.58. *Sei $G = N \rtimes_\alpha H$ ein semi-direktes Produkt bezüglich der Operation von H auf N gegeben durch $\alpha : H \to \mathrm{Aut}(N)$.*

(1) Die Projektion auf die erste Koordinate ist ein Isomorphismus

$$\{(x, 1) \ ; \ x \in N\} \xrightarrow{\sim} N.$$

Wir betrachten dadurch im Folgenden N als Untergruppe von G.

(2) Die Projektion auf die zweite Koordinate ist ein Isomorphismus

$$\{(1, h) \ ; \ h \in H\} \xrightarrow{\sim} H.$$

Wir betrachten dadurch im Folgenden H als Untergruppe von G.

(3) N ist ein Normalteiler in G.

(4) Als Untergruppen von G gilt $N \cap H = \{1\}$.

(5) Jedes $g \in G$ besitzt eine eindeutige Darstellung als $g = xh$ mit $x \in N$ und $h \in H$.

(6) Die Operation von H auf N mittels α entspricht der Konjugation in G.

Beweis. Die Aussagen (1) und (2) sind klar: für $x, y \in N$ und $h, k \in H$ gelten

$$(x, 1)(y, 1) = (x\alpha_1(y), 1) = (xy, 1) \quad \text{ und } \quad (1, h)(1, k) = (1, \alpha_h(1), hk) = (1, hk).$$

(3) Die Projektion $\mathrm{pr}_2 : G \to H$ definiert durch $\mathrm{pr}_2(x, h) = h$ für alle $(x, h) \in G$ ist ein Gruppenhomomorphismus. Als $N = \ker(\mathrm{pr}_2)$ ist N ein Normalteiler.

(4) Per Definition ist nur $(1, 1) \in N \cap H$, und das ist das neutrale Element in G.

(5) Sei $g = (x, h)$ in G beliebig. Dann ist

$$g = (x, h) = (x\alpha_1(1), h) = (x, 1)(1, h)$$

eine gesuchte Zerlegung. Wenn $g = (y, 1)(1, k)$ eine weiter solche Zerlegung ist, dann gilt

$$(x, h) = (y, 1)(1, k) = (y, k).$$

Dies zeigt die Eindeutigkeit.

(6) Wir lassen $h = (1, h) \in H \subseteq G$ auf $x = (x, 1) \in N \subseteq G$ durch Konjugation wirken:

$$\begin{aligned} hxh^{-1} &= (1,h)(x,1)(1,h)^{-1} = (1\alpha_h(x), h)(1, h^{-1}) \\ &= (\alpha_h(x)\alpha_h(1), hh^{-1}) = (\alpha_h(x), 1) = \alpha_h(x). \end{aligned}$$ □

Beispiel 4.59. Sei K ein Körper. Die Gruppe

$$\mathrm{Aff}^n(K) = \{f : K^n \to K^n \ ; \ \text{ es gibt } A \in \mathrm{GL}_n(K),\ b \in K^n \text{ mit } f(x) = Ax + b \text{ für alle } x \in K^n\}$$

der invertierbaren affin-linearen Abbildungen des K^n mit Komposition als Verknüpfung ist isomorph zum semi-direkten Produkt

$$K^n \rtimes \mathrm{GL}_n(K),$$

wobei $A \in \mathrm{GL}_n(K)$ auf $b \in K^n$ durch Matrixmultiplikation $b \mapsto Ab$ operiert. Dazu betrachten wir zu $(b, A) \in K^n \rtimes \mathrm{GL}_n(K)$ die affin-lineare Abbildung

$$f_{(b,A)}(x) = Ax + b.$$

Die Zuordnung $f : K^n \rtimes \mathrm{GL}_n(K) \to \mathrm{Aff}^n(K)$ definiert durch $(b, A) \mapsto f_{(b,A)}$ ist ein Gruppenhomomorphismus wegen

$$\begin{aligned} \big(f_{(b,A)} \circ f_{(d,C)}\big)(x) &= A(Cx + d) + b = ACx + (Ad + b) \\ &= f_{(Ad+b,AC)}(x) = f_{(b,A)(d,C)}(x) \end{aligned}$$

und außerdem klarerweise bijektiv.

Der Normalteiler K^n im semi-direkten Produkt $K^n \rtimes \mathrm{GL}_n(K)$ entspricht den Translationen $x \mapsto x + b$, und die Untergruppe $\mathrm{GL}_n(K)$ entspricht den linearen Abbildungen $K^n \to K^n$ durch Matrixmultiplikation, also den affin-linearen Abbildungen, welche den Ursprung fixieren.

Beispiel 4.60. Die Gruppe der Bewegungen des $\mathbb{R}$-Vektorraums $\mathbb{R}^n$ als euklidischem Vektorraum bezüglich des Standardskalarprodukts ist die Untergruppe von $\mathrm{Aff}^n(\mathbb{R})$ gegeben durch

$$\mathbb{R}^n \rtimes \mathrm{O}_n(\mathbb{R}).$$

Dies sind die affin-linearen Abbildungen mit orthogonalem Matrixanteil.

Übungsaufgaben zu §4

Übungsaufgabe 4.1. Sei G eine Gruppe und X eine G-Menge. Wir definieren durch

$$(x, g) \mapsto g^{-1}.x$$

eine Abbildung $X \times G \to X$. Zeigen Sie, daß dies eine Rechtsoperation von G auf X definiert, und zeigen Sie so, daß man jede Linksoperation in eine Rechtsoperation übersetzen kann (und analog umgekehrt).

Übungsaufgabe 4.2. Seien $U_i < G$ für $i = 1, \ldots, r$ Untergruppen von endlichem Index in der Gruppe G. Zeigen Sie, daß die Untergruppe $U = \bigcap_{i=1}^r U_i$ auch von endlichem Index ist, genauer

$$(G : U) \leq \prod_{i=1}^r (G : U_i).$$

Übungsaufgabe 4.3. Sei G eine Gruppe und seien $U \subseteq G$ und $V \subseteq U$ Untergruppen. Zeigen Sie die folgenden Aussagen.

(1) V ist eine Untergruppe von G.
(2) Der Index $(G : V)$ ist endlich genau dann, wenn $(G : U)$ und $(U : V)$ endlich sind, und
(3) dann gilt:
$$(G : V) = (G : U) \cdot (U : V).$$
(4) Leiten Sie für eine spezielle Wahl von V erneut den Satz von Lagrange ab.

Tipp: Zerlegen Sie G in Linksnebenklassen bezüglich der Rechtstranslation mit U bzw. mit V und beobachten Sie, wieviele der gV man braucht, um eine Nebenklasse gU zu überdecken.

Übungsaufgabe 4.4. Sei G eine Gruppe. Zeigen Sie durch konkrete Rechnung die Axiome einer Äquivalenzrelation für die Konjugationsrelation

$$a \sim b \quad \Longleftrightarrow \quad \text{es gibt ein } g \in G \text{ mit } b = gag^{-1}.$$

Übungsaufgabe 4.5. Beschreiben Sie analog zum Beispiel 4.12 die Rechtsnebenklassen

$$B \backslash \mathrm{GL}_2(K),$$

wobei B die Untergruppe der oberen Dreiecksmatrizen ist:

$$B = \left\{ \begin{pmatrix} \lambda & x \\ 0 & \mu \end{pmatrix} \; ; \; \lambda, \mu, x \in K, \lambda, \mu \neq 0 \right\}.$$

Übungsaufgabe 4.6. Beschreiben Sie ein Gegenbeispiel zu folgender Aussage: In einer endlichen Gruppe G gibt es zu jedem Teiler $n \mid |G|$ der Gruppenordnung ein Element $g \in G$ der Ordnung $\mathrm{ord}(g) = n$.

Übungsaufgabe 4.7. Seien G eine Gruppe und $U \subseteq G$ eine Untergruppe. Zeigen Sie die Behauptung aus dem Text, daß $U \subseteq N_G(U)$ und daß $N_G(U)$ die größte Untergruppe von G ist, in der U ein Normalteiler ist.

Übungsaufgabe 4.8. Sei G (bzw. H) eine Gruppe, die auf einer Menge X von links (bzw. von rechts) operiert. Die Operation von H sei frei und transitiv, und beide Operationen 'kommutieren' (sagt man, sind assoziativ wäre besser): für alle $g \in G$, $x \in X$ und $h \in H$ gilt

$$g.(x.h) = (g.x).h.$$

Nach Wahl von $y \in X$ gibt es einen eindeutigen Gruppenhomomorphismus

$$\varphi : G \to H$$

mit der Eigenschaft

$$g.y = y.(\varphi(g)).$$

Wie ändert sich φ, wenn man ein anderes Element $y \in X$ wählt?

Übungsaufgabe 4.9. Sei $\varphi : G \to \mathrm{Aut}(G)$ der Gruppenhomomorphismus mit

$$\varphi(g) = \varphi_g = (h \mapsto ghg^{-1}).$$

Zeigen Sie, daß das Bild von φ ein Normalteiler in $\mathrm{Aut}(G)$ ist.

5. Die symmetrische Gruppe

5.1. **Operationen und die symmetrische Gruppe.** Die symmetrische Gruppe ist aus der Linearen Algebra bekannt, wo sie eine Rolle bei der Theorie der Determinante spielt.

Definition 5.1. Sei $n \geq 1$ eine natürliche Zahl. Die **symmetrische Gruppe** S_n auf n Elementen ist die Gruppe der Automorphismen der Menge $\{1, \ldots, n\}$:

$$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \; ; \; \sigma \text{ ist eine Bijektion}\}.$$

Die Gruppenverknüpfung von S_n ist die Komposition von Bijektionen.

Bemerkung 5.2. Ein $\sigma \in S_n$ kann durch eine Wertetabelle

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

notiert werden. Wenn wir nur die Zeile der Werte betrachten, dann beschreiben wir σ als Permutation der Menge von n Elementen $\{1, \ldots, n\}$

$$\sigma(1), \; \sigma(2), \; \sigma(3), \; \ldots, \; \sigma(n-1), \; \sigma(n).$$

Als **Permutation** bezeichnen wir dabei eine Anordnung einer geordneten Menge, hier $1, \ldots, n$. Die Gruppe S_n wird daher auch als Gruppe der Permutationen von $1, \ldots, n$ angesprochen.

Bemerkung 5.3. Sei $G \times X \to X$ eine Gruppenoperation. Für jedes $g \in G$ definiert

$$x \mapsto g.x$$

eine Abbildung $X \to X$. Dies ist eine Permutation der Elemente von X, denn $x \mapsto g^{-1}.x$ ist die Umkehrabbildung. Mit dieser Konstruktion haben wir in Proposition 3.3 aus einer Gruppenoperation einen Gruppenhomomorphismus

$$\rho : G \to \mathrm{Aut}(X)$$

übersetzt. Im Spezialfall $X = \{x_1, \ldots, x_n\}$ einer Menge von n Elementen beschreiben wir Automorphismen von X durch die entsprechende Permutation der Indexmenge, d.h., $\rho : G \to S_n$ mit

$$g.x_i = x_{\rho(g)(i)} \tag{5.1}$$

für alle $1 \leq i \leq n$ und $g \in G$. Proposition 3.3 besagt in diesem Fall, daß die Formel (5.1) zu einer Bijektion führt:

$$\{\rho : G \to S_n \ ; \ \text{Gruppenhomomorphismus}\} \xleftrightarrow{\sim} \{\text{Operation von } G \text{ auf } \{1, \ldots, n\}\}.$$

Beispiel 5.4. Sei T die Gruppe der Symmetrien eines Tetraeders, die **volle Tetraedergruppe**. Per Definition operiert T auf der Menge der Ecken des Tetraeders. Wir beschriften die Ecken mit $1, 2, 3$ und 4. Jede Symmetrie induziert eine Permutation der Ecken. Die dadurch definierte Abbildung

$$\rho : T \to S_4$$

ist ein konkretes Beispiel für die Konstruktion aus Bemerkung 5.3, also ein Gruppenhomomorphismus. Wir zeigen, daß ρ ein Isomorphismus der Tetraedergruppe T mit S_4 ist.

Die Symmetrien des Tetraeders sind durch ihre Wirkung auf den Ecken eindeutig bestimmt: wenn $\rho(g) = \mathrm{id}$, dann ist $g = \mathrm{id}$. Damit ist $\ker(\rho) = \{\mathrm{id}\}$, und ρ ist injektiv nach Proposition 2.26.

Andererseits gibt es die folgenden Elemente: Für jedes Paar von Ecken

$$P, Q \in \{1, \ldots, 4\}$$

betrachten wir die Spiegelung $s_{P,Q}$ an der Ebene E durch die anderen beiden Ecken und den Mittelpunkt der Kante zwischen P und Q. Diese Spiegelung induziert die Transposition

$$\rho(s_{P,Q}) = (P, Q).$$

Damit enthält $\mathrm{im}(\rho)$ alle Transpositionen von S_4. Die Transpositionen erzeugen S_4, und damit ist ρ surjektiv, also sogar ein Isomorphismus.

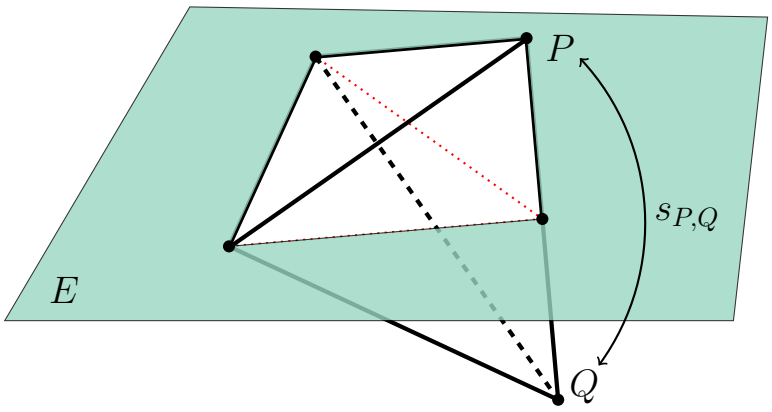


Abbildung 4. Transposition in der Tetraedergruppe.

Die Untergruppen von $\mathbb{Z}$ haben wir in Satz 2.20 mit einer übersichtlichen Antwort bestimmt. Die entsprechende Frage für S_n mit $n \in \mathbb{N}$ beliebig hat keine einfache Antwort, wie der folgende Satz von Cayley zeigt.

Satz 5.5 (Satz von Cayley)**.** *Jede Gruppe der Ordnung n ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

Beweis. Wir nummerieren die Elemente von G als $G = \{g_1, \ldots, g_n\}$. Die Translationsoperation von G auf sich selbst übersetzt Bemerkung 5.3 in einen Gruppenhomomorphismus

$$\rho : G \to S_n.$$

Wir müssen zeigen, daß ρ injektiv ist. Dann ist ρ ein Isomorphismus auf das Bild $\mathrm{im}(\rho) \subseteq S_n$.

Es gilt $g \in \ker(\rho)$ genau dann, wenn für alle $x \in G$ gilt $gx = x$. Speziell für $x = 1$ folgt $g = 1$. Nach Proposition 2.26 ist daher ρ injektiv. □

5.2. **Zykelschreibweise.** Zykel sind besonders einfache Elemente in S_n.

Definition 5.6. Ein **Zykel** in der Gruppe S_n ist eine Permutation $\sigma \in S_n$ der folgenden Form. Es gibt eine Teilmenge, die **Trägermenge** des Zykels,

$$A = \{a_1, \ldots, a_r\} \subseteq \{1, \ldots, n\}$$

mit $r \geq 2$ Elementen, so daß $\sigma(b) = b$ für alle $b \notin A$ und

$$\sigma(a_i) = a_{i+1},$$

wobei wir die Indizes modulo r betrachten. Die Zahl $r = |A|$ heißt **Länge des Zykels**, der dann auch **r-Zykel** genannt wird. Eine **Transposition** ist ein Zykel der Länge 2.

Als Notation verwenden wir

$$\sigma = (a_1, a_2, \ldots, a_r).$$

Haben mehrere Zykel disjunkte Trägermengen, so spricht man von **disjunkten Zykeln**.

Bemerkung 5.7. (1) Man beachte, daß die Elemente der Trägermenge im Zykel nicht der Größe nach geordnet sein müssen. So bildet der Zykel

$$(1, 4, 2) \in S_4$$

durch

$$1 \mapsto 4 \mapsto 2 \mapsto 1 \text{ und } 3 \mapsto 3$$

ab, während

$$(1, 2, 4) \in S_4$$

die folgende andere Abbildung darstellt:

$$1 \mapsto 2 \mapsto 4 \mapsto 1 \text{ und } 3 \mapsto 3.$$

(2) Die Notation für einen Zykel ist nicht eindeutig. Für jedes $2 \leq i \leq r$ ist

$$(a_1, a_2, \ldots, a_r) = (a_i, a_{i+1}, \ldots, a_r, a_1, \ldots, a_{i-1})$$

als Elemente der symmetrischen Gruppe. Die Reihenfolge der Elemente a_i ist wichtig! Aber bei zyklischer Vertauschung beschreiben wir dasselbe Element der S_n.

(3) Nach unserer Definition gibt es keine Zykel der Länge 1. Übertragen wir die Definition sinngemäß auf Zykel der Länge 1, so beschreibt jeder solche die Identität.

Beispiel 5.8. In der S_6 betrachten wir die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Diese bildet die Elemente $\{1, \ldots, 6\}$ wie folgt ab:

$$1 \mapsto 6 \mapsto 4 \mapsto 1, \quad 2 \mapsto 3 \mapsto 2, \quad 5 \mapsto 5,$$

was zu den Zykeln $(1, 6, 4)$ und $(2, 3)$ führt. Man verifiziert sofort

$$\sigma = (1, 6, 4)(2, 3) = (2, 3)(1, 6, 4).$$

Proposition 5.9. *Für Zykel in S_n gelten die folgenden Regeln:*

(1) $(a_1, \ldots, a_r)^{-1} = (a_r, \ldots, a_1)$.

(2) $(a_1, a_2, \ldots, a_r) = (a_1, a_r) \ldots (a_1, a_3)(a_1, a_2)$.

(3) $\operatorname{sign}((a_1, a_2, \ldots, a_r)) = (-1)^{r-1}$.

Beweis. (1) ist klar. (2) beweisen wir per vollständiger Induktion nach $r \geq 2$. Für $r = 2$ ist nichts zu tun. Nehmen wir also an, daß für $r - 1$ die Formel bereits gilt. Dann rechnet man sofort

$$(a_1, a_r) \ldots (a_1, a_3)(a_1, a_2) = (a_1, a_r)(a_1, a_2, \ldots, a_{r-1}) = (a_1, a_2, \ldots, a_r).$$

Aussage (3) folgt sofort aus (2) durch Zählen der Transpositionen. □

Proposition 5.10. *Für Zykel in S_n gelten die folgenden Regeln:*

(1) Disjunkte Zykel kommutieren miteinander.

(2) Ist $\sigma = z_1 \cdot \ldots \cdot z_s$ ein Produkt paarweise disjunkter Zykel z_i mit Trägermenge A_i, dann gilt für alle i

$$\sigma|_{A_i} = z_i|_{A_i}$$

und mit dem Komplement $B = \{1, \ldots, n\} \setminus \bigcup_{i=1}^{s} A_i$ auch

$$\sigma|_B = \mathrm{id}_B\,.$$

Beweis. (1) Das ist klar: ein Zykel macht nur etwas Nichttriviales auf seiner Trägermenge. Sind diese disjunkt, so kommutieren die entsprechenden zyklischen Permutationen. In Formeln sieht das so aus: seien $\sigma, \pi \in S_n$ disjunkte Zykel mit Trägermenge $A, B \subseteq \{1, \ldots, n\}$. Dann gilt

$$\sigma\pi(i) = \sigma\left(\begin{cases} \pi(i) & i \in B \\ i & i \notin B \end{cases}\right) = \begin{cases} \sigma(i) & i \in A \\ \pi(i) & i \in B \\ i & i \notin A \cup B \end{cases}$$

und genauso für $\pi\sigma$. Damit gilt $\sigma\pi = \pi\sigma$ wie behauptet.

(2) Weil die Trägermengen disjunkt sind, gilt für alle $i \neq j$

$$z_j|_{A_i} = \mathrm{id}_{A_i}\,.$$

Insbesondere bildet jeder der Zykel A_i auf A_i ab. Wir können daher rechnen

$$\sigma|_{A_i} = z_1|_{A_i} \cdot \ldots z_s|_{A_i} = \mathrm{id} \cdot \ldots \cdot z_i|_{A_i} \cdot \ldots \cdot \mathrm{id} = z_i|_{A_i}.$$

□

Sei $\sigma \in S_n$. Wir definieren die folgende Operation der Gruppe $\mathbb{Z}$ durch Potenzen von σ:

$$\mathbb{Z} \times \{1, \ldots, n\} \to \{1, \ldots, n\}$$
$$(m, i) \mapsto \sigma^m(i).$$

Dies ist im Prinzip die Einschränkung auf die Untergruppe $\langle\sigma\rangle \subseteq S_n$ der definierenden Operation von S_n auf $\{1, \ldots, n\}$.

Lemma 5.11. *Sei $\sigma \in S_n$. Sei $A \subseteq \{1, \ldots, n\}$ eine Bahn der Länge $r \geq 2$ für die Operation von $\mathbb{Z}$ durch Potenzen von σ. Dann gibt es einen r-Zykel*

$$(a_1, \ldots, a_r)$$

mit Trägermenge A, so daß

$$(a_1, \ldots, a_r)|_A = \sigma|_A.$$

Das bedeutet: für alle $m \in \mathbb{Z}$ (mit Indizes modulo r betrachtet)

$$\sigma^m(a_i) = a_{i+m}.$$

Beweis. Sei $a \in A$ beliebig. Der Stabilisator G_a von a ist eine Untergruppe von $G = \mathbb{Z}$, und Satz 4.10 liefert

$$(\mathbb{Z} : G_a) = |A| = r.$$

Weil wir nach Satz 2.20 alle Untergruppen von $\mathbb{Z}$ kennen, schließen wir $G_a = r\mathbb{Z}$. Satz 4.10 liefert nun genauer eine Bijektion

$$\mathbb{Z}/r\mathbb{Z} \xrightarrow{\sim} A, \qquad [i] \mapsto \sigma^i(a).$$

Wir setzen für alle $1 \leq i \leq r$

$$a_i = \sigma^i(a).$$

Die Bijektion zeigt, daß $A = \{a_1, \ldots, a_r\}$ und außerdem für alle $m \in \mathbb{Z}$

$$\sigma^m(a_i) = \sigma^m(\sigma^i(a)) = \sigma^{m+i}(a) = a_{i+m},$$

wobei wir die Indizes modulo r betrachten. □

Satz 5.12. *Jede Permutation $\sigma \in S_n$ ist ein Produkt von disjunkten Zykeln, und zwar eindeutig bis auf die Reihenfolge der Zykel.*

Beweis. Wenn $\sigma = \mathrm{id}$ das neutrale Element ist, dann ist σ der Wert des leeren Produkts[9] von Zykeln, dessen Wert per Definition das neutrale Element ist.

Sei nun $\sigma \neq \mathrm{id}$. Wir lassen $\mathbb{Z}$ durch Potenzen von σ auf $\{1, \ldots, n\}$ operieren. Dabei zerfällt diese Menge in disjunkte Orbits

$$\{1, \ldots, n\} = \bigcup_{j=1}^{s} A_j.$$

Auf jeder Bahn A_j der Länge ≥ 2 wird nach Lemma 5.11 die Wirkung von σ durch einen Zykel z_j mit Trägermenge A_j beschrieben. Auf Bahnen der Länge 1 wirkt σ als Identität, dies sind die Fixpunkte von σ. Wir setzen $z_j = \mathrm{id}$, falls $|A_j| = 1$.

Es gilt nun

$$\sigma = z_1 \cdot \ldots \cdot z_s,$$

denn nach Proposition 5.10 (2) und per Definition von z_j gilt:

$$(z_1 \cdot \ldots \cdot z_s)|_{A_j} = z_j|_{A_j} = \sigma|_{A_j}.$$

Für das Produkt von Zykeln der geforderten Form lassen wir die $z_j = \mathrm{id}$ zu Bahnen der Länge 1 weg. Dies zeigt die Existenz.

[9] Dies ist eine Konvention, die uns erspart, das neutrale Element von der Behauptung der Zerlegung in Zykel auszusparen.

Die Eindeutigkeit der Zerlegung in disjunkte Zykel bis auf die Reihenfolge der Faktoren folgt aus Proposition 5.10 (2): demnach sind nämlich die Trägermengen der Zykel die Bahnen von $\langle\sigma\rangle$ auf $\{1,\dots,n\}$. Und wenn zwei Zykel z, z' mit Trägermenge A beide $\sigma|_A$ beschreiben, dann sind sie gleich. □

Proposition 5.13. *Die Ordnung eines Zykels und eines Elements in Form eines Produkts disjunkter Zykel berechnet sich wie folgt:*

(1) Ein Zykel der Länge r hat die Ordnung r.

(2) Sei $\sigma \in S_n$ das Produkt von paarweise disjunkten Zykeln der Längen $r_1,\dots,r_m$. Dann gilt

$$\operatorname{ord}(\sigma) = \operatorname{kgV}\{r_1, r_2, \dots, r_m\}$$

Beweis. (1) Sei $\sigma = (a_1, a_2, \dots, a_r)$ ein r-Zykel. Dann folgt für alle $m \in \mathbb{Z}$

$$\sigma^m(a_i) = a_{i+m},$$

wobei der Index in $\mathbb{Z}/r\mathbb{Z}$ zu lesen ist. Daher gilt $\sigma^r = 1$ und r ist minimal in $\mathbb{N}$ mit dieser Eigenschaft.

(2) Sei $\sigma = z_1 \dots z_m$ die Zerlegung in Zykel $z_i \in S_n$ der Länge r_i mit paarweise disjunkten Trägermengen A_i. Dann kommutieren z_i und z_j für alle i, j miteinander. Per vollständiger Induktion zeigt man (vgl. Aufgabe 1.4), daß

$$\sigma^d = z_1^d \dots z_m^d.$$

Die Potenz z_i^d wirkt höchstens auf A_i nichttrivial, während $\{1,\dots,n\} \setminus A_i$ punktweise fixiert wird. Es gilt daher $\sigma^d = \mathrm{id}$ genau dann, wenn für alle $1 \le i \le m$ gilt $z_i^d = \mathrm{id}$, und damit $r_i = \operatorname{ord}(z_i) \mid d$. Daraus folgt sofort die Behauptung. □

Satz 5.14. *Die symmetrische Gruppe S_n ist durch Transpositionen erzeugt: jede Permutation ist ein Produkt von Transpositionen.*

Beweis. Nach Satz 5.12 reicht es, einen beliebigen Zykel $(a_1, a_2, \dots, a_r)$ als Produkt von Transpositionen zu erzeugen. Dafür liefert Proposition 5.9(2) eine explizite Formel. □

Satz 5.15. *Die alternierende Gruppe A_n hat die folgenden zwei Erzeugendensysteme:*

(1) die Menge der Produkte von zwei Transpositionen

$$A_n = \langle (a,b)(c,d) \ ; \ 1 \le a,b,c,d \le n, a \ne b, c \ne d \rangle,$$

(2) die Menge der 3-Zykel

$$A_n = \langle (a,b,c) \ ; \ 1 \le a,b,c \le n \text{ paarweise verschieden} \rangle.$$

Beweis. Man überlege sich zuerst, daß die angegebenen Elemente $(a,b)(c,d)$ bei $a \ne b$ und $c \ne d$, sowie (a,b,c) gerade Permutationen sind, also Elemente von A_n. Es bleibt zu zeigen, daß jedes Element von A_n sich als Produkt solcher Produkte von zwei Transpositionen (bzw. von 3-Zykeln) schreiben läßt.

(1) Für jede Transposition(a,b) gilt $\operatorname{sign}(a,b) = -1$. Nach Satz 5.14 ist jedes $\sigma \in S_n$ das Produkt von Transpositionen. Wenn σ das Produkt von r Transpositionen ist, dann gilt $\operatorname{sign}(\sigma) = (-1)^r$, also ist

$$\sigma \in A_n \iff \operatorname{sign}(\sigma) = 1 \iff r \text{ gerade.}$$

In diesem Fall kann man die Faktoren zu Paaren zusammenfassen und erhält die erste Aussage.

(2) Nach (1) reicht es, die Elemente $(a,b)(c,d)$ mit $a \ne b$ und $c \ne d$ als Produkte von 3-Zykeln zu schreiben. Wir unterscheiden die Fälle nach $N = |\{a,b,c,d\}|$.

- Fall $N = 4$: dann sind (a,b,c) und (c,a,d) 3-Zykel und

$$(a,b)(c,d) = (c,a,d)(a,b,c).$$

- Fall $N = 3$: dann ist $(a, b)(c, d)$ eine gerade Permutation in der Permutationsgruppe auf 3 Elementen. In A_3 sind aber die geraden Elemente gerade die 3-Zykel und die Identität.
- Fall $N = 2$: dann ist $\{a, b\} = \{c, d\}$ und das fragliche Element $(a, b)(c, d) = \mathrm{id}$. □

5.3. **Konjugation in der symmetrischen und der alternierenden Gruppe.** Die Konjugation von Elementen in S_n wird in der Zykelschreibweise besonders einfach.

Lemma 5.16 („Kochtopflemma“). *Seien $\sigma \in S_n$ beliebig und $\pi \in S_n$ geschrieben als Produkt disjunkter Zykel*

$$\pi = (a_{11}, \ldots, a_{1r_1}) \cdot \ldots \cdot (a_{s1}, \ldots, a_{sr_s}).$$

Dann ist als Produkt disjunkter Zykel:

$$\sigma\pi\sigma^{-1} = (\sigma(a_{11}), \ldots, \sigma(a_{1r_1})) \cdot \ldots \cdot (\sigma(a_{s1}), \ldots, \sigma(a_{sr_s})).$$

Beweis. Weil $\sigma(-)\sigma^{-1}$ ein Homomorphismus ist, gilt

$$\sigma\pi\sigma^{-1} = \Big(\sigma(a_{11}, \ldots, a_{1r_1})\sigma^{-1}\Big) \cdot \ldots \cdot \Big(\sigma(a_{s1}, \ldots, a_{sr_s})\sigma^{-1}\Big).$$

Somit reicht es, den Fall $\pi = (a_1, \ldots, a_r)$ zu betrachten, bei dem π nur aus einem Zykel besteht.

Zum einen gilt für $b \notin \{\sigma(a_1), \ldots, \sigma(a_r)\}$, daß $\sigma^{-1}(b) \notin \{a_1, \ldots, a_r\}$ und daher

$$\pi(\sigma^{-1}(b)) = \sigma^{-1}(b),$$

woraus

$$\sigma\pi\sigma^{-1}(b) = \sigma(\pi(\sigma^{-1}(b))) = \sigma(\sigma^{-1}(b)) = b$$

folgt. Weiter rechnen wir für $1 \leq i \leq r$ (mit Indizes modulo r)

$$\sigma\pi\sigma^{-1}(\sigma(a_i)) = \sigma\pi(a_i) = \sigma(a_{i+1}).$$ □

Definition 5.17. Eine **Partition** einer natürlichen Zahl $n \in \mathbb{N}$ ist eine monoton fallende Folge

$$n_1 \geq n_2 \geq \ldots n_r \geq 1$$

mit

$$n = n_1 + \ldots + n_r.$$

Beispiel 5.18. (1) Die Partitionen von 4 sind

$$4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1.$$

(2) Die Partitionen von 5 sind

$$5,\ 4+1,\ 3+2,\ 3+1+1, 2+2+1,\ 2+1+1+1,\ 1+1+1+1+1.$$

(3) Zu einem $\sigma \in S_n$ gehört die Partition von n durch die Längen der Zykel in der eindeutigen Darstellung als Produkt disjunkter Zykel und dann aufgefüllt durch 1 für die Fixpunkte von σ. Dies ist die Partition von n durch die Längen der Bahnen der Operation von $\mathbb{Z}$ durch Potenzen von σ auf $\{1, \ldots, n\}$.

Korollar 5.19. *Die Konjugationsklassen von S_n sind durch Partitionen von n parametrisiert: $\sigma, \pi \in S_n$ sind konjugiert genau dann, wenn die zugehörigen Partitionen von n übereinstimmen.*

Beweis. Das folgt sofort aus Lemma 5.16. □

Beispiel 5.20. Zu den Konjugationsklassen von S_5 haben wir die folgenden Informationen.

Partition	Beispiel σ	$\operatorname{ord}(\sigma)$	$\lvert C_\sigma\rvert$	$\lvert Z_{S_5}(\sigma)\rvert$	$Z_{S_5}(\sigma)$
5	$(1,2,3,4,5)$	5	$5!/5 = 24$	5	$\langle\sigma\rangle$
$4+1$	$(1,2,3,4)$	4	$5\cdot 4!/4 = 30$	4	$\langle\sigma\rangle$
$3+2$	$(1,2,3)(4,5)$	6	$10\cdot 3!/3 = 20$	6	$A_3\times S_2$
$3+1+1$	$(1,2,3)$	3	$10\cdot 3!/3 = 20$	6	$A_3\times S_2$
$2+2+1$	$(1,2)(3,4)$	2	$5\cdot 3 = 15$	8	$\simeq D_4$
$2+1+1+1$	$(1,2)$	2	10	12	$S_2\times S_3$
$1+1+1+1+1$	id	1	1	120	S_5

Die Klassengleichung für S_5 verifizieren wir zum Test, ob wir in der Tabelle alle Konjugationsklassen richtig berechnet haben:

$$|S_5| = 120 = 24 + 30 + 20 + 20 + 15 + 10 + 1 = \sum |C_\sigma|,$$

wobei über alle Konjugationsklassen von S_5 summiert wird.

Für die folgende Proposition benutzen wir für eine Untergruppe $H \subseteq G$ und ein $x \in H$ für die Konjugationsklassen in H bzw. G die Notation $C_x(H)$ und $C_x(G)$. Offensichtlich gilt

$$C_x(H) \subseteq C_x(G).$$

Proposition 5.21. *Sei $n \in \mathbb{N}$ und $\sigma \in A_n$. Die Konjugationsklasse $C_\sigma(S_n)$ von σ als Element von S_n zerlegt sich bezüglich A_n in*

(1) eine Konjugationsklassen, wenn $Z_{S_n}(\sigma) \not\subseteq A_n$,
(2) und in zwei Konjugationsklassen, wenn $Z_{S_n}(\sigma) \subseteq A_n$.

Im Fall der Zerlegung in zwei Konjugationsklassen haben beide die gleiche Mächtigkeit.

Beweis. Sei $\tau \in S_n \setminus A_n$. Dann gilt $S_n = A_n \cup A_n\tau$ und daher

$$C_\sigma(S_n) = C_\sigma(A_n) \cup C_{\tau\sigma\tau^{-1}}(A_n).$$

Ferner ist Konjugation mit τ wegen $\tau A_n = A_n\tau$ eine Bijektion

$$\tau(-)\tau^{-1} : C_\sigma(A_n) \xrightarrow{\sim} C_{\tau\sigma\tau^{-1}}(A_n).$$

Es geht also nur noch darum zu sehen, unter welchen Bedingungen die beiden Konjugationsklassen zusammenfallen. Weil Bahnen entweder disjunkt oder gleich sind, ist äquivalent dazu $\tau\sigma\tau^{-1} \in C_\sigma(A_n)$. Und das bedeutet: es gibt $\pi \in A_n$ mit

$$\sigma = \pi(\tau(\sigma)\tau^{-1})\pi^{-1},$$

also gibt es $\pi\tau \in Z_{S_n}(\sigma)$. Weil $\pi \in A_n$ beliebig und $\tau \in S_n \setminus A_n$ beliebig sind, bedeutet dies gerade die Existenz eines Elements in $Z_{S_n}(\sigma) \setminus A_n$. □

Beispiel 5.22. Zu den Konjugationsklassen von A_5 haben wir die folgenden Informationen. Von den Elementen aus A_5 betrachtet als Elemente von S_5 hat nur der 5-Zykel seinen Zentralisator

$Z_{S_5}(\sigma) \subseteq A_5$. Damit spaltet nur diese Konjugationsklasse in 2 auf:

Partition	Beispiel σ	ord(σ)	$\lvert C_\sigma\rvert$	$\lvert Z_{A_5}(\sigma)\rvert$	$Z_{A_5}(\sigma)$
5 Fall I	$(1,2,3,4,5)$	5	12	5	$\langle\sigma\rangle$
5 Fall II	$(1,2,3,5,4)$	5	12	5	$\langle\sigma\rangle$
$3+1+1$	$(1,2,3)$	3	20	3	A_3
$2+2+1$	$(1,2)(3,4)$	2	15	4	$\simeq V_4$
$1+1+1+1+1$	id	1	1	60	A_5

Die Klassengleichung für S_5 verifizieren wir zum Test, ob wir in der Tabelle alle Konjugationsklassen richtig berechnet haben:

$$|A_5| = 60 = 12 + 12 + 20 + 15 + 1 = \sum |C_\sigma|,$$

wobei über alle Konjugationsklassen von A_5 summiert wird.

Satz 5.23. *Die Gruppe A_5 hat keinen nichttrivialen Normalteiler.*

Beweis. Sei $N \subseteq A_5$ ein Normalteiler. Dann ist N eine Vereinigung von Konjugationsklassen und $|N|$ teilt $60 = |A_5|$. Aus der Tabelle entnimmt man, daß das nicht nichttrivial geht.

- Es ist sicher $1 \in N$ und mit einer weiteren Konjugationsklasse hat man schon $|N| \geq 13$.
- Dann bleiben als Teiler von 60 nur noch
$$|N| \in \{15, 20, 30, 60\}.$$
- Für $|N| = 15$ kommen nur die Konjugationsklasse mit 1 und die beiden mit 12 Elementen in Frage (1 muß ja dabei sein). Diese kombinieren nicht zu 15 Elementen. Bleibt $|N| = 20, 30$ oder 60.
- Nun ist $|N|$ gerade, also brauchen wir neben der Konjugationsklasse der 1 auch die einzige andere Konjugationsklasse mit einer ungeraden Anzahl. Das macht bereits 16 Elemente. Damit scheidet $|N| = 20$ aus und $|N| = 30$ kann man auch nicht kombinieren. □

Definition 5.24. Eine **einfache** Gruppe ist eine Gruppe ohne nichttriviale Normalteiler.

Satz 5.25. *Die Gruppen A_n ist einfach für $n \geq 5$.*

Beweis. Sei $1 \neq N \subseteq A_n$ ein Normalteiler. Dann gibt es $1 \neq \sigma \in N$ und für alle 3-Zykel (a,b,c) gilt

$$N \ni \sigma\big((a,b,c)\sigma^{-1}(a,b,c)^{-1}\big) = \big(\sigma(a,b,c)\sigma^{-1}\big)(c,b,a) = (\sigma(a),\sigma(b),\sigma(c))(c,b,a) =: \pi.$$

Wir wählen nun a, b, c geschickt, so daß

(i) $\pi \neq \mathrm{id}$, und
(ii) $|\{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}| \leq 5$.

Weil $\sigma \neq \mathrm{id}$, gibt es $1 \leq a \leq n$ mit $b = \sigma(a) \neq a$. Zu vermeiden ist

$$\pi = 1 \iff (\sigma(a),\sigma(b),\sigma(c)) = (a,b,c) \iff (\sigma(a),\sigma(b),\sigma(c)) = (b,c,a),$$

also $c \neq \sigma(b)$. Wir wählen daher $c \neq a, b, \sigma(b)$ beliebig (das geht wegen $n \geq 5$) und erhalten nach eventuellem Umnummerieren (das ist eine Konjugation in S_n)

$$\{a, b, c, \sigma(a), \sigma(b), \sigma(c)\} \subseteq \{1, 2, 3, 4, 5\},$$

also $1 \neq \pi \in N \cap A_5$.

Der Schnitt $N \cap A_5$ ist ein Normalteiler in A_5, also nach Satz 5.23 gilt $N \cap A_5 = A_5$, denn $N \cap A_5 = 1$ verbietet π. Dann enthält $N \cap A_5$ und damit N einen 3-Zykel.

Weil $n \geq 5$, enthält der Zentralisator eines 3-Zykles in S_n eine Transposition, nämlich eine mit zum 3-Zykel disjunkter Trägermenge. Nach Proposition 5.21 ist die Konjugationsklasse des

3-Zykels in A_n gleich der Konjugationsklasse in S_n. Nach Korollar 5.19 sind also alle 3-Zykel in A_n konjugiert. Mit einem 3-Zykel enthält N damit alle 3-Zykel.

Die 3-Zykel erzeugen A_n, Satz 5.15 (2), also ist $N = A_n$. □

Übungsaufgaben zu §5

Übungsaufgabe 5.1. Sei G eine endliche Gruppe der Ordnung n, die wir wie im Satz von Cayley als Untergruppe von S_n auffassen. Zeigen Sie, daß

$$Z_{S_n}(G) = G.$$

Übungsaufgabe 5.2. Eine Doppeltransposition ist ein Produkt zweier disjunkter Transpositionen. Zeigen Sie, daß die Doppeltranspositionen in S_n eine Konjugationsklasse sind.

Übungsaufgabe 5.3. Sei $M = \{\text{alle Doppeltranspositionen } \in S_4\}$. Zeigen Sie, daß die Menge

$$V_4 = \{1\} \cup M \subseteq S_4$$

ein Normalteiler ist (genannt: **Kleinsche Vierergruppe**).

Die Operation durch Konjugation $S_4 \times M \to M$ definiert einen Homomorphismus $S_4 \to S_3$. Bestimmen Sie Kern und Bild.

Übungsaufgabe 5.4. Sei $n \geq 1$ eine natürliche Zahl. Bestimmen Sie das Zentrum von S_n.

Übungsaufgabe 5.5. Bestimmen Sie die Anzahl der Konjugationsklassen in S_6.

Übungsaufgabe 5.6. Zeigen Sie, daß für $n \neq 6$ jeder Automorphismus von S_n ein innerer Automorphismus ist.

Tipp: Jeder 3-Zykel geht auf einen 3-Zykel.

Übungsaufgabe 5.7. Zeigen Sie, daß die Diedergruppe D_3 und die symmetrische Gruppe S_3 isomorph sind.

Tipp: finden Sie eine Operation von D_3 auf einer 3-elementigen Menge.

Übungsaufgabe 5.8. Wir lassen die Gruppe S_6 mittels Permutationsmatrizen auf $V = (\mathbb{F}_2)^6$ operieren und erhalten einen Gruppenhomomorphismus $S_6 \to \mathrm{GL}_6(\mathbb{F}_2)$. Wir setzen $v = (1, \ldots, 1)$ und definieren $v^\perp$ als Orthogonalraum bezüglich der Standardbilinearform auf V. Zeigen Sie:

(1) Es gilt
$$(0) \subset \langle v \rangle \subset v^\perp \subset V.$$
(2) Die Unterräume $\langle v \rangle$ und $v^\perp$ werden von S_6 jeweils in sich überführt.
(3) In einer geeigneten Basis unabhängig von $\sigma \in S_6$ haben die Permutationsmatrizen in $\mathrm{GL}_6(\mathbb{F}_2)$ die Blockform
$$\begin{pmatrix} 1 & * & * \\ 0 & A(\sigma) & * \\ 0 & 0 & 1 \end{pmatrix}$$
mit $A(\sigma) \in GL_4(\mathbb{F}_2)$.
(4) Die Zuordung $\rho : S_6 \to \mathrm{GL}_4(\mathbb{F}_2)$ gegeben durch $\sigma \mapsto A(\sigma)$ ist ein Gruppenhomomorphismus.

Übungsaufgabe 5.9. Zeigen Sie, daß $\mathbb{Z}/n\mathbb{Z}$ genau dann eine einfache Gruppe ist, wenn n eine Primzahl ist.

Übungsaufgabe 5.10. Sei $n \geq 5$. Zeigen Sie, daß S_n nur den einen nichttrivialen Normalteiler A_n hat.

6. Quotienten und Isomorphiesätze

In diesem Kapitel behandeln wir die Faktorgruppe beruhend auf dem Prinzip der **universellen Eigenschaft**. Dies illustriert ein wiederkehrendes Motiv in der Mathematik: ein mathematischer Gegenstand wird nicht (nur) durch seine Konstruktion, sondern durch die Eigenschaften, die er hat (bestens) beschrieben.

Konstruktion konkret, explizit	$\longleftrightarrow$	**universelle Eigenschaft** theoretisch, instrumental, konzeptionell

Beides hat seinen Wert, Vorteile und Nachteile. Mehrwert ensteht, wenn man in der Lage ist, ein Objekt von beiden Seiten zu betrachten.

6.1. **Quotienten.** Hier kommt die versprochene universelle Eigenschaft.

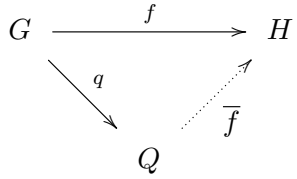
Definition 6.1. Seien G eine Gruppe und $N \subseteq G$ ein Normalteiler. Ein **Quotient** für $N \subseteq G$ ist eine Gruppe Q zusammen mit einem Homomorphismus

$$q : G \to Q,$$

genannt **Quotientenabbildung** oder genauer **Quotientenhomomorphismus**, so daß

(i) $N \subseteq \ker(q)$, und

(ii) für jeden Gruppenhomomorphismus $f : G \to H$ mit $N \subseteq \ker(f)$ gibt es einen eindeutigen Gruppenhomomorphismus $\overline{f} : Q \to H$ mit $f = \overline{f} \circ q$, d.h. das Diagramm



kommutiert, und $\overline{f}$ ist der einzige Homomorphismus $Q \to H$, für den das gilt.

Bevor wir einen Quotienten konstruieren, zeigen wir seine Eindeutigkeit! Dies illustriert, wie gut man mit den Eigenschaften umgehen kann, ohne zu wissen, ob es das Ding überhaupt gibt oder wie es konstruiert ist.

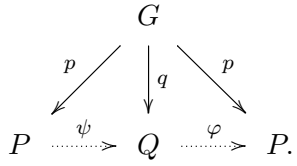
Proposition 6.2. *Seien G eine Gruppe und $N \subseteq G$ ein Normalteiler. Ein Quotient für $N \subseteq G$ ist eindeutig bis auf eindeutigen Isomorphismus.*

Das bedeutet genauer: sind $q : G \to Q$ und $p : G \to P$ Quotienten für $N \subseteq G$, dann gibt es eindeutige Isomorphismen

$$\varphi : Q \to P, \qquad \psi : P \to Q,$$

so daß $p = \varphi \circ q$ und $q = \psi \circ p$. Es sind φ und ψ zueinander invers.

Beweis. Weil $N \subseteq \ker(p)$ und $q : G \to Q$ ein Quotient ist (bzw. weil $N \subseteq \ker(q)$ und $p : G \to P$ ein Quotient ist), schließen wir aus der universellen Eigenschaft auf eindeutige Homomorphismen φ (bzw. ψ) wie im kommutativen Diagramm:



Damit erfüllt $\varphi \circ \psi$ die von der universellen Eigenschaft gestellte Anforderung im Fall $f := p$, genauso wie $\mathrm{id}_P : P \to P$. Die geforderte Eindeutigkeit erzwingt $\varphi \circ \psi = \mathrm{id}_P$. Aus Symmetrie folgt $\psi \circ \varphi = \mathrm{id}_Q$. Dies zeigt, daß φ und ψ sogar zueinander inverse Isomorphismen sind und weiter die Eindeutigkeit des Quotienten. □

Nachdem die Eindeutigkeit geklärt ist, gilt es, einen Quotienten zu konstruieren.

Satz 6.3 (Existenz des Quotienten nach einem Normalteiler)**.** *Seien G eine Gruppe und $N \subseteq G$ ein Normalteiler. Dann ist die Faktorgruppe G/N zusammen mit dem Gruppenhomomorphismus*

$$p : G \to G/N, \qquad p(g) = gN$$

ein Quotient für $N \subseteq G$.

Beweis. Es gilt $N = \ker(p)$. Es gilt somit (i) aus Definition 6.1.

Sei nun $f : G \to H$ ein Gruppenhomomorphismus mit $N \subseteq \ker(f)$. Dann ist f konstant auf Nebenklassen von N, denn

$$f(gN) = f(g)f(N) = f(g).$$

Damit ist die Abbildung

$$\begin{aligned} \bar{f} : G/N &\to H \\ gN &\mapsto f(g) \end{aligned}$$

wohldefiniert. Außerdem ist $\bar{f}$ ein Gruppenhomomorphismus:

$$\bar{f}(gN \cdot hN) = \bar{f}(ghN) = f(gh) = f(g) \cdot f(h) = \bar{f}(gN) \cdot \bar{f}(hN).$$

Es gilt offensichtlich $f = \bar{f} \circ p$

$$f(g) = \bar{f}(gN) = \bar{f}(p(g)).$$

Jeder Homomorphismus $\varphi : G/N \to H$ mit $f = \varphi \circ p$ stimmt mit $\bar{f}$ überein, weil p surjektiv ist:

$$\varphi(gN) = \varphi(p(g)) = f(g) = \bar{f}(p(g)) = \bar{f}(gN).$$

Dies zeigt die Eindeutigkeit der geforderten Faktorisierung in (ii) aus Definition 6.1. □

Bemerkung 6.4. Aus dem Beweis von Satz 6.3 folgt, daß Faktorgruppen G/N zusammen mit der natürlichen Abbildung $G \to G/N$ Quotienten sind. Wegen der Eindeutigkeit des Quotienten, Proposition 6.2, sind Quotientenabbildungen für Normalteiler $N \subseteq G$ immer surjektiv, und der Kern ist gleich N. Das folgt **nicht** aus der **definierenden universellen Eigenschaft** des Quotienten, sondern aus der **Konstruktion** mittels Faktorgruppe und der Eindeutigkeit.

Beispiel 6.5 (Quotienten von $\mathbb{Z}$). Die Gruppe $\mathbb{Z}$ ist abelsch und daher jede Untergruppe auch Normalteiler. Für $N = \{0\}$ ist $\mathbb{Z}/N = \mathbb{Z}$ und die Quotientenabbildung die Identität. Sei $n > 0$ eine natürliche Zahl. Wir betrachten nun den Normalteiler $N = n\mathbb{Z}$. Dann ist

$$\mathbb{Z}/n\mathbb{Z}$$

die Gruppe der Restklassen modulo n. Die Elemente

$$a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$$

bestehen aus allen Elementen in $\mathbb{Z}$ mit vorgegebenem Rest bei Ganzzahldivision durch n. Die Addition in $\mathbb{Z}/n\mathbb{Z}$ wird mittels Addition in $\mathbb{Z}$ von Vertretern definiert. Für $b \in a + n\mathbb{Z}$ schreibt man auch

$$b \equiv a \mod n,$$

d.h. die Äquivalenzrelation, die durch die Nebenklassen nach $n\mathbb{Z}$ definiert ist, wird mit dem Symbol "$\equiv \mod n$" bezeichnet. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ hat die Ordnung n.

Das spezielle Beispiel $n = 12$ zusammen mit der *modularen Arithmetik* modulo 12 lernt jedes Kind zusammen mit der Uhr in der Regel spätestens in der Grundschule.

6.2. **Die Isomorphiesätze.** Wir kommen nun zu klassischen Isomorphiesätzen. Der erste, der Homomorphiesatz, beweist die anderen Isomorphiesätze als Spezialfall, und ist doch selbst im Grunde ein Spezialfall der Existenz und Eindeutigkeit von Quotienten nach Normalteilern.

Beispiel 6.6. Sei $n \in \mathbb{N}$. Die alternierende Gruppe A_n hat Index 2 in S_n und ist daher ein Normalteiler. Die Nebenklassen sind die Mengen konstanten Signums, daher parametrisiert man S_n/A_n am besten mittels des Signums als $\{\pm 1\}$. Es fällt nicht schwer, dies als Isomorphismus

$$S_n/A_n \simeq \{\pm 1\}$$

zu erkennen. Dies ist ein Beispiel für den folgenden Satz, hier angewandt auf $\operatorname{sign} : S_n \to \{\pm 1\}$.

Satz 6.7 (Homomorphiesatz)**.** *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gibt es einen Isomorphismus*

$$\varphi : G/\ker(f) \xrightarrow{\sim} \operatorname{im}(f), \qquad g\ker(f) \mapsto f(g).$$

Beweis. Der Kern $N = \ker(f)$ ist ein Normalteiler und $p : G \to G/N$ ein Quotient. Daher faktorisiert f eindeutig über einen Gruppenhomomorphismus

$$\tilde{\varphi} : G/N \to H$$

mit $f = \tilde{\varphi} \circ p$. Weil p surjektiv ist, nimmt $\tilde{\varphi}$ nur Werte

$$\tilde{\varphi}(gN) = f(g) \in \operatorname{im}(f)$$

an. Man kann daher $\tilde{\varphi}$ eindeutig als Komposition eines Gruppenhomomorphismus

$$\varphi : G/N \to \operatorname{im}(f)$$

und der Inklusion $i : \operatorname{im}(f) \hookrightarrow H$ schreiben. Es ergibt sich das folgende kommutative Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & H \\ \downarrow{\scriptstyle p} & \overset{\tilde{\varphi}}{\nearrow} & \uparrow{\scriptstyle \subseteq} \\ G/N & \overset{\varphi}{\dashrightarrow} & \operatorname{im}(f) \end{array}$$

Zu zeigen bleibt, daß φ ein Isomorphismus ist.

Wir bestimmen den Kern von φ. Sei $gN \in G/N$ ein Element im Kern von φ. Dann ist

$$f(g) = \varphi(gN) = 1,$$

also $g \in N$. Damit ist $gN = N$ und $\ker(\varphi) = 1$. Somit ist φ injektiv nach Proposition 2.26.

Die Abbildung φ ist surjektiv, denn für jedes $h \in \operatorname{im}(f)$ gibt es $g \in G$ mit $f(g) = h$ und

$$\varphi(gN) = f(g) = h.$$

Damit ist φ sogar bijektiv und ein Isomorphismus. □

Korollar 6.8. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann hat $\ker(f)$ endlichen Index genau dann, wenn $\operatorname{im}(f)$ endliche Ordnung hat. Es gilt dann:*

$$(G : \ker(f)) = |\operatorname{im}(f)|.$$

Beweis. Das folgt sofort aus dem Homomorphiesatz, Satz 6.7. □

Korollar 6.9. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Wenn G eine endliche Gruppe ist, dann gilt*

$$|G| = |\ker(f)| \cdot |\operatorname{im}(f)|.$$

Beweis. Das folgt sofort aus Korollar 6.8 und dem Satz von Lagrange, Satz 4.13,

$$|G| = |\ker(f)| \cdot (G : \ker(f)) = |\ker(f)| \cdot |\operatorname{im}(f)|.$$ □

Beispiel 6.10. Sei G eine Gruppe. In Satz 2.32 haben wir bereits eine Version des Homomorphiesatz bewiesen, und zwar für die Exponentialabbildung $\varphi(a) = g^a$ zu einem Element $g \in G$. Der Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$ hat Kern $\ker(\varphi) = n\mathbb{Z}$ für $n = \operatorname{ord}(g)$ und induziert einen Gruppenisomorphismus

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \operatorname{im}(\varphi) = \langle g \rangle.$$

Das ist nichts anderes als der Homomorphiesatz, Satz 6.7, angewandt auf φ.

Satz 6.11 (Erster Isomorphiesatz)**.** *Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler. Dann ist*

$$\begin{aligned} H/(H \cap N) &\xrightarrow{\sim} HN/N \\ h(H \cap N) &\mapsto hN \end{aligned}$$

ein Gruppenisomorphismus. Insbesondere gilt:

(1) Das Produkt in G von Mengen

$$HN = \{hn \ ; \ h \in H, n \in N\} \subseteq G$$

ist eine Untergruppe in G, und

(2) $N \subseteq HN$ ist ein Normalteiler.

(3) $N \cap H$ ist ein Normalteiler in H.

Beweis. (1) Sei $i : H \hookrightarrow G$ die Inklusion und $p : G \to G/N$ die Quotientenabbildung. Die Abbildung

$$f = p \circ i : H \to G \to G/N$$

ist ein Gruppenhomomorphismus und

$$HN = p^{-1}(f(H))$$

ist eine Untergruppe als Urbild einer Untergruppe.

(2) Es gilt $N \subseteq HN$ und als Normalteiler in G ist N Normalteiler in jeder Untergruppe von G, in der N enthalten ist.

(3) Der Kern von f ist $f^{-1}(1) = i^{-1}(N) = H \cap N$ und als Kern ist $H \cap N$ ein Normalteiler von H.

Nun beweisen wir die Isomorphieaussage. Per Konstruktion ist $HN/N \subseteq G/N$ eine Untergruppe. Genauer ist HN/N das Bild von $f : H \to G/N$ wie oben. Der Homomorphiesatz, Satz 6.7, angewandt auf f liefert den gesuchten Isomorphismus

$$\varphi : H/(H \cap N) \xrightarrow{\sim} HN/N,$$

denn für alle $h \in H$ gilt $\varphi(h(H \cap N)) = f(h) = hN$ nach Konstruktion von φ wie in Satz 6.7. □

Beispiel 6.12. (1) Sei $G = \mathbb{Z}$, $H = 5\mathbb{Z}$ und $N = 3\mathbb{Z}$. Dann ist $H \cap N = 15\mathbb{Z}$ und wegen $1 = 2 \cdot 3 - 5$ gilt $HN = \mathbb{Z}$. Nach dem ersten Isomorphiesatz gilt

$$5\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}.$$

(2) Sei K ein Körper und $n \in \mathbb{N}$. Sei $\mathbf{1} \in \mathrm{GL}_n(K)$ die Einheitsmatrix. Die Gruppe $D \subseteq \mathrm{GL}_n(K)$ der Diagonalmatrizen mit konstantem Eintrag auf der Diagonale aus $K^\times$ ist isomorph zu $K^\times$ vermöge

$$\begin{aligned} K^\times &\to D \\ \lambda &\mapsto \lambda\mathbf{1} = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda \end{pmatrix} \end{aligned}$$

Ferner ist D ein Normalteiler in $\mathrm{GL}_n(K)$, denn für $\lambda \in K^\times$ und $A \in \mathrm{GL}_n(K)$ gilt

$$A(\lambda \mathbf{1})A^{-1} = \lambda(A\mathbf{1}A^{-1}) = \lambda(AA^{-1}) = \lambda\mathbf{1}.$$

Die Faktorgruppe ist

$$\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/D,$$

genannt die **projektiv lineare Gruppe**.

(3) Wir betrachten nun $H = \mathrm{SL}_n(K)$ als Untergruppe von $\mathrm{GL}_n(K)$. Dann ist

$$\mu_n(K) := \{\lambda \in K^\times \ ; \ \lambda^n = 1\}$$

über die Einschränkung des Isomorphismus $K^\times \simeq D$ selbst isomorph zu

$$\mu_n(K) \simeq D_n := \mathrm{SL}_n(K) \cap D.$$

Der erste Isomorphiesatz liefert dann den Isomorphismus

$$\mathrm{SL}_n(K)/D_n \xrightarrow{\sim} \mathrm{SL}_n(K)D/D$$

auf die Untergruppe

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)D/D \subseteq \mathrm{GL}_n(K)/D = \mathrm{PGL}_n(K).$$

Satz 6.13 (Zweiter Isomorphiesatz)**.** *Sei G eine Gruppe und N und K seien Normalteiler in G mit $N \subseteq K \subseteq G$. Dann ist*

$$(G/N)/(K/N) \xrightarrow{\sim} G/K$$
$$gN(K/N) \mapsto gK$$

ein Gruppenisomorphismus. Insbesondere ist K/N ein Normalteiler in G/N.

Beweis. Die Quotientenabbildung $p : G \to G/K$ hat Kern K, daher gilt $p(N) = 1$. Die universelle Eigenschaft aus Satz 6.3 des Quotienten $q : G \to G/N$ liefert einen eindeutigen Gruppenhomomorphismus

$$f : G/N \to G/K$$

mit

$$f(gN) = f(q(g)) = p(g) = gK.$$

Die Abbildung f ist offensichtlich surjektiv und $\ker(f) = K/N$, denn $gK = K$ bedeutet $g \in K$. Der Homomorphiesatz, Satz 6.7, angewandt auf f liefert den gesuchten Isomorphismus

$$\varphi : (G/N)/(K/N) \xrightarrow{\sim} G/K$$

und $\varphi(gN(K/N)) = f(gN) = gK$ wie behauptet. □

Beispiel 6.14. Seien $n, m \in \mathbb{N}$ natürliche Zahlen. Dann ist $mn\mathbb{Z} \subseteq m\mathbb{Z} \subseteq \mathbb{Z}$. Nach dem zweiten Isomorphiesatz gilt dann

$$(\mathbb{Z}/nm\mathbb{Z})/(m\mathbb{Z}/nm\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}.$$

6.3. **Kommutatoren und abelsche Quotienten.** Kommutatoren messen die Abweichung von Kommutativität.

Definition 6.15. Der **Kommutator** zweier Gruppenelemente $g, h \in G$ ist das Element

$$[g, h] = ghg^{-1}h^{-1} \in G.$$

Notation 6.16. Unter Gruppentheoretikern ist auch die Notation

$$(g, h) = g^{-1}h^{-1}gh = g^{-1}g^h$$

geläufig. Das ist im Sinne dieses Skripts nichts weiter als der Kommutator der inversen Elemente.

Lemma 6.17. *Seien $g, h \in G$ Gruppenelemente. Dann kommutieren g und h genau dann, wenn gilt:*

$$[g, h] = 1.$$

Beweis. Es gilt $gh = hg$ genau dann, wenn $[g,h] = ghg^{-1}h^{-1} = hg(g^{-1}h^{-1}) = 1$ gilt. □

Lemma 6.18. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Für alle $x, y \in G$ gilt*

$$f([x,y]) = [f(x), f(y)].$$

Beweis. Das ist trivial. □

Definition 6.19. Die **Kommutator(unter)gruppe** einer Gruppe G ist die Untergruppe

$$[G,G] = \langle [g,h] \ ; \ g,h \in G \rangle,$$

welche von allen Kommutatoren in G erzeugt wird.

Notation 6.20. Als Notation für die Kommutatorgruppe zu G findet man auch $G' = [G,G]$.

Lemma 6.21. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$f([G,G]) \subseteq [H,H].$$

Beweis. Das folgt aus Lemma 6.18 und Proposition 2.44. □

Proposition 6.22 (Kommutatorfaktorgruppe)**.** *Sei G eine Gruppe. Dann ist die Kommutatorgruppe $[G,G]$ ein Normalteiler in G, und die Faktorgruppe $G/[G,G]$ ist abelsch.*

*Wir nennen die Gruppe $G/[G,G]$ die **Kommutatorfaktorgruppe** von G.*

Beweis. Seien $g, x, y \in G$ beliebig und $a = gxg^{-1}$ und $b = gyg^{-1}$. Dann ist

$$g[x,y]g^{-1} = \varphi_g([x,y]) = \varphi_g(xyx^{-1}y^{-1}) = \varphi_g(x)\varphi_g(y)\varphi_g(x)^{-1}\varphi_g(y)^{-1} = [a,b].$$

Daher gilt

$$g[G,G]g^{-1} = \varphi_g(\langle [x,y] \ ; \ x,y \in G \rangle) = \langle \varphi_g([x,y]) \ ; \ x,y \in G \rangle \subseteq \langle [a,b] \ ; \ a,b \in G \rangle = [G,G].$$

Nach Proposition 4.41 ist damit $[G,G]$ ein Normalteiler in G.

Seien $\overline{a}, \overline{b} \in G/[G,G]$ beliebige Elemente und $a, b \in G$ mit $p(a) = \overline{a}$ und $p(b) = \overline{b}$. Dann:

$$[\overline{a}, \overline{b}] = p(a)p(b)p(a)^{-1}p(b)^{-1} = p(aba^{-1}b^{-1}) = p([a,b]) = 1.$$

Also ist $G/[G,G]$ kommutativ. □

Definition 6.23. Die **Abelisierung** einer Gruppe G ist eine abelsche Gruppe G^{ab} zusammen mit einem Homomorphismus $p : G \to G^{\mathrm{ab}}$, so daß es für alle Homomorphismen $f : G \to H$ mit Ziel in einer abelschen Gruppe H einen eindeutigen Homomorphismus

$$\varphi : G^{\mathrm{ab}} \to H$$

gibt mit $f = \varphi \circ p$.

Die Eindeutigkeit der Abelisierung folgt dem gewohnten Muster bei universellen Eigenschaften. Wir beschränken uns deshalb darauf zu zeigen, daß die Kommutatorfaktorgruppe eine (die) Abelisierung ist.

Satz 6.24 (Abelisierung)**.** *Sei G eine Gruppe. Dann hat die Quotientenabbildung*

$$p : G \to G/[G,G]$$

die universelle Eigenschaft der Abelisierung.

Beweis. Die Gruppe $G/[G,G]$ ist abelsch nach Proposition 6.22.

Sei $f : G \to H$ ein beliebiger Homomorphismus mit einer abelschen Gruppe H als Ziel. Dann gilt für beliebige Elemente $x, y \in G$:

$$f([x,y]) = [f(x), f(y)] = 1,$$

also gilt $[G,G] \subseteq \ker(f)$. Die Existenz und Eindeutigkeit der Faktorisierung folgt nun aus der universellen Eigenschaft des Quotienten nach Satz 6.3 zusammen damit, daß $p : G \to G/[G,G]$ eine Quotientenabbildung ist. □

Übungsaufgaben zu §6

Übungsaufgabe 6.1. (Die universelle Eigenschaft des Produkts) Sei I eine Menge und G_i eine Gruppe für jedes $i \in I$. Ein **Produkt** der Gruppen G_i besteht aus einer Gruppe P zusammen mit Homomorphismen für alle $i \in I$

$$p_i : P \to G_i,$$

so daß die **universelle Eigenschaft für Produkte** gilt: für jede Gruppe Γ und Gruppenhomomorphismen $f_i : \Gamma \to G_i$ für alle $i \in I$ existiert ein eindeutiger Gruppenhomomorphismus

$$f : \Gamma \to P$$

mit $p_i \circ f = f_i$.

Zeigen Sie, daß $\prod_{i\in I} G_i$ zusammen mit den Projektionen $\mathrm{pr}_j : \prod_{i\in I} G_i \to G_j$ ein Produkt der Gruppen G_i ist. Zeigen Sie weiter, daß jedes Produkt P der G_i auf eindeutige Weise zu $\prod_{i\in I} G_i$ isomorph ist, d.h., es gibt einen eindeutigen Isomorphismus

$$\varphi : P \xrightarrow{\sim} \prod_{i\in I} G_i$$

mit $p_i = \mathrm{pr}_i \circ \varphi$.

Übungsaufgabe 6.2. Zeigen Sie, daß die Operation von $\mathrm{GL}_{n+1}(K)$ auf $\mathbb{P}^n(K)$ aus Aufgabe 3.5 eine Operation von $\mathrm{PGL}_{n+1}(K)$ auf $\mathbb{P}^n(K)$ induziert.

Übungsaufgabe 6.3. Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Berechnen Sie die Ordnung der Gruppe $\mathrm{PGL}_n(\mathbb{F})$.

Übungsaufgabe 6.4. Bestimmen Sie die Kommutatorfaktorgruppe von S_n.

Übungsaufgabe 6.5. Sei G eine endliche Gruppe, p der kleinste Primteiler von $|G|$ und $U \subseteq G$ eine Untergruppe vom Index $p = (G : U)$. Zeigen Sie, daß U ein Normalteiler ist.

Tipp: Lassen Sie G auf G/U durch Tanslation operieren. Das führt zu einem Gruppenhomomorphismus $\rho : G \to S_p$, indem $g \in G$ auf die Permutation der Nebenklassen abgebildet wird, die es induziert. Bestimmen Sie die Ordnung des Bildes mithilfe des Satzes von Lagrange. Der Kern von ρ ist ein Normalteiler, den Sie mit U identifizieren müssen.

Übungsaufgabe 6.6. Seien H und N Untergruppen von G. Dann ist das naive mengentheoretische Produkt

$$HN = \{hk \ ; \ h \in H, k \in N\}$$

in der Regel keine Untergruppe von G mehr. Geben Sie ein Beispiel.

Zeigen Sie, daß HN eine Untergruppe von G ist, sofern N ein Normalteiler von G ist.

Übungsaufgabe 6.7 (Lineare Darstellung der Diedergruppe). Sei $n \geq 3$ eine natürliche Zahl und D_n die n-te Diedergruppe mit einer Drehung d und einer Spiegelung s als Erzeugern. Zeigen Sie, daß durch

$$\begin{aligned} D_n &\to \mathrm{GL}_2(\mathbb{R}) \\ d &\mapsto \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \\ s &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

ein injektiver Gruppenhomomorphismus definiert wird.

Teil 2. **Ringe**

7. Ringe

7.1. **Definition, Beispiele und elementare Regeln.** Ringe sind Strukturen mit Addition und Multiplikation.

Definition 7.1. (1) Ein **Ring (mit Eins)** ist eine Menge R zusammen mit Verknüpfungen **Addition**

$$+ : R \times R \to R$$

und **Multiplikation**

$$\cdot : R \times R \to R$$

mit den folgenden Eigenschaften.

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

(ii) Die Multiplikation ist **assoziativ**: für alle $a, b, c \in R$ gilt

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(iii) Addition und Multiplikation sind **distributiv**: für alle $a, b, r \in R$ gilt

$$r \cdot (a + b) = (r \cdot a) + (r \cdot b),$$
$$(a + b) \cdot r = (a \cdot r) + (b \cdot r).$$

(iv) Es gibt ein neutrales Element $1 \in R$ für die Multiplikation: für alle $a \in R$ gilt

$$1 \cdot a = a = a \cdot 1.$$

(2) Ein **kommutativer Ring** ist ein Ring, so daß für alle $a, b \in R$ gilt

$$a \cdot b = b \cdot a.$$

Bemerkung 7.2. Der Name hat nichts mit der Geometrie eines ringförmigen Objekts zu tun. Es geht um den Zusammenschluß von Elementen zu einer Gesamtstruktur, ähnlich einer juristischen Person (Weißer Ring, etc.). Dabei steht (juristisch) Ring in Abgrenzung zu (juristisch) Körper(schaft) als eine Organisationsstruktur mit einer Regel weniger: es wird nicht gefordert, daß es für Elemente $a \neq 0$ ein Inverses a^{-1} bezüglich der Multiplikation gibt.

Notation 7.3. (1) Die Multiplikation kürzen wir ab durch

$$ab := a \cdot b.$$

Außerdem gilt 'Punkt vor Strich'. Diese Festlegung spart Klammern.

(2) Das neutrale Element der Addition wird mit 0 bezeichnet, das additive Inverse zu $a \in R$ hat die Notation

$$-a$$

also $a + (-a) = (-a) + a = 0$. Statt $a + (-b)$ schreiben wir wie gewöhnlich $a - b$.

(3) Zu $a \in R$ und $n \in \mathbb{N}_0$ definieren wir rekursiv $a^0 = 1$ und

$$a^n := a \cdot a^{n-1}.$$

Damit ist $a^n = a \cdot \ldots \cdot a$ mit n-Faktoren a. Es gelten die erwarteten Potenzgesetze

$$a^n a^m = a^{n+m},$$
$$(a^n)^m = a^{nm},$$
$$(ab)^n = a^n b^n. \qquad \text{(nur wenn } ab = ba\text{)}$$

Beispiel 7.4. (1) Jeder Körper ist ein Ring: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_p$, $\mathbb{C}$, ...

(2) Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring mit der üblichen Addition und Multiplikation.

(3) Sei X eine Menge und R ein Ring. Dann ist die Menge

$$\mathrm{Abb}(X,R) := \{f \ ; \ f : X \to R \text{ Abbildung}\}$$

der Abbildungen von X nach R ein Ring, der **Ring der Funktionen** von X nach R, und zwar mit punktweiser Addition und Multiplikation: für $f_1, f_2 \in \mathrm{Abb}(X,R)$ und $x \in X$ gilt

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 \cdot f_2)(x) = f_1(x) \cdot f_2(x).$$

Die Ringaxiome sind erfüllt, weil sie in R erfüllt sind. Man überlege sich dies!

(4) Sei K ein Körper und $n \in \mathbb{N}$. Dann ist $\mathrm{M}_n(K)$, der **Matrizenring (über K)**, ein Ring mit der üblichen Matrizenmultiplikation und Matrizenaddition.

(5) Sei V ein K-Vektorraum. Dann ist $\mathrm{End}_K(V)$ ein Ring bezüglich Addition und Komposition von linearen Abbildungen.

(6) Sei R ein Ring und $n \in \mathbb{N}$. Matrizen mit Einträgen in R lassen sich genauso addieren und multiplizieren wie Matrizen mit Einträgen in einem Körper. Mit der üblichen Matrizenmultiplikation und Matrizenaddition ist $\mathrm{M}_n(R)$, der **Matrizenring (über R)**, ein Ring.

(7) Der **Nullring** ist der einzige Ring mit genau einem Element. Addition und Multiplikation ergeben sich von selbst.

Beispiel 7.5. Sei G eine Gruppe und K ein Körper. Der **Gruppenring** mit Koeffizienten aus K ist der Ring

$$K[G] = \bigoplus_{g \in G} K \cdot g,$$

also als K-Vektorraum einfach die direkte Summe von 1-dimensionalen Vektorräumen mit Basis g für jedes Gruppenelement $g \in G$. Elemente von $K[G]$ sind daher endliche Summen

$$a = \sum_{g \in G} a(g) g$$

mit $a(g) \in K$ und alle bis auf endlich viele $a(g) = 0$. Dies kann man auch als Funktionen

$$a : G \to K$$

auffassen mit einem Wert $\neq 0$ an nur endlich vielen Stellen $g \in G$. Die Basisvektoren $g \in K \cdot g$ liefern Elemente $g \in K[G]$.

Die Addition von $K[G]$ ist die Addition als Vektorraum. Die Multiplikation wird definiert für $a, b \in K[G]$ durch (Faltung)

$$a \cdot b(g) = \sum_{x,y \in G,\ xy=g} a(x) b(y).$$

Dies ist wohldefiniert, weil nur endlich viele x und endlich viele y zu $a(x) \neq 0 \neq b(y)$ führen: die Summe ist eine endliche Summe. Diese Multiplikation setzt die Gruppenverknüpfung auf den Elementen $g \in K[G]$ für $g \in G$ linear fort: für alle $g, h \in G$ gilt

$$g \cdot h = gh.$$

Wir überlassen den Nachweis der Ringaxiome als Übungsaufgabe.

Bemerkung 7.6. Manchmal versteht man unter einem Ring einen Ring ohne Eins, also eine Menge R mit $+$ und $\cdot$, so daß (i)-(iii) der obigen Definition gelten. Dies tun wir hier nicht. Manchmal wird für Ringe mit Eins noch verlangt, daß $0 \neq 1$ gilt. Das tun wir hier auch nicht, um den Nullring nicht auszuschließen.

Die Eins in einem Ring ist eindeutig. Das geht wie beim neutralen Element einer Gruppe. Sind 1 und $1'$ Einsen, dann gilt

$$1 = 1 \cdot 1' = 1'.$$

Es gelten die üblichen Rechenregeln für $-$, insbesondere das Distributivgesetz mit $-$ statt $+$.

Lemma 7.7. *Sei R ein Ring. Dann gilt für alle $a, b, c \in R$*
(1) $0 \cdot a = a \cdot 0 = 0$,
(2) $(-a)b = a(-b) = -(ab)$,
(3) $a(b-c) = ab - ac$ *und* $(a-b)c = ac - bc$.
(4) $(-a)(-b) = ab$.
(5) $-a = (-1)a = a(-1)$.

Beweis. (1) Aus $0a = (0+0)a = 0a + 0a$ folgt durch Addition mit $-(0a)$ schon $0 = 0a$. Die Gleichung $a0 = 0$ folgt analog.

(2) Wegen $ab + (-a)b = (a + (-a))b = 0b = 0$ folgt $(-a)b = -(ab)$. Die andere Gleichung folgt analog.

(3) Es gilt $a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-ac) = ab - ac$. Die andere Gleichung folgt analog.

(4) Wir verwenden zweimal (2) und rechnen: $(-a)(-b) = -(a)(-b) = -(-(ab)) = ab$.

(5) Aus (2) folgt $(-1)a = -(1a) = -a$. Die andere Gleichung folgt analog. □

Lemma 7.8. *Sei $0 = 1$ in einem Ring R, dann ist R der Nullring.*

Beweis. Sei $a \in R$ ein beliebiges Element. Dann gilt

$$a = a \cdot 1 = a \cdot 0 = 0$$

und R enthält nur ein einziges Element. □

Bemerkung 7.9. Jeder Ring ist ein Ring von geeigneten Funktionen auf einer Menge. Das Beispiel $\mathrm{Abb}(X, R)$ ist also gut für die Intuition, aber trotzdem noch eine grobe Approximation, denn man muß akzeptieren, daß der Wertebereich der Funktionen von $x \in X$ abhängt. So ist beispielsweise $\mathbb{Z}$ der Ring der algebraischen Funktionen auf $\mathrm{Spec}(\mathbb{Z})$, einer Menge die im Wesentlichen aus den Primzahlen besteht. Der Wert von $n \in \mathbb{Z}$ an der Primzahl p ist die Restklasse $n \mod p$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Man kann zumindest sehen, daß diese Funktionswerte die ganzen Zahlen als Funktionen eindeutig festlegen. Denn falls für $n, m \in \mathbb{Z}$ und alle Primzahlen p gilt $n \equiv m \mod p$, so wählen wir einfach eine Primzahl p, die größer als $2\max\{|n|, |m|\}$ ist, und finden wegen

$$-p < n - m < p$$

und $p \mid n - m$, daß $n = m$ sein muß. Entscheidend geht hier ein, daß es unendlich viele Primzahlen in $\mathbb{Z}$ gibt und damit die gewünschte Wahl von p auch durchgeführt werden kann. Wenn Sie nicht wissen, wie man beweist, daß es unendlich viele Primzahlen gibt, dann holen Sie das schnellstmöglich nach. Speziell Euklids Beweis hierfür sollte jede/r Mathematikstudierende kennen.

Beispiel 7.10. Die Menge der geraden ganzen Zahlen $2\mathbb{Z} \subseteq \mathbb{Z}$ ist für den allgemeineren Begriff des Rings, wo keine Eins gefordert wird, ein Unterring, und gleichzeitig ein Beispiel eines Rings ohne Eins.

Definition 7.11. Seien $n, k \in \mathbb{N}_0$. Der Binomialkoeffizient $\binom{n}{k}$ ist definiert als

$$\binom{n}{k} = |\{k\text{-elementige Teilmengen von } \{1, \ldots, n\}\}|$$

und damit eine ganze Zahl ≥ 0. Für $0 \leq k \leq n$ gilt $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ und sonst $\binom{n}{k} = 0$.

Proposition 7.12 (Binomischer Lehrsatz)**.** *Seien $a, b \in R$ kommutierende Elemente: $ab = ba$. Dann gilt für alle $n \in \mathbb{N}_0$:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Beweis. Aus $ab = ba$ zeigt man zunächst per Induktion nach k, daß auch $ba^k = a^k b$ gilt.

Wir argumentieren nun per Induktion nach n. Der Anfang $n = 0$ ist klar. Im Schritt von n auf $n+1$ muß man bei

$$(a+b)^{n+1} = (a+b) \cdot \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n+1} \left(\binom{n}{k} + \binom{n}{k-1} \right) a^k b^{n+1-k}$$

das Element b an a^k „vorbeiziehen“. Nun folgt die Formel durch Koeffizientenvergleich mittels der Rekursionsformel für Binomialkoeffizienten

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Aus der $n+1$-elementigen Menge wählen wir einen Präsidenten. Die k-elementigen Teilmengen teilen sich auf in $\binom{n}{k}$-viele ohne und $\binom{n}{k-1}$-viele mit dem Präsidenten. □

7.2. **Homomorphismen.** Wir wollen algebraische Strukturen stets zusammen mit den strukturerhaltenden Abbildungen untersuchen.

Definition 7.13. Ein **Ringhomomorphismus** (oder kürzer **Homomorphismus**) zwischen Ringen R und S ist eine Abbildung $f : R \to S$, so daß für alle $a, b \in R$ gilt:

(i) $f(a+b) = f(a) + f(b)$,
(ii) $f(ab) = f(a)f(b)$,
(iii) $f(1) = 1$.

Ein **Ringisomorphismus** ist ein bijektiver Ringhomomorphismus.

Bemerkung 7.14. (1) Für jeden Ringhomomorphismus $f : R \to S$ ist f ein Gruppenhomomorphismus der zugrundeliegenden abelschen Gruppen. Inbesondere gilt für alle $a \in R$

$$f(-a) = -f(a).$$

(2) Ein **Ringisomorphismus** zu sein ist äquivalent dazu, daß es einen inversen Ringhomomorphismus gibt: das Inverse ist aufgrund der Bijektivität automatisch ein Ringhomomorphismus.

Beispiel 7.15. (1) Sei R ein Ring und $\varphi : Y \to X$ eine Abbildung von Mengen. Der **Pullback** (oder **Rückzug**) ist der folgende Ringhomomorphismus:

$$\varphi^* : \mathrm{Abb}(X, R) \to \mathrm{Abb}(Y, R), \qquad \varphi^*(f) = f \circ \varphi,$$

also $(\varphi^* f)(y) = f(\varphi(y))$ für alle $y \in Y$.

(2) Ist $i : Y \hookrightarrow X$ die Inklusion einer Teilmenge, dann ist der Pullback die **Einschränkung**

$$i^*(f) = f|_Y.$$

(3) Für eine einpunktige Menge $Y = \{y\}$ ist $\mathrm{Abb}(Y, R) \simeq R$. Die Abbildung $f \mapsto f(y)$ ist bijektiv und ein Ringisomorphismus.

(4) Ein Spezialfall des Pullback: zu $x \in X$ und der Inklusion $i : Y = \{x\} \hookrightarrow X$ ist

$$i^* : \mathrm{Abb}(X, R) \to \mathrm{Abb}(\{x\}, R) \simeq R$$
$$f \mapsto i^* f = f(x).$$

Dies ist der **Auswertungsringhomomorphismus** im Punkt $x \in X$.

Beispiel 7.16. Die **komplexe Konjugation** $\mathbb{C} \to \mathbb{C}$ definiert durch

$$z = x + iy \mapsto \bar{z} = x - iy$$

ist ein Ringhomomorphismus, sogar ein Ringisomorphismus.

Beispiel 7.17. Sei K ein Körper. Dann ist

$$\begin{aligned} K &\to \mathrm{M}_2(K) \\ a &\mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

kein Ringhomomorphismus. Wohl aber ist mit der Einheitsmatrix $\mathbf{1}_n \in \mathrm{M}_n(K)$ die Abbildung

$$\lambda \mapsto \lambda \mathbf{1}_n = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

ein Ringhomomorphismus $K \to \mathrm{M}_n(K)$.

Für einen K-Vektorraum V ist $\lambda \mapsto \lambda \cdot \mathrm{id}_V$ ein Ringhomomorphismus. Dies ist die koordinatenfreie Version des Ringhomomorphismus $K \to \mathrm{M}_n(K)$.

7.3. **Potenzreihenringe und Polynomringe.** Wir kommen zu zwei wichtigen Beispielen für Ringe.

Definition 7.18. Sei R ein Ring. Der **Potenzreihenring** mit Koeffizienten in R und der (formalen) Variablen X ist der Ring

$$R[[X]] = \{\sum_{i=0}^{\infty} a_i X^i \ ; \ a_i \in R \text{ für alle } i\}$$

der formalen Potenzreihen mit der folgenden Addition und Multiplikation:

$$\begin{aligned} \Big(\sum_{i=0}^{\infty} a_i X^i\Big) + \Big(\sum_{i=0}^{\infty} b_i X^i\Big) &= \sum_{i=0}^{\infty} (a_i + b_i) X^i, \\ \Big(\sum_{i=0}^{\infty} a_i X^i\Big) \cdot \Big(\sum_{i=0}^{\infty} b_i X^i\Big) &= \sum_{i=0}^{\infty} \big(\sum_{j+k=i} a_j b_k\big) X^i. \end{aligned}$$

Die innere Summe geht hier über $0 \leq j \leq i$ mit $k = i - j$, aber in unserer Schreibweise ist es symmetrischer. Die Bedingung $j, k \geq 0$ nehmen wir stillschweigend dazu, denn a_j und b_k sind ja nur für $j, k \geq 0$ vorhanden. Insbesondere handelt es sich um eine **endliche Summe**, somit ist die Multiplikation in $R[[X]]$ wohldefiniert.

Die Ringaxiome verifiziert man leicht, etwa die Assoziativität:

$$\begin{aligned} \big(\sum_{i=0}^{\infty} a_i X^i \cdot \sum_{i=0}^{\infty} b_i X^i\big) \cdot \sum_{i=0}^{\infty} c_i X^i &= \sum_{i=0}^{\infty} \big(\sum_{j+k=i} a_j b_k\big) X^i \cdot \sum_{i=0}^{\infty} c_i X^i \\ &= \sum_{i=0}^{\infty} \big(\sum_{r+s=i} \big(\sum_{j+k=r} a_j b_k\big) c_s\big) X^i \\ &= \sum_{i=0}^{\infty} \big(\sum_{j+k+l=i} a_j b_k c_l\big) X^i \\ &= \sum_{i=0}^{\infty} \big(\sum_{r+s=i} a_r \big(\sum_{k+l=s} b_k c_l\big)\big) X^i \\ &= \sum_{i=0}^{\infty} a_i X^i \cdot \sum_{i=0}^{\infty} \big(\sum_{k+l=i} b_k c_l\big) X^i = \sum_{i=0}^{\infty} a_i X^i \cdot \big(\sum_{i=0}^{\infty} b_i X^i \cdot \sum_{i=0}^{\infty} c_i X^i\big). \end{aligned}$$

Notation 7.19. (1) Wir schreiben suggestiv

$$\sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 + \dots.$$

'Formale Variable' bedeutet, daß man nicht erwartet, hier etwas einsetzen zu können. Insbesondere wird auch kein analytischer Limes gebildet. Die formalen Potenzreihen sind einzig Symbole mit gewissen Rechenregeln, die an Polynome und Potenzreihen aus der Analysis erinnern.

(2) Das Element $X \in R[[X]]$ bezeichne die Potenzreihe

$$X = 0 + 1 \cdot X + 0 \cdot X^2 + \dots.$$

Man rechnet leicht nach, daß X^i die folgende Potenzreihe ist:

$$X^i = 0 + \ldots + 0 \cdot X^{i-1} + 1 \cdot X^i + 0 \cdot X^{i+1} + \ldots$$

Bemerkung 7.20. Eine beliebige Potenzreihe ist trotzdem nicht die Summe von Vielfachen der Potenzen X^i schlicht und einfach deshalb, weil man in diesem algebraischen Kontext keine unendlichen Summen bilden kann. Das ist nicht definiert, wohl aber das formale Symbol

$$\sum_{i=0}^{\infty} a_i X^i.$$

Definition 7.21. Ein **Unterring** (oder **Teilring**) eines Rings R ist eine Teilmenge $S \subseteq R$, die 1 enthält und die bezüglich der Addition eine Untergruppe ist und bezüglich der Multiplikation abgeschlossen ist.

Beispiel 7.22. Sei $f : R \to S$ ein Ringhomomorphismus. Das **Bild** von f ist ein Unterring

$$\mathrm{im}(f) = f(R) \subseteq S.$$

In der Tat: zu $x, y \in \mathrm{im}(f)$ gibt es $a, b \in R$ mit $f(a) = x$ und $f(b) = y$. Dementsprechend gilt

$$x - y = f(a) - f(b) = f(a - b) \in \mathrm{im}(f)$$

und $f(R)$ mit Addition ist eine Untergruppe von S mit Addition. Das folgt auch sofort aus der entsprechenden Aussage zu Untergruppen. Das Bild $\mathrm{im}(f)$ ist nichts anderes als das Bild des zugrundeiegenden Gruppenhomomorphsimus $f : (R, +) \to (S, +)$ der additiven Gruppen, damit eine Untergruppe. Weiter ist

$$1 = f(1) \in \mathrm{im}(f)$$

und $xy = f(a)f(b) = f(ab) \in \mathrm{im}(f)$.

Der Polynomring ist ein Unterring im formalen Potenzreihenring.

Definition 7.23. Sei R ein Ring.

(1) Der **Polynomring** mit Koeffizienten in R ist der Unterring

$$R[X] = \left\{ f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]] \ ; \text{ es gibt } n \geq 0 \text{ mit } a_i = 0 \text{ für alle } i > n \right\} \subseteq R[[X]].$$

Man schreibt dann (nicht notwendigerweise mit dem minimal möglichen n):

$$f = \sum_{i=0}^{n} a_i X^i = a_n X^n + \ldots + a_1 X + a_0.$$

Die Addition und Multiplikation von $R[[X]]$ führen $R[X]$ in sich über und definieren Addition und Multiplikation für den Polynomring $R[X]$. Die Ringaxiome vererben sich automatisch.

(2) Für $f \in R[X]$, $f \neq 0$, gibt es eine eindeutige Darstellung

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

mit $a_i \in R$ für $0 \leq i \leq n$ und $a_n \neq 0$. Dann ist $n = \deg(f)$ der **Grad** von f. Außerdem heißt f **normiert**, wenn darüberhinaus $a_n = 1$ gilt.

Beispiel 7.24. Sei R ein Ring. Die Abbildung

$$\begin{aligned} R &\to R[X] \\ a &\mapsto a = a \cdot X^0 + 0 \cdot X^1 + 0 \cdot X^2 + \ldots, \end{aligned}$$

die jedes Element auf das konstante Polynom a abbildet, ist ein injektiver Ringhomomorphismus. Wir identifizieren R mit dem Unterring von $R[X]$ der konstanten Polynome, der durch das Bild gegeben ist.

Satz 7.25 (Universelle Eigenschaft des Polynomrings)**.** *Sei $f : R \to S$ ein Ringhomomorphismus. Sei $y \in S$ ein Element, das mit allen Elementen aus $f(R)$ kommutiert, d.h. für alle $a \in R$ gilt*

$$f(a)y = yf(a).$$

Dann gehört zu y ein Ringhomomorphismus $\mathrm{ev}_y : R[X] \to S$, der Auswertungshomomorphismus in y:

$$\begin{aligned} \mathrm{ev}_y : R[X] &\to S \\ P(X) = \sum_{i=0}^{n} a_iX^i &\mapsto P(y) = \sum_{i=0}^{n} f(a_i)y^i, \end{aligned}$$

der eindeutig durch die folgenden Eigenschaften charakterisiert ist:

(i) $\mathrm{ev}_y(a) = f(a)$ *für jedes a in $R \subseteq R[X]$.*
(ii) $\mathrm{ev}_y(X) = y$.

Beweis. Die Auswertung $P(X) \mapsto P(y)$ ist ein Ringhomomorphismus, denn für

$$P(X) = \sum_{i=0}^{n} a_iX^i \quad \text{und} \quad Q(X) = \sum_{j=0}^{m} b_jX^j$$

gilt

$$\begin{aligned} P(y)Q(y) &= \big(\sum_{i=0}^{n} f(a_i)y^i\big) \cdot \big(\sum_{j=0}^{m} f(b_j)y^j\big) && \text{(ziehe } y^i \text{ an } f(b_j) \text{ vorbei)} \\ &= \sum_{0 \leq i \leq n, 0 \leq j \leq m} f(a_i)f(b_j)y^iy^j \\ &= \sum_{0 \leq i \leq n, 0 \leq j \leq m} f(a_ib_j)y^{i+j} \\ &= \sum_{k=0}^{n+m} \sum_{i+j=k} f(a_ib_j)y^k \\ &= \sum_{k=0}^{n+m} f(\sum_{i+j=k} a_ib_j)y^k = (PQ)(y). \end{aligned}$$

und für die Addition analog. Weiter wird die Eins, also das konstante Polynom 1 zu $f(1) = 1 \in R$ ausgewertet. Die Auswertung erfüllt die geforderten Eigenschaften.

Sei umgekehrt $F : R[X] \to S$ wie gefordert. Dann muß für $P(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ gelten

$$F(P) = F(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} F(a_i X^i) = \sum_{i=0}^{n} F(a_i) \cdot F(X)^i = \sum_{i=0}^{n} f(a_i) y^i = P(y) = \mathrm{ev}_y(P).$$

Dies zeigt die Eindeutigkeit. □

Man überlege sich zur Übung, wo im Satz 7.25 der Unterschied zwischen $R[X]$ und $R[[X]]$ wichtig ist.

Beispiel 7.26. Sei $A \in \mathrm{M}_n(K)$ eine quadratische Matrix über dem Körper K. Dann ist

$$\mathrm{ev}_A : K[X] \to \mathrm{M}_n(K)$$

der Auswertungshomomorphismus in A eindeutig dadurch bestimmt, daß $X \mapsto A$ und $\lambda \in K$ auf λE abgebildet wird.

Sei V ein K-Vektorraum und $f : V \to V$ ein K-linearer Endomorphismus. Dann ist

$$\mathrm{ev}_f : K[X] \to \mathrm{End}_K(V)$$

der Auswertungshomomorphismus in f eindeutig dadurch bestimmt, daß $X \mapsto f$ und $\lambda \in K$ auf $\lambda \cdot \mathrm{id}_V$ abgebildet wird.

Definition 7.27. Sei $n \in \mathbb{N}_0$. Der **Polynomring** $R[X_1, \ldots, X_n]$ **in n-Variablen mit Koeffizienten aus** R ist induktiv definiert als R für $n = 0$ und als Polynomring

$$R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n].$$

Ein **Monom** ist ein Element der Form

$$X_1^{k_1} \cdot \ldots \cdot X_n^{k_n}$$

für $k_1, \ldots, k_n \in \mathbb{N}_0$.

Lemma 7.28. *Jedes Element $P \in R[X_1, \ldots, X_n]$ ist eine eindeutige R-Linearkombination von paarweise verschiedenen Monomen: es gibt $d_1, \ldots, d_n \in \mathbb{N}_0$ und eindeutige*

$$a_{k_1,\ldots,k_n} \in R \qquad \text{für alle } 0 \le k_\alpha \le d_\alpha (1 \le \alpha \le n)$$

mit

$$P = \sum_{k_1=0}^{d_1} \cdots \sum_{k_n=0}^{d_n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdot \ldots \cdot X_n^{k_n}.$$

Die Eindeutigkeit ist dabei wie folgt gemeint: Darstellungen als Linearkombination, die sich nur in Koeffizienten $a_{k_1,\ldots,k_n} = 0$ unterscheiden, werden nicht als verschiedene Linearkombination betrachtet.

Beweis. Per Induktion nach n. □

Notation 7.29. Eine vernünftige Notation für Polynome in mehreren Variablen benutzt Multiindizes. Ein Multiindex ist ein Tupel

$$\underline{k} = (k_1, \ldots, k_n) \in (\mathbb{N}_0)^n,$$

zu dem wir das Monom wie folgt definieren:

$$X^{\underline{k}} := X_1^{k_1} \cdot \ldots \cdot X_n^{k_n}.$$

Ein Element $P \in R[X_1, \ldots, X_n]$ hat dann die Form

$$P = \sum_{\underline{k} \in (\mathbb{N}_0)^n} a_{\underline{k}} X^{\underline{k}}$$

mit eindeutigen $a_{\underline{k}} \in R$, von denen nur endlich viele $\neq 0$ sind.

7.4. **Einheiten.** Bezüglich der Addition ist ein Ring eine (abelsche) Gruppe. Dies gilt nicht für den Ring und die Multiplikation. Ein Inverses bezüglich der Multiplikation fehlt im Allgemeinen.

Definition 7.30. Eine **Einheit** ist ein Ringelement $a \in R$ mit multiplikativem Inversen in R: es gibt ein $b \in R$ mit

$$ab = ba = 1.$$

Satz 7.31. *Für einen Ring R ist die Menge der Einheiten*

$$R^\times = \{a \in R \,;\ \ a \text{ ist Einheit}\}$$

eine Gruppe bezüglich Multiplikation in R. Insbesondere ist das multiplikative Inverse einer Einheit eindeutig. Diese Gruppe heißt ***Einheitengruppe*** *von R.*

Beweis. Die Multiplikation von R schränkt ein zu einer Verknüpfung

$$R^\times \times R^\times \to R^\times, \qquad (a, b) \mapsto ab,$$

denn mit Inversem a^{-1} von a und Inversem b^{-1} von b ist $b^{-1}a^{-1}$ Inverses zu ab.

Offensichtlich ist $1 \in R^\times$, und 1 ist neutrales Element in $R^\times$. Die Existenz in $R^\times$ eines Inversen zu $a \in R^\times$ folgt, weil es per Definition ein $b \in R$ gibt mit $ab = ba = 1$ und aus Symmetriegründen dann auch $b \in R^\times$.

Die Assoziativität der Multiplikation in $R^\times$ folgt trivial aus der Assoziativität der Multiplikation in R. □

Beispiel 7.32. (1) Die Einheiten von $\mathbb{Z}$ sind $\mathbb{Z}^\times = \{1, -1\}$ und als Gruppe isomorph zu $\mathbb{Z}/2\mathbb{Z}$.

(2) Sei G eine Gruppe und K ein Körper. Dann definiert

$$G \to K[G]^\times, \qquad g \mapsto g$$

einen injektiven Gruppenhomomorphismus.

(3) Die Einheiten des Matrizenrings $\mathrm{M}_n(K)$ sind die Gruppe der invertierbaren Matrizen

$$\mathrm{M}_n(K)^\times = \mathrm{GL}_n(K).$$

(4) Sei K ein Körper und $f(X) = a_d X^d + a_{d-1}X^{d-1} + \ldots$ und $g(X) = b_e X^e + b_{e-1}X^{e-1} + \ldots$ Polynome vom Grad d und e, d.h., $a_d \neq 0$ und $b_e \neq 0$. Dann ist

$$(f \cdot g)(X) = a_d b_e X^{d+e} + \text{ Terme kleineren Grades}$$

mit $a_d b_e \neq 0$, weil K ein Körper ist, und damit

$$\deg(fg) = \deg(f) + \deg(g).$$

Insbesondere sind daher die Einheiten genau die konstanten Polynome ungleich 0. Die Einbettung $K \hookrightarrow K[X]$ induziert einen Isomorphismus

$$K^\times \xrightarrow{\sim} (K[X])^\times.$$

Beispiel 7.33. (1) Der Potenzreihenring hat Möglichkeiten, die der Polynomring nicht hat. Etwa hat das Polynom $1 - X \in R[X]$ kein multiplikatives Inverses, wohl aber die formale Potenzreihe $1 - X \in R[[X]]$ das multiplikative Inverse $\sum_{i=0}^\infty X^i$, es gilt nämlich in $R[[X]]$

$$(1 - X) \cdot \sum_{i=0}^{\infty} X^i = 1 + (X - X) + (X^2 - X^2) + \ldots = 1.$$

Dies ist nichts anderes als die geometrische Reihe, die aus der Analysis bekannt ist. Spätestens hier sieht man, daß man mit formalen Potenzreihen *Analysis für Algebraiker* betreibt.

(2) Sei (a_n) die Fibonacci-Folge mit $a_0 = 0$, $a_1 = 1$ und für alle $n \geq 2$

$$a_n = a_{n-1} + a_{n-2}.$$

Wir betrachten die erzeugende Funktion

$$F(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{R}[[X]].$$

Aufgrund der Rekursionsgleichung und $a_0 = 0$ finden wir

$$\begin{aligned}(X + X^2)F(X) &= \sum_{n=1}^{\infty} a_{n-1}X^n + \sum_{n=2}^{\infty} a_{n-2}X^n = \sum_{n=2}^{\infty}(a_{n-1} + a_{n-2})X^n \\ &= \sum_{n=2}^{\infty} a_n X^n = F(X) - X,\end{aligned}$$

oder umgeformt

$$F(X) \cdot (1 - X - X^2) = X.$$

Nun sind die Lösungen der quadratischen Gleichung $T^2 - T - 1 = 0$ gegeben durch

$$\varphi = \frac{1+\sqrt{5}}{2}, \qquad \bar{\varphi} = \frac{1-\sqrt{5}}{2},$$

so daß nach Vieta $T^2 - T - 1 = (T - \varphi)(T - \bar{\varphi})$ beziehungsweise

$$1 - X - X^2 = (1 - \varphi X)(1 - \bar{\varphi}X).$$

Nun haben die Faktoren der Form $1 - \alpha X$ in $\mathbb{R}[[X]]$ das Inverse $\sum_{n=0}^{\infty} \alpha^n X^n$. Damit können wir weiter nach $F(X)$ auflösen:

$$F(X) = X \cdot \Big(\sum_{n=0}^{\infty} \varphi^n X^n\Big) \cdot \Big(\sum_{n=0}^{\infty} (\bar{\varphi})^n X^n\Big) = \sum_{n=0}^{\infty} \Big(\sum_{r+s=n-1} \varphi^r \bar{\varphi}^s\Big) \cdot X^n.$$

Koeffizientenvergleich liefert nun die geschlossene Formel für die Fibonacci-Folge

$$a_n = \sum_{r+s=n-1} \varphi^r \bar{\varphi}^s = \frac{\varphi^n - \bar{\varphi}^n}{\varphi - \bar{\varphi}} = \frac{1}{\sqrt{5}}\Big(\big(\frac{1+\sqrt{5}}{2}\big)^n - \big(\frac{1-\sqrt{5}}{2}\big)^n\Big).$$

Definition 7.34. Sei R ein Ring. Wir sagen Elemente $a, b \in R$ sind assoziiert, wenn

$$a \sim b : \Longleftrightarrow \exists \varepsilon \in R^\times \text{ mit } a = \varepsilon b.$$

Lemma 7.35. *Assoziiert zu sein ist eine Äquivalenzrelation.*

Beweis. Das ist eine einfache Übungsaufgabe. □

Definition 7.36. Ein **Schiefkörper** ist ein Ring R mit $R^\times = R \setminus \{0\}$ und $0 \neq 1$.
Ein **Körper** ist ein abelscher Schiefkörper.

Beispiel 7.37. Die Quaternionen $\mathbb{H}$, die man als Unterring

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix} \; ; \; z, w \in \mathbb{C} \right\} \subseteq \mathrm{M}_2(\mathbb{C})$$

definieren kann, bilden einen nichtkommutativen Schiefkörper. Die Determinante auf $\mathrm{M}_2(\mathbb{C})$ schränkt ein zu einer multiplikativen Abbildung, der (reduzierten) Norm

$$\mathrm{Nrd} : \mathbb{H} \to \mathbb{R}, \qquad \mathrm{Nrd}\Big(\begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix}\Big) = |z|^2 + |w|^2.$$

Wenn $x = \begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix} \neq 0$, dann ist auch $\mathrm{Nrd}(x) \neq 0$. Offensichtlich ist damit das Inverse zu x durch das folgende Quaternion gegeben:

$$\frac{1}{|z|^2 + |w|^2} \begin{pmatrix} \bar{z} & \bar{w} \\ -w & z \end{pmatrix}.$$

Die Quaternionen bilden einen $\mathbb{R}$-Untervektorraum von $\mathrm{M}_2(\mathbb{C})$ und

$$\dim_{\mathbb{R}} \mathbb{H} = 4.$$

Die übliche $\mathbb{R}$-Basis ist

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Jedes Quaternion $x \in \mathbb{H}$ ist also von der Form

$$x = a + bi + cj + dk$$

mit eindeutigen $a, b, c, d \in \mathbb{R}$. Die Addition ist die des $\mathbb{R}$-Vektorraums

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k.$$

Die Multiplikation ist durch $\mathbb{R}$-lineare Fortsetzung bestimmt durch die Werte

$$i^2 = j^2 = k^2 = -1, \text{ und } ij = k = -ji.$$

Übungsaufgaben zu §7

Übungsaufgabe 7.1. Sei R ein Ring und X eine nichtleere Menge. Man überlege sich für den Ring $\mathrm{Abb}(X, R)$ das Nullelement, die Eins und das inverse Element zu einem $f : X \to R$.

Übungsaufgabe 7.2. Sei R ein Ring und R^{op} die gleiche Menge R mit Addition von R und Multiplikation $\cdot^{\mathrm{op}}$ definiert durch

$$a \cdot^{\mathrm{op}} b = ba$$

für alle $a, b \in R$. Zeigen Sie, daß R^{op} ein Ring ist.

Übungsaufgabe 7.3. Sei R ein Ring. Berechnen Sie in $R[[X]]$ das Produkt $(1 - X) \cdot \sum_{i=0}^{\infty} X^i$.

Übungsaufgabe 7.4. Sei A eine Menge und zu $\alpha \in A$ ein Ring R_α gegeben. Dann definiert komponentenweise Addition und Multiplikation eine Ringstruktur auf dem Produkt

$$\prod_{\alpha \in A} R_\alpha.$$

(1) Zeigen Sie, daß für jedes $\beta \in A$ die Projektion

$$\mathrm{pr}_\beta : \prod_{\alpha \in A} R_\alpha \to R_\beta$$

definiert durch

$$\mathrm{pr}_\beta((x_\alpha)_{\alpha \in A}) = x_\beta$$

ein Ringhomomorphismus ist.

(2) Zeigen Sie, daß zu Ringhomomorphismen $f_\alpha : S \to R_\alpha$ für alle $\alpha \in A$ genau ein Ringhomomorphismus

$$f : S \to \prod_{\alpha \in A} R_\alpha$$

existiert mit $\mathrm{pr}_\alpha \circ f = f_\alpha$ für alle $\alpha \in A$.

Zeigen Sie, daß $\prod_{\alpha \in A} R_\alpha$ mit den pr_α bis auf eindeutige Isomorphie durch diese Eigenschaft bestimmt ist.

(3) Zeigen Sie, daß die Abbildungen

$$i_\beta : R_\beta \to \prod_{\alpha\in A} R_\alpha$$
$$x \mapsto (0,\dots,0,\underset{\uparrow\beta}{x},0\dots,0)$$

keine Ringhomomorphismen sind.

Übungsaufgabe 7.5. Zeigen Sie, daß es für jeden Ring R genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt.

Übungsaufgabe 7.6. Sei K ein Körper. Wir betrachten im Potenzreihenring $K[[X]]$ die Teilmenge

$$R = \{f = \sum_{i=0}^{\infty} a_i X^i \ ; \ a_i \in K \text{ für alle } i \geq 0 \text{ und } a_1 = 0\} \subseteq K[[X]]$$

der Potenzreihen ohne linearen Term. Zeigen Sie, daß R ein Unterring ist.

Übungsaufgabe 7.7. Welches sind die invertierbaren Elemente in $\mathrm{Abb}(X,R)$ und wie sieht die Gruppenstruktur auf $\mathrm{Abb}(X,R)^\times$ aus?

Übungsaufgabe 7.8. Bestimmen Sie die Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$: zeigen Sie

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{d + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \ ; \ d \text{ und } n \text{ sind teilerfremd}\}.$$

Wieviele Elemente hat sie?

Übungsaufgabe 7.9. Sei $\mathrm{Aut}_{\mathrm{Gruppe}}(\mathbb{Z}/n\mathbb{Z})$ die Gruppe der Automorphismen von $\mathbb{Z}/n\mathbb{Z}$ als Gruppe. Beschreiben Sie einen Isomorphismus.

$$\mathrm{Aut}_{\mathrm{Gruppe}}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times.$$

Bestimmen Sie die Automorphismen von $\mathbb{Z}/n\mathbb{Z}$ als Ring.

Übungsaufgabe 7.10. Sei K ein Körper. Wir definieren $K[\varepsilon]$ als 2-dimensionalen K-Vektorraum mit Basis $1, \varepsilon$ und schreiben die Vektoren mit Koordinaten $a, b \in K$ bezüglich dieser Basis als $a + b\varepsilon$. Dann definieren wir eine Addition

$$(a + b\varepsilon) + (c + d\varepsilon) = (a + c) + (b + d)\varepsilon$$

und eine Multiplikation

$$(a + b\varepsilon)(c + d\varepsilon) = ac + (bc + ad)\varepsilon.$$

Zeigen Sie, daß $K[\varepsilon]$ ein Ring ist und $\varepsilon \neq 0$ mit $\varepsilon^2 = 0$.

Sei R ein Ring und $\varphi : R \to K[\varepsilon]$ ein Ringhomomorphismus. Wir schreiben φ in Koordinaten für $f \in R$ als

$$\varphi(f) = f(0) + \partial f \varepsilon$$

mit $f(0) \in K$ und $\partial f \in K$. Zeigen Sie, daß

$$f \mapsto f(0)$$

ein Ringhomomorphismus $R \to K$ ist und für $f, g \in R$ gilt

$$\partial(fg) = f(0)\partial g + g(0)\partial f.$$

Anmerkung: Die Notation f für ein Element ist suggestiv für einen Ring von Funktionen R. Die Notation $f(0)$ suggeriert eine Auswertung, ist aber rein formal nur eine Notation für die erste Komponente. Die Notation ∂f suggeriert eine Ableitung, ist aber rein formal nur eine Notation für die zweite Komponente. Das $\varepsilon \in K[\varepsilon]$ ist die algebraische Variante einer infinitesimal kleinen Zahl.

8. Ideale und Quotienten

Ab jetzt betrachten wir nur noch kommutative Ringe mit Eins!

8.1. **Ideale und Faktorringe.** Das Bild eines Ringhomomorphismus $f : R \to S$ ist ein Unterring. Da wir Ringe mit 1 betrachten, gilt dasselbe **nicht** für den **Kern** von f

$$\ker(f) = \{a \in R \; ; \; f(a) = 0\}.$$

Was ist der Kern für eine Teilmenge?

Definition 8.1. Ein **Ideal** ist eine Teilmenge I eines Rings R, die

(i) eine Untergruppe bezüglich Addition ist,
(ii) und für alle $x \in I$ und $a \in R$ gilt $ax \in I$.

Lemma 8.2. *Eine Teilmenge I eines Rings R ist ein Ideal genau dann, wenn*

(i) $I \neq \emptyset$,
(ii) *für alle $x, y \in I$ ist $x + y \in I$,*
(iii) *und für alle $x \in I$ und $a \in R$ gilt $ax \in I$.*

Beweis. Wir müssen nachweisen, daß ein $I \subseteq R$ wie im Lemma mit (i)–(iii) eine Untergruppe von $(R, +)$ ist. Aus dem Untergruppenkriterium fehlt nur die Existenz des Inversen. Zu $x \in I$ ist aber nach (iii) auch

$$-x = (-1)x \in I. \qquad \square$$

Proposition 8.3. *Der Kern eines Ringhomomorphismus $f : R \to S$ ist ein Ideal.*

Beweis. Seien $x, y \in \ker(f)$ und $a \in R$. Dann gilt

$$\begin{aligned} f(x + y) &= f(x) + f(y) = 0 \\ f(ax) &= f(a)f(x) = f(a)0 = 0. \end{aligned}$$

Damit ist auch $x + y, ax \in \ker(f)$. Außerdem ist $0 \in \ker(f) \neq \emptyset$. Lemma 8.2 zeigt, daß $\ker(f)$ ein Ideal ist. $\square$

Proposition 8.4. *Ein Ringhomomorphismus $f : R \to S$ ist injektiv* $\iff \ker(f) = \{0\}$.

Beweis. Ob f injektiv ist, hängt nicht von der Multiplikation ab. Es reicht, f als Gruppenhomomorphismus $f : (R, +) \to (S, +)$ zu betrachten. Dann folgt die Aussage sofort aus der Aussage für Gruppen, Proposition 2.26. $\square$

Lemma 8.5. *Sei A eine Menge und für jedes $\alpha \in A$ ein Ideal I_α im Ring R gegeben. Dann ist der Schnitt ein Ideal von R:*

$$I = \bigcap_{\alpha \in A} I_\alpha.$$

Beweis. Das ist eine einfache Übungsaufgabe. $\square$

Lemma 8.6. *Sei für jedes $n \in \mathbb{N}$ ein Ideal I_n im Ring R gegeben, so daß diese eine aufsteigende Kette*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

bilden. Dann ist die Vereinigung ein Ideal von R:

$$I = \bigcup_{n \in \mathbb{N}} I_n.$$

Beweis. Das ist eine einfache Übungsaufgabe. $\square$

Definition 8.7. Seien R ein Ring und $M \subseteq R$ eine Teilmenge. Das von M **erzeugte Ideal** ist

$$(M) = \{a_1x_1 + \ldots + a_nx_n \ ; \ \exists n \in \mathbb{N}_0, a_i \in R, x_i \in M \text{ für } 1 \leq i \leq n\}\,.$$

Für eine endliche Menge $M = \{x_1, \ldots, x_n\}$ schreiben wir

$$(x_1, \ldots, x_n).$$

Wir überlegen uns, daß (M) ein Ideal ist: Die Menge der R-Linearkombinationen ist abgeschlossen unter Addition (klar) und Multiplikation mit Elementen von R:

$$r(a_1x_1 + \ldots + a_nx_n) = (ra_1)x_1 + \ldots + (ra_n)x_n \in (M)$$

mit $a_i \in R$ und $x_i \in M$ für alle $1 \leq i \leq n$ und $r \in R$. Da überdies $0 \in (M)$ als Wert der R-Linearkombination aus 0 Summanden, ist (M) ein Ideal nach Lemma 8.2.

Offensichtlich ist (M) das kleinste Ideal in R bezüglich Inklusion, das die Menge M enthält:

$$(M) = \bigcap_{M \subseteq I,\ I \text{ Ideal in } R} I.$$

Wenn $(M) = I$ für ein Ideal $I \subseteq R$, dann nennen wir die Menge $M \subseteq R$ ein **Erzeugendensystem** von I, und die Elemente von M heißen **Erzeuger** von I.

Beispiel 8.8. (1) Im Ring $\mathbb{Z}$ ist für jedes $n \in \mathbb{Z}$ die von n erzeugte Untergruppe ein Ideal

$$(n) = n\mathbb{Z} = \{na \ ; \ a \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Dies sind demnach alle Ideale von $\mathbb{Z}$, denn es gibt ja schon keine anderen Untergruppen.

(2) In jedem Ring R sind $(0) = \{0\}$ und $(1) = R$ Ideale. Die Ideale $\neq (0), (1)$ von R heißen **echte Ideale** von R.

(3) Im Ring $\mathbb{Z}[X]$ haben wir das Ideal

$$(2, X) = \{f \ ; \ f \text{ der Form } \sum_{i=0}^{d} a_iX^i \ ; \ a_i \in \mathbb{Z} \text{ für alle } i > 0 \text{ und } a_0 \in 2\mathbb{Z}\}.$$

Bemerkung 8.9. In $\mathbb{Z}$ sind Ideale sehr nahe an den Zahlen, also den Elementen. Ideale können nur nicht zwischen n und $-n$ unterscheiden: $(n) = (-n)$. Historisch entstanden Ideale aus dem Versuch, für Erweiterungen von $\mathbb{Z}$ zu Zahlbereichen in $\mathbb{C}$ die guten Eigenschaften von $\mathbb{Z}$ zu erhalten (eindeutige Faktorisierung in Primfaktoren). Das Wort 'Ideal' erinnert dabei an 'ideale Zahl'.

Die Vorstellung, Ideale seien 'ideale Zahlen', ist allerdings im allgemeinen Fall irreführend.

Satz 8.10 (Faktorring)**.** *Sei $I \subseteq R$ ein Ideal im Ring R. Dann existiert auf der Faktorgruppe R/I eine eindeutige Ringstruktur, so daß die Quotientenabbildung*

$$p : R \to R/I$$

ein Ringhomomorphismus ist. Es gilt dann $I = \ker(p)$.

*Der Ring R/I wird **Faktorring** von R nach I genannt, und $p : R \to R/I$ heißt **kanonische Projektion** oder **Quotientenabbildung**.*

Beweis. Als Homomorphismus abelscher Gruppen gibt es $p : R \to R/I$ und $\ker(p) = I$. Es bleibt zu zeigen, daß wir auf R/I eine verträgliche Ringstruktur definieren können. Da p surjektiv ist und ein Ringhomomorphismus sein soll, haben wir keine Wahl, als für alle $a, b \in R$ zu definieren:

$$(a + I) \cdot (b + I) := ab + I.$$

Es ist nur zu zeigen, daß diese Multiplikation wohldefiniert ist. Alle anderen Ringaxiome gelten automatisch: sie werden via p von R geerbt. (Das überlege man sich!)

Aus Symmetriegründen reicht es, einen Faktor durch einen anderen Repräsentanten auszudrücken. Sei $a + I = a' + I$, also $x = a - a' \in I$. Dann gilt

$$ab = (a' + x)b = a'b + xb \in a'b + I,$$

und die Nebenklassen $ab + I$ und $a'b + I$ sind nicht disjunkt, also gleich. Dies zeigt, daß die Multiplikation auf R/I wohldefiniert ist. □

Korollar 8.11. *Jedes Ideal ist der Kern eines geeigneten Ringhomomorphimus.*

Beweis. Sofort aus Satz 8.10. □

Beispiel 8.12. Der Faktorring $\mathbb{Z}/n\mathbb{Z}$ von $\mathbb{Z}$ nach dem Ideal $(n) = n\mathbb{Z}$ ist der Ring der Restklassen modulo n. Addiert und multipliziert wird in $\mathbb{Z}/n\mathbb{Z}$ durch Addition und Multiplikation von Vertretern. Daß dies alles wohldefiniert ist, dafür sorgt Satz 8.10.

Notation 8.13. Wir übertragen die Notation der Kongruenz von $\mathbb{Z}/n\mathbb{Z}$ auf beliebige Faktorringe R/I. Für $a, b \in R$ gilt dann

$$a \equiv b \pmod{I} \iff a + I = b + I \in R/I \iff a - b \in I.$$

Beispiel 8.14. Das folgende Beispiel zeigt, wie man die Existenz von Nullstellen erzwingen kann.

(1) Sei K ein Körper und $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom positiven Grades. Mittels eines Faktorrings kann man eine Nullstelle von f erzwingen. Sei $I = (f(X))$ und $L = K[X]/I$. Die Inklusion der Konstanten gefolgt von der Quotientenabbildung

$$K \subseteq K[X] \to L = K[X]/I$$

ist injektiv, weil I keine konstanten Polynome enthält und damit der Kern der Komposition nur aus der 0 besteht. In L schreiben wir für das Bild von X

$$\alpha = X + I.$$

Dann ist α eine Nullstelle von $f(X)$ im folgenden Sinne: $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$ wird repräsentiert von

$$f(X) = \sum_{i=0}^{n} a_i X^i \equiv 0 \pmod{I}.$$

Damit ist $f(\alpha) = 0$ in L.

(2) Im Faktorring $\mathbb{R}[X]/(X^2 + 1)$ hat das Polynom $X^2 + 1$ eine Nullstelle. Wir sehen gleich, zu welchem bekannten Ring $\mathbb{R}[X]/(X^2 + 1)$ isomorph ist, aber man kann es hier vielleicht schon erraten.

8.2. **Quotienten und Isomorphiesätze.**

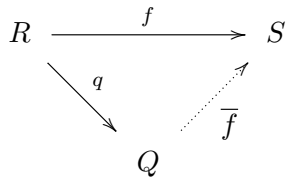
Definition 8.15. Seien R ein Ring und $I \subseteq R$ ein Ideal. Ein **Quotient** für $I \subseteq R$ ist ein Ring Q zusammen mit einem Homomorphismus

$$q : R \to Q,$$

genannt **Quotientenabbildung** oder genauer **Quotientenhomomorphismus**, so daß

(i) $I \subseteq \ker(q)$, und

(ii) für jeden Ringhomomorphismus $f : R \to S$ mit $I \subseteq \ker(f)$ gibt es einen eindeutigen Ringhomomorphismus $\overline{f} : Q \to S$ mit $f = \overline{f} \circ q$, d.h. das Diagramm



kommutiert, und $\overline{f}$ ist der einzige Homomorphismus $Q \to S$, für den das gilt.

Bemerkung 8.16. Wie in Proposition 6.2 im Fall von Gruppen zeigt man die Eindeutigkeit von Quotienten (sofern sie existieren!) bis auf Isomorphismus, der darüberhinaus selbst eindeutig ist, wenn er mit der Quotientenabbildung verträglich ist.

Satz 8.17 (Quotienten)**.** *Seien R ein Ring und $I \subseteq R$ ein Ideal. Dann ist der Faktorring R/I zusammen mit der kanonischen Projektion $p : R \to R/I$ ein Quotient.*

Beweis. Das geht genauso wie im Satz 6.3 im Fall von Gruppen. □

Bemerkung 8.18. Aus Satz 8.17 folgt, daß aufgrund der Eindeutigkeit des Quotienten, Bemerkung 8.16, die Quotientenabbildungen $q : R \to Q$ für Ideale $I \subseteq R$ immer surjektiv sind und $\ker(q) = I$ gilt. Das folgt **nicht** aus der **definierenden universellen Eigenschaft** des Quotienten, sondern aus der **Konstruktion** mittels Faktorring und der Eindeutigkeit.

Proposition 8.19. *Sei $f : R \to S$ ein Ringhomomorphismus.*

(1) Sei $I \subseteq S$ ein Ideal. Dann ist $f^{-1}(I)$ ein Ideal in R.
(2) Sei f surjektiv und $I \subseteq R$ ein Ideal. Dann ist $f(I)$ ein Ideal in S.

Beweis. Das geht genauso wie in Proposition 4.50 im Fall von Gruppen:

(1) Es gilt $f^{-1}(I) = \ker(R \to S \to S/I)$.
(2) Das Bild $f(I)$ ist eine Untergruppe von S. Für alle $b \in S$ gibt es ein $a \in R$ mit $b = f(a)$. Daher gilt auch $bf(I) = f(a)f(I) = f(aI) \subseteq f(I)$. □

Satz 8.20 (Homomorphiesatz)**.** *Sei $f : R \to S$ ein Ringhomomorphismus. Dann induziert f einen Isomorphismus*

$$\bar{f} : R/\ker(f) \xrightarrow{\sim} \operatorname{im}(f), \qquad \bar{f}(a + I) := f(a).$$

Beweis. Der Beweis folgt analog zum Homomorphiesatz für Gruppen, Satz 6.7, aus der Quotienteneigenschaft von R/I, siehe Satz 8.17.

Man kann auch sagen, daß $\bar{f}$ als Abbildung der zugrundeliegenden Gruppen wegen Satz 6.7 existiert und ein Isomorphismus von Gruppen ist. Weiter ist die Multiplikation auf R/I aber genau so definiert, daß $\bar{f}$ sogar ein Ringhomomorphismus und damit Ringisomorphismus ist. □

Beispiel 8.21. Die Struktur eines Faktorrings R/I bestimmt man am besten, indem man einen Isomorphismus $S \simeq R/I$ rät, den entsprechenden surjektiven Homomorphismus $f : R \twoheadrightarrow S$ hinschreibt und dann $I = \ker(f)$ nachweist. Mit dieser Methode bestimmen wir

$$\mathbb{Z}[X]/(2, X) \simeq \mathbb{F}_2.$$

Der surjektive Homomorphismus $\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_2$ ist die Auswertung $X \mapsto 0 \in \mathbb{F}_2$ und auf Koeffizienten die kanonische Projektion $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. In der Tat sind 2 und X im Kern der Auswertung, und genauer $f(0) = 0 \mod 2$ genau dann, wenn der konstante Koeffizient von f gerade ist. Dies beschreibt das Ideal $(2, X)$.

Beispiel 8.22. Aus Satz 7.25 bekommen wir zu $\mathbb{R} \subseteq \mathbb{C}$ einen Ringhomomorphismus

$$\mathbb{R}[X] \to \mathbb{C}, \qquad X \mapsto i,$$

die Auswertung in $i \in \mathbb{C}$. Dieser Homomorphismus ist surjektiv mit Kern $(X^2 + 1)$, woraus sich nach dem Homomorphiesatz der folgende Isomorphismus ergibt:

$$\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}.$$

Es lassen sich auch die Isomorphiesätze übertragen. Die Beweise sind formal die gleichen wie bei Gruppen, basierend auf dem Homomorphiesatz bzw. der Quotienteneigenschaft der Faktorringe.

Satz 8.23 (Erster Isomorphiesatz)**.** *Sei $U \subseteq R$ ein Unterring und $I \subseteq R$ ein Ideal.*
Dann ist $U \cap I$ ein Ideal in U und

$$U/(U \cap I) \xrightarrow{\sim} (U + I)/I$$
$$u + (U \cap I) \mapsto u + I$$

ist ein Isomorphismus.

Beweis. Das ist der Homomorphiesatz für den Homomorphismus $U \to R \to R/I$. □

Satz 8.24 (Zweiter Isomorphiesatz)**.** *Sei R ein Ring und seien $I \subseteq J$ Ideale in R. Dann ist*

$$(R/I)/(J/I) \xrightarrow{\sim} R/J$$
$$(a+I)+J \mapsto a+J$$

ein Ringisomorphismus. Insbesondere ist J/I ein Ideal in R/I.

Beweis. Das ist der Homomorphiesatz für den Ringhomomorphismus $R/I \to R/J$, der durch die Quotienteneigenschaft von $R \to R/I$ induziert wird. □

Beispiel 8.25. Sei K ein Körper. Wir betrachten im Ring $K[X,Y]$ das Ideal $J = (X-Y^3, Y-2)$. Zunächst liefert die Auswertung in $y = 2$ einen (offensichtlich surjektiven) Ringhomomorphismus

$$K[X,Y] \to K[X], \qquad X \mapsto X, Y \mapsto 2,$$

also nach dem Homomorphiesatz einen Isomorphismus $K[X,Y]/(Y-2) \simeq K[X]$. Es ist $I = (Y-2) \subseteq J$ und J/I wird in $K[X]$ zum Ideal $(X-8)$. Nach dem zweiten Isomorphiesatz ist dann

$$K[X,Y]/(X-Y^3, Y-2) \simeq K[X]/(X-8).$$

Eine erneute Anwendung des Homomorphiesatzes angewandt auf die Auswertung in $x = 8$ führt zu $K[X]/(X-8) \simeq K$.

9. Hauptidealringe

9.1. **Integritätsringe und Hauptidealringe.** Den Körpern am nächsten kommen die Integritätsringe.

Lemma–Definition 9.1. *Ein **Integritätsring** ist ein Ring mit $1 \neq 0$, in dem die folgenden äquivalenten Bedingungen gelten.*

(a) Die Kürzungsregel gilt, d.h. für alle $a, x, y \in R$ mit $a \neq 0$ gilt

$$ax = ay \quad \Longrightarrow \quad x = y.$$

*(b) Der Ring ist **nullteilerfrei**, d.h. für alle $x, y \in R$ gilt*

$$xy = 0 \quad \Longrightarrow \quad x = 0 \text{ oder } y = 0.$$

Beweis. Es gelte die Kürzungsregel und sei $xy = 0$. Wenn $x = 0$ ist nichts zu tun. Ansonsten gilt $xy = 0 = x0$ und man kann wegen $x \neq 0$ zu $y = 0$ kürzen.

Umgekehrt sei R nun nullteilerfrei. Wenn $a \neq 0$, so folgt aus $ax = ay$, also $a(x-y) = 0$, schon $x - y = 0$ oder eben $x = y$. Das zeigt die Kürzungsregel. □

Beispiel 9.2. (1) Ein Körper ist ein Integritätsring: Sei K ein Körper, $a, x, y \in K$ mit $ax = ay$ und $a \neq 0$. Dann gibt es $a^{-1} \in K$ und so

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

Also erfüllt K die Kürzungsregel.

(2) Jeder Unterring eines Integritätsrings erbt die Kürzungsregel, zum Beispiel jeder Unterring eines Körpers wie etwa $\mathbb{Z} \subseteq \mathbb{Q}$. Dies ist kein Zufall, wie Satz A.1 zeigt.

(3) Sei R ein Ring mit $1 \neq 0$, und es habe die Menge X mindestens 2 Elemente $x_1 \neq x_2$. Dann ist $\mathrm{Abb}(X, R)$ kein Integritätsring. Sei dazu für $i = 1, 2$ die Funktion $f_i : X \to R$ mit

$$f_i(x) = \begin{cases} 1 & x = x_i \\ 0 & x \neq x_i \end{cases}$$

Dann gilt $f_1 \cdot f_2 = 0$, aber beide f_i sind von 0 verschieden.

Die nach den Körpern einfachsten Ringe sind die Hauptidealringe.

Definition 9.3. (1) Ein **Hauptideal** ist ein Ideal I in einem Ring R, das von einem Element erzeugt werden kann: es gibt $a \in R$ mit

$$I = (a) = \{ra \ ; \ r \in R\} = Ra.$$

(2) Ein **Hauptidealring** ist ein Integritätsring, in dem alle Ideale Hauptideale sind.

Beispiel 9.4. (1) Das typische Beispiel ist $\mathbb{Z}$. Ideale sind Untergruppen und damit von der Form (n), also Hauptideale.
(2) Jeder Körper ist ein langweiliges Beispiel. Dort gibt es einfach keine nichttrivialen Ideale. Die trivialen Ideale sind stets Hauptideale.
(3) Sei K ein Körper. Der Polynomring $K[X]$ ist ein Hauptidealring. Dies ist aus der Linearen Algebra bekannt.
(4) Das Ideal $(2, X) \subseteq \mathbb{Z}[X]$ ist kein Hauptideal. Angenommen, $(2, X) = (f)$, dann gibt es $g, h \in \mathbb{Z}[X]$ mit $2 = gf$ und $X = hf$. Betrachtet man f als Polynom in $\mathbb{Q}[X]$, so muß es wegen $2 = gf$ konstant sein, und zwar $f = \pm 1$ wegen $X = hf$. Dann aber erzeugt f schon das triviale Ideal R, Widerspruch. Insbesondere ist $\mathbb{Z}[X]$ kein Hauptidealring.

9.2. **Euklidische Ringe.** Wir formalisieren den Beweis, daß $\mathbb{Z}$ ein Hauptidealring ist, indem wir **Division mit Rest** abstrahieren.

Definition 9.5. Eine **euklidische Gradfunktion** auf einem Ring R ist eine Abbildung

$$\delta : R \setminus \{0\} \to \mathbb{N}_0,$$

so daß es für alle $a \in R$ und $0 \neq d \in R$ Elemente $q, r \in R$ gibt mit

(i) $a = qd + r$,
(ii) $r = 0$ oder $\delta(r) < \delta(d)$.

Ein **euklidischer Ring** ist ein Integritätsring, den man mit einer euklidischen Gradfunktion versehen kann.

Beispiel 9.6. Die ganzen Zahlen $\mathbb{Z}$ sind ein euklidischer Ring mit der euklidischen Gradfunktion $\delta(n) = |n|$, dem reellen Absolutbetrag $|\cdot|$.

Satz 9.7. *Sei K ein Körper.*
(1) Für alle $f, g \in K[X] \setminus \{0\}$ gilt $fg \neq 0$ und

$$\deg(fg) = \deg(f) + \deg(g).$$

Insbesondere ist der Polynomring $K[X]$ ein Integritätsring.
(2) Die Einheiten des Polynomrings sind $K[X]^\times = K^\times$ als konstante Polynome $\neq 0$.

Beweis. (1) Sei $n = \deg(f)$ und $m = \deg(g)$. Dann ist $f = a_n X^n +$ Terme kleineren Grades und $g = b_m X^m +$ Terme kleiner Grades und $a_n, b_m \in K^\times$. Dann ist

$$fg = a_n b_m X^{n+m} + \text{ Terme kleineren Grades.}$$

Weil $a_n b_m \neq 0$, folgt insbesondere $fg \neq 0$ und $\deg(fg) = n + m$.
(2) Wenn $f \in K[X]^\times$, dann gibt es $g \in K[X]$ mit $fg = 1$. Es folgt aus (1), daß $0 = \deg(fg) = \deg(f) + \deg(g)$, somit $\deg(f) = 0$ und f ist konstant. □

Satz 9.8. *Sei K ein Körper. Dann ist der Polynomring $K[X]$ mit dem Grad als euklidischer Gradfunktion ein euklidischer Ring.*

Beweis. Mit $f, g \in K[X]$ verschieden von 0 ist $fg \neq 0$, weil nach Satz 9.7 ja $\deg(fg) = \deg(f) + \deg(g)$ gilt. Insbesondere ist $K[X]$ ein Integritätsring.

Der Nachweis der Division mit Rest basiert auf dem Algorithmus der Polynomdivision. Zu $0 \neq d \in K[X]$ und jedem $f \in K[X]$ müssen wir $q, r \in K[X]$ finden mit

$$f = qd + r$$

und $r = 0$ oder $\deg(r) < \deg(d)$. Für $f = 0$ wählen wir $q = r = 0$ und sind fertig. Wir nehmen daher im Folgenden $f \neq 0$ an.

Wir zeigen die Behauptung per Induktion nach $\deg(f)$. Falls $\deg(f) < \deg(d)$, so wählen wir $q = 0$ und $r = f$, fertig. Wenn $m = \deg(f) \geq n = \deg(d)$, so schreiben wir

$$\begin{aligned} f &= a_m X^m + \dots \text{ Terme kleineren Grades} \\ d &= b_n X^n + \dots \text{ Terme kleineren Grades} \end{aligned}$$

mit $a_m \neq 0 \neq b_n$. Dann ist

$$\begin{aligned} \tilde{f} &= f - \frac{a_m}{b_n} X^{m-n} d \\ &= a_m X^m - \frac{a_m}{b_n} X^{m-n} \cdot b_n X^n + \dots \text{ Terme vom Grad } < m \\ &= \text{ Terme vom Grad } < m \end{aligned}$$

also

$$\deg(\tilde{f}) < \deg(f).$$

Per Induktionsannahme gibt es nun $\tilde{q}, \tilde{r}$ mit $\tilde{f} = \tilde{q}d + \tilde{r}$ und $\tilde{r} = 0$ oder $\deg(\tilde{r}) < \deg(d)$. Wir setzen dann

$$\begin{aligned} q &= \tilde{q} + \frac{a_m}{b_n} X^{m-n} \\ r &= \tilde{r} \end{aligned}$$

und rechnen

$$f = \tilde{f} + \frac{a_m}{b_n} X^{m-n} d = \tilde{q}d + \tilde{r} + \frac{a_m}{b_n} X^{m-n} d = (\tilde{q} + \frac{a_m}{b_n} X^{m-n})d + \tilde{r} = qd + r.$$

Weiterhin erfüllt das Restglied r die geforderten Eigenschaften.

Jetzt kümmern wir uns um den Induktionsanfang: $\deg(f) = 0$. Wenn $\deg(f) < \deg(d)$, dann ist wie oben nichts zu tun. Es fehlt also nur der Fall $\deg(f) = \deg(d) = 0$. Da $d \neq 0$ gibt es also $d^{-1} \in K[X]$ und die Wahl $q = fd^{-1}$ mit $r = 0$ erfüllt die Anforderungen. □

Theorem 9.9. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R ein euklidischer Ring und $\delta : R \setminus \{0\} \to \mathbb{N}_0$ eine euklidische Gradfunktion. Sei $I \subseteq R$ ein Ideal. Für $I = (0)$ ist nichts zu tun. Sei also $I \neq (0)$

Da jede nichtleere Teilmenge von $\mathbb{N}_0$ ein minimales Element hat, gibt es $a \in I$ mit $a \neq 0$ und minimalem euklidischen Grad

$$\delta(a) = \min\{\delta(x) \ ; \ x \in I, x \neq 0\}.$$

Wir zeigen nun $I = (a)$. Sei dazu $x \in I$ beliebig. Dann gibt es $q, r \in R$ mit $x = qa + r$ und $r = 0$ oder $\deg(r) < \deg(a)$. Weil

$$r = x - qa \in I,$$

gilt aber $r = 0$ oder $\deg(r) \geq \deg(a)$ nach Wahl von a. Also muß $r = 0$ gelten. Damit ist $x = qa \in (a)$. Weil dies für jedes $x \in I$ gilt, folgt $I \subseteq (a)$. Die umgekehrte Inklusion gilt wegen $a \in I$. Also gilt $I = (a)$. □

Korollar 9.10. *Der Polynomring $K[X]$ mit Koeffizienten aus einem Körper K ist ein Hauptidealring.*

Beweis. Dies folgt aus Theorem 9.9, da nach Satz 9.8 der Polynomring euklidisch ist. □

Übungsaufgaben zu §9

Übungsaufgabe 9.1. Sei R ein Integritätsring. Bestimmen Sie die Einheitengruppe im Polynomring $R[X]$ und im Potenzreihenring $R[[X]]$.

Übungsaufgabe 9.2. Sei K ein Körper. Zeigen Sie, daß $K[[X]]$ ein Hauptidealring ist. Gibt es eine euklidische Gradfunktion auf $K[[X]]$?

Übungsaufgabe 9.3. Wir betrachten den Unterring $R \subseteq K[[X]]$ aus Aufgabe 7.6 bestehend aus allen Potenzreihen f mit verschwindendem linearen Term. Zeigen Sie, daß das Ideal (X^2, X^3) von R kein Hauptideal in R ist.

10. Arithmetik in Hauptidealringen

10.1. **Teilbarkeit in Integritätsringen.** Über den Unterschied zwischen Elementen und den davon erzeugten Hauptidealen gibt die folgende Proposition Auskunft.

Proposition 10.1. *Sei R ein Ring und $a, b \in R$.*

(1) *Wenn $a \sim b$ (a assoziiert zu b), dann ist $(a) = (b)$.*
(2) $a \in R^\times \iff (a) = R$.
(3) *Sei R ein Integritätsring. Dann gilt* $(a) = (b) \iff a \sim b$.

Beweis. (1) Wenn $a \sim b$, dann gibt es $\varepsilon \in R^\times$ und $a = \varepsilon b$. Aber dann ist

$$(a) = Ra = R\varepsilon b \subseteq (b).$$

Da assoziiert zu sein symmetrisch ist, folgt auch $(b) \subseteq (a)$.

(2) Es gilt per Definition und nach (1)

$$a \in R^\times \iff a \sim 1 \iff (a) = (1) \iff (a) = R.$$

(3) Wegen (1) ist nur zu zeigen, daß mit $(a) = (b)$ die Elemente a, b assoziiert sind. Sei $(a) = (b)$. Dann gibt es $\varepsilon, \delta \in R$ mit $a = \varepsilon b$ und $b = \delta a$. Es folgt

$$a = \varepsilon b = \varepsilon(\delta a) = a(\varepsilon\delta),$$

woraus die Kürzungsregel $\varepsilon\delta = 1$ macht: ε ist eine Einheit. Es gibt eine Ausnahme, nämlich wenn $a = 0$, so daß die Kürzungsregel nicht gilt. Dann muß aber wegen $b \in (a) = (0)$ auch $b = 0$ sein. Dann gilt $a = 1 \cdot b$ mit der Einheit 1. Die Behauptung gilt also in jedem Fall. □

Definition 10.2. Sei R ein Integritätsring und $a, x \in R$. Dann sagt man x **teilt** a oder x **ist Teiler von** a und verwendet die Notation

$$x \mid a,$$

wenn eine (also alle) der folgenden offensichtlich äquivalenten Bedingungen erfüllt sind:

$$\exists y \in R : \ a = xy \iff a \in (x) \iff (a) \subseteq (x).$$

Ansonsten schreiben wir $x \nmid a$, wenn x kein Teiler von a ist.

Proposition 10.3 (Eigenschaften der Teilerrelation)**.** *Seien a, a', b, c, x, x' Elemente eines Integritätsrings R. Dann gilt:*

(1) $1 \mid a$.
(2) $x \mid 0$.
(3) $x \mid 1 \iff x \in R^\times$.
(4) *Wenn $x \mid a$, dann gilt $xb \mid ab$. Und wenn $b \neq 0$, dann folgt aus $xb \mid ab$ auch $x \mid a$.*
(5) $a \mid b$ *und* $b \mid c \Longrightarrow a \mid c$.
(6) *Seien $a_1, \ldots, a_n$ Elemente von R. Dann folgt aus $x \mid a_i$ für alle i, daß für alle $b_i \in R$, für $1 \leq i \leq n$ auch*

$$x \mid b_1 a_1 + \ldots + b_n a_n.$$

(7) *Sind $a \sim a'$ und $x \sim x'$ jeweils assoziiert, dann gilt*

$$x \mid a \iff x' \mid a'.$$

(8) $(a \mid b$ *und* $b \mid a) \iff (a) = (b) \iff a \sim b$ *sind assoziiert.*

Beweis. (1) $a \in (1) = R$.
(2) $0 \in (x)$.
(3) Proposition 10.1 (2).
(4) Wenn $x \mid a$, dann gibt es $y \in R$ mit $a = xy$. Dann auch $ab = xby$, somit $xb \mid ab$. Wenn $b \neq 0$, zeigt die Kürzungsregel auch die umgekehrte Implikation.
(5) Nach Voraussetzung gibt es $x, y \in R$ mit $b = ax$ und $c = by$. Dann ist $c = a(xy)$ und $a \mid c$.
(6) Es gibt y_i mit $a_i = xy_i$ für alle $1 \leq i \leq n$. Dann gilt
$$x \mid x(b_1y_1 + \ldots + b_ny_n) = b_1a_1 + \ldots + b_na_n.$$
(7) Nach Proposition 10.1 gilt $(a) = (a')$ und $(x) = (x')$. Dann folgt
$$x \mid a \iff (a) \subseteq (x) \iff (a') \subseteq (x') \iff x' \mid a'.$$
(8) Es gilt $a \mid b$ und $b \mid a$ genau dann, wenn $(b) \subseteq (a)$ und $(a) \subseteq (b)$, was äquivalent ist zu $(a) = (b)$. Dies ist nach Proposition 10.1 dasselbe wie $a \sim b$. □

10.2. **Primelemente und irreduzible Elemente.**

Definition 10.4. Ein Element $a \neq 0$ eines Rings R heißt **irreduzibel**, wenn
(i) a keine Einheit ist und
(ii) aus $a = xy$ für $x, y \in R$ folgt $x \in R^\times$ oder $y \in R^\times$.

Beispiel 10.5. (1) Die positiven irreduziblen Elemente von $\mathbb{Z}$ sind genau die **Primzahlen** (per Definition).
(2) Ein lineares Polynom $X - a \in K[X]$ ist irreduzibel, denn in einer Zerlegung $X - a = f(x)g(X)$ hat einer der Faktoren Grad 0 und ist daher eine Einheit.
(3) Ein Polynom $f \in K[X]$ vom Grad $\deg(f) \geq 2$ mit Nullstelle $a \in K$ ist nicht irreduzibel. Polynomdivision von f durch $X - a$ liefert
$$f = q(X - a) + r$$
mit $r(a) = f(a) - q(a)(a - a) = 0$. Da $r = 0$ oder $\deg(r) < \deg(X - a) = 1$, ist r konstant und in jedem Fall 0. Damit hat f den Faktor $X - a$ und $\deg(q) = \deg(f) - \deg(X - a) > 0$ zeigt, daß $q \notin K[X]^\times$.

Definition 10.6. Ein **Primelement** ist ein Element $\pi \neq 0$ eines Rings R, das keine Einheit ist, und für alle $x, y \in R$
$$\pi \mid xy \quad \Longrightarrow \quad \pi \mid x \quad \text{oder} \quad \pi \mid y.$$
Man sagt dann auch, π ist **prim**.

Bemerkung 10.7. Sind $p \sim q$ assoziierte Elemente in R, dann folgt aus Proposition 10.3 (7)
$$p \text{ ist Primelement} \iff q \text{ ist Primelement.}$$
Für ein Primelement $p \in R$ und eine Einheit $u \in R^\times$ ist damit auch $q = up$ ein Primelement.

Proposition 10.8. *Sei R ein Integritätsring. Dann ist jedes Primelement irreduzibel.*

Beweis. Sei π ein Primelement und $\pi = xy$ eine beliebige Zerlegung. Dann gilt $\pi \mid xy$ und oBdA $\pi \mid x$. Es gibt also $z \in R$ mit $\pi z = x$. Dann ist $\pi zy = xy = \pi = \pi \cdot 1$ und Kürzen von π zeigt $zy = 1$. Damit ist y eine Einheit. □

Der folgende Satz und der Fall der Primelemente in $\mathbb{Z}$, nämlich der Primzahlen, rechtfertigt den Namen Primelement.

Satz 10.9. *Seien R ein Hauptidealring und $a \in R$, $a \neq 0$, $a \notin R^\times$. Dann sind äquivalent:*
(i) *a ist Primelement.*
(ii) *a ist irreduzibel.*
(iii) *$R/(a)$ ist ein Körper.*

(iv) $R/(a)$ *ist ein Integritätsring.*

Beweis. Wir zeigen (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) $\Longrightarrow$ (i). Dabei ist (i) $\Longrightarrow$ (ii) die Aussage von Proposition 10.8, und (iii) $\Longrightarrow$ (iv) ist trivial.

(ii) $\Longrightarrow$ (iii): Es ist $0 \neq 1$ in $R/(a)$, weil sonst $R/(a) = 0$ nach Lemma 7.8, also $R = (a)$ und gleichbedeutend $a \in R^\times$ nach Proposition 10.1.

Sei $0 \neq \bar{x} = x + (a) \in R/(a)$. Wir müssen ein Inverses zu $\bar{x}$ finden. Da $\bar{x} \neq 0$, gilt $x \notin (a)$, also ist (a, x) echt größer als (a). Da R ein Hauptidealring ist, gibt es ein $b \in R$ mit

$$(b) = (a, x).$$

Damit gibt es ein $c \in R$ mit $a = bc$. Weil a irreduzibel ist, muß einer der beiden Faktoren b oder c eine Einheit sein. Wenn $c \in R^\times$, dann gibt es einen Widerspruch durch

$$(b) = (ac^{-1}) = (a) \subsetneq (a, x) = (b).$$

Also muß $b \in R^\times$ Einheit sein. Dann ist $R = (b) = (a, x)$ und es gibt $\alpha, y \in R$ mit

$$1 = \alpha a + yx.$$

Dann gilt in $R/(a)$ (mit der Notation $\bar{y} = y + (a)$):

$$\bar{x}\bar{y} = (x + (a))(y + (a)) = xy + (a) = 1 + (a) = 1 \in R/(a).$$

Damit ist $\bar{y}$ das gesuchte Inverse zu $\bar{x}$.

(iv) $\Longrightarrow$ (i): Sei $R/(a)$ ein Integritätsring und $a \mid xy$. Wir setzen $\bar{x} = x + (a)$ und $\bar{y} = y + (a)$ für die Bilder in $R/(a)$. Dann ist in $R/(a)$

$$\bar{x} \cdot \bar{y} = (x + (a))(y + (a)) = xy + (a) = (a) = 0 \in R/(a).$$

Da $R/(a)$ nullteilerfrei ist, muß $\bar{x} = 0$ oder $\bar{y} = 0$ gelten. OBdA sei $\bar{x} = 0$, also $x \in (a)$, also $a \mid x$. Damit ist a ein Primelement. □

Bemerkung 10.10. Wir brauchen Satz 10.9 im Beweis von Korollar 10.11, weil wir mit der traditionellen Definition einer Primzahl arbeiten, anstatt von Primelementen in $\mathbb{Z}$ zu sprechen. Beides ist äquivalent, erfordert aber den Satz 10.9.

Die Äquivalenz (i) $\Longleftrightarrow$ (ii) in Satz 10.9 geht im Spezialfall $R = \mathbb{Z}$, also der Primzahlen, auf Euklid zurück.

Korollar 10.11. *Sei $n > 0$ eine ganze Zahl. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper genau dann, wenn n eine Primzahl ist.*

Beweis. Das folgt sofort aus Satz 10.9 und der Definition einer Primzahl. □

Notation 10.12. Für eine Primzahl p bezeichnen wir $\mathbb{Z}/p\mathbb{Z}$ der Deutlichkeit halber mit

$$\mathbb{F}_p,$$

wenn wir den **endlichen Körper** und nicht nur die zugrundeliegende additive zyklische Gruppe meinen.

Korollar 10.13. *Sei K ein Körper und $f(X) \in K[X]$ ein irreduzibles Polynom. Dann ist*

$$L = K[X]/(f(X))$$

ein Körper.

*(1) Genauer ist L ein **Oberkörper** von K über die Einbettung $K \subseteq L$ durch die Restklassen konstanter Polynome.*

(2) In L hat $f(X)$ die Nullstelle $\alpha \equiv X \pmod{f(X)}$.

(3) Jede Restklasse $P + (f(X)) \in L = K[X]/(f(X))$ hat einen eindeutigen Repräsentanten $P \in K[X]$ vom Grad $\deg(P) < \deg(f)$. (Hier setzen wir $\deg(0) = -\infty$.)

(4) *Die Einschränkung der Multiplikation auf $K \times L \to L$ macht aus L einen K-Vektorraum der Dimension $\dim_K(L) = \deg(f)$ mit den Restklassen zu*

$$1, X, X^2, \ldots, X^{\deg(f)-1}$$

als Basis.

Beweis. (1) Das folgt sofort aus Satz 10.9 (ii) $\iff$ (iii) und (2) wurde in Beispiel 8.14 behandelt. (3) folgt aus Division mit Rest in $K[X]$ aus dem Beweis von Satz 9.8 und in (4) ist die Verifikation der Vektorraumaxiome eine Übungsaufgabe. Die Beschreibung der Basis folgt sofort aus (3). □

Beispiel 10.14. Das Polynom $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$ ist irreduzibel. Ansonsten hätte X^2+X+1 einen Linearfaktor in $\mathbb{F}_2[X]$ und folglich eine Nullstelle in $\mathbb{F}_2$. Aber dies schließt man durch Ausprobieren aus: $f(0) = f(1) = 1$. Der Körper

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$$

hat 4 Elemente, denn Division mit Rest zeigt, daß jede Restklasse einen eindeutigen Vertreter in $\mathbb{F}_2[X]$ vom Grad ≤ 1 hat. Davon gibt es 4.

Man kann zu jeder Primzahl p und einer Potenz $q = p^d$ ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ vom Grad $d = \deg(f)$ finden, so daß

$$\mathbb{F}_q \simeq \mathbb{F}_p[X]/(f)$$

ein Körper mit q Elementen ist. Man kann weiter zeigen, daß $\mathbb{F}_q$ bis auf Isomorphie eindeutig durch q gegeben ist und die Mächtigkeit eines endlichen Körpers stets eine Primzahlpotenz sein muß. Damit hat man einen vollständigen Überblick über die Klassifikation endlicher Körper. Mehr dazu in der Vorlesung Algebra.

10.3. **Die Eindeutigkeit der Primzerlegung in Hauptidealringen.** Wir zerlegen zuerst als Produkt von irreduziblen Elementen, obwohl nach Satz 10.9 irreduzibel und prim in Hauptidealringen äquivalent sind, weil der Existenzbeweis mit der Eigenschaft ‚irreduzibel' spielt.

Lemma 10.15. *Sei R ein Integritätsring und $a, x, y \in R$ mit $a = yx \neq 0$. Wenn $(a) = (x)$, dann ist $y \in R^\times$.*

Beweis. Wegen $(a) = (x)$ gibt es $z \in R$ mit $x = az$. Dann folgt $a = a(yz)$ und wegen $a \neq 0$ bereits $1 = yz$. Dies zeigt $y \in R^\times$. □

Satz 10.16. *Sei R ein Hauptidealring. Dann läßt sich jedes $0 \neq a \in R$ als Produkt einer Einheit und endlich vieler irreduzibler Elemente schreiben.*

Beweis. Schritt 1: Wir betrachten die Menge der Gegenbeispiele

$$\mathscr{M} = \{x \in R \,;\, x \neq 0 \text{ nicht der Form } x = u \cdot \prod_{i=1}^{n} p_i \text{ mit } u \in R^\times,\ p_i \text{ irreduzibel in } R\}$$

und zeigen, daß $\mathscr{M}$ leer ist. Wir führen einen Widerspruchsbeweis und nehmen $\mathscr{M} \neq \emptyset$ an.

Schritt 2: Angenommen, es gibt unter den Hauptidealen (x) zu $x \in \mathscr{M}$ kein bezüglich Inklusion maximales Ideal, dann gibt es echte unendlich aufsteigende Ketten

$$(x_1) \subsetneq (x_2) \subsetneq \ldots \subsetneq (x_i) \subsetneq \ldots$$

mit $x_i \in \mathscr{M}$ für alle $i \geq 1$. Da R Hauptidealring ist, gibt es $x \in R$ mit

$$(x) = \bigcup_{i \geq 1} (x_i),$$

denn die Vereinigung ist nach Lemma 8.6 ein Ideal. Für hinreichend großes j muß schon $x \in (x_j)$ gelten. Daraus folgt für $i > j$

$$\bigcup_{i \geq 1} (x_i) = (x) \subseteq (x_j) \subsetneq (x_i) \subseteq \bigcup_{i \geq 1} (x_i),$$

ein Widerspruch. Es gibt also maximale Gegenbeispiele.

Schritt 3: Sei $a \in \mathscr{M}$ ein maximales Gegenbeispiel, d.h. für alle $(a) \subsetneq (y)$ gilt $y \notin \mathscr{M}$. Dann kann a weder Einheit noch irreduzibel sein, denn a wäre ein Produkt (mit höchstens einem Faktor) von irreduziblen Elementen.

Sei also $a = xy$ eine nichttriviale Zerlegung mit $x, y \notin R^\times$. Dann ist $(a) \subsetneq (x)$ eine echte Inklusion, da sonst y Einheit wäre nach Lemma 10.15. Entsprechend ist $(a) \subsetneq (y)$ eine echte Inklusion. Also sind $x, y \notin \mathscr{M}$. Es gibt daher Zerlegungen

$$x = u \cdot p_1 \cdot \ldots \cdot p_n$$
$$y = v \cdot q_1 \cdot \ldots \cdot q_m$$

für irreduzible Elemente $p_1, \ldots, p_n, q_1, \ldots, q_m$ von R und $u, v \in R^\times$. Daraus folgt die Zerlegung

$$a = xy = (uv) \cdot p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m$$

im Widerspruch zu $a \in \mathscr{M}$. Es kann keine Gegenbeispiele zur Aussage des Satzes geben. □

Bemerkung 10.17. Sei K ein Körper. Im Polynomring $K[X]$ kann man Satz 10.16 leicht per Induktion über den Grad beweisen. Für $\deg(f) \leq 0$ handelt es sich um 0 oder eine Einheit. Für $\deg(f) > 0$ ist entweder f irreduzibel, dann ist nach Satz 10.9 f prim und nichts zu tun. Andernfalls ist f nicht irreduzibel und wir können $f = gh$ mit $g, h \notin K[X]^\times$ schreiben. Nach Satz 9.7 folgt $\deg(g), \deg(h) > 0$ und $\deg(f) = \deg(g) + \deg(h)$, also

$$\deg(g), \deg(h) < \deg(f),$$

und die Induktionsannahme findet auf g, h Anwendung. Eine Zerlegung für g und h als Produkt irreduzibler Polynome kann man zu einer Faktorzerlegung von f multiplizieren.

Der Satz über die Eindeutigkeit der Primfaktorzerlegung ist schon sehr alt (Euklid für $R = \mathbb{Z}$). In Hauptidealringen gilt der Satz allgemein. Nicht aber in beliebigen Ringen als Satz über eindeutige Faktorisierung in irreduzible Elemente, wie das klassische Beispiel in

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \ ; \ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

zeigt[10] mit den zwei echt verschiedenen Faktorisierungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Theorem 10.18 (Eindeutige Primfaktorzerlegung in Hauptidealringen)**.** *Sei R ein Hauptidealring und $a \in R$, $a \neq 0$. Dann hat a eine Produktzerlegung*

$$a = u \cdot p_1 \cdot \ldots \cdot p_n$$

in Primelemente p_i für $1 \leq i \leq n$ und eine Einheit u.

Die Zerlegung ist eindeutig bis auf Permutation und assoziierte Primelemente. Genauer, sei

$$a = v \cdot q_1 \cdot \ldots \cdot q_m$$

eine zweite solche Faktorisierung mit $v \in R^\times$ und q_j prim für $1 \leq j \leq m$. Dann gilt $m = n$ und es gibt eine Permutation $\sigma \in S_n$, sowie Einheiten ε_i mit

$$q_{\sigma(i)} = \varepsilon_i p_i$$

für alle $1 \leq i \leq n$ und $u = v \prod_{i=1}^n \varepsilon_i$.

Beweis. Die Existenz der Zerlegung folgt aus Satz 10.16 mit Satz 10.9.

Wir zeigen die Eindeutigkeit per Induktion nach n. Für $n = 0$ ist $a = u \in R^\times$, somit muß für alle $1 \leq j \leq m$ in

$$R = (a) \subseteq (q_j) \subseteq R$$

Gleichheit gelten. Damit ist q_j eine Einheit und nicht prim, Widerspruch zu $m > 0$. Damit gilt die Aussage im Fall $n = 0$.

[10] Hier ist natürlich noch einiges zu zeigen: die Elemente 2, 3 und $1 \pm \sqrt{-5}$ sind irreduzibel.

Sei der Satz für $n-1$ bewiesen. Da

$$p_n \mid a = v \cdot q_1 \cdot \ldots \cdot q_m,$$

gibt es ein j mit $p_n \mid q_j$. Nach Permutation[11] der q_j dürfen wir annehmen, daß $j = m$. Dann gibt es $\varepsilon_n \in R$ mit $q_m = \varepsilon_n p_n$. Da q_m prim, also irreduzibel nach Satz 10.9, und $p_n \notin R^\times$ ist, muß ε_n eine Einheit sein. Wir betrachten

$$b = a/q_m = (u\varepsilon_n^{-1}) \cdot p_1 \cdot \ldots \cdot p_{n-1}$$

mit der zweiten Faktorisierung

$$b = v \cdot q_1 \cdot \ldots \cdot q_{m-1}.$$

Per Induktionsannahme gilt nun $n-1 = m-1$, also $n = m$, und es gibt eine Permutation $\sigma' \in S_{n-1}$ und Einheiten ε_i mit den geforderten Eigenschaften für die Faktorisierungen von b. Setzen wir σ' zu $\sigma \in S_n$ fort durch $\sigma(n) := n$, dann folgt damit die Behauptung. □

Definition 10.19. Ein **faktorieller Ring** ist ein Integritätsring R, in dem jedes $a \in R$, $a \neq 0$ eine eindeutige Primfaktorzerlegung im Sinne von Theorem 10.18 besitzt.

Korollar 10.20. *Es gilt für einen Integritätsring:*

$$R \text{ euklidisch} \implies R \text{ Hauptidealring} \implies R \text{ faktoriell}.$$

□

Bemerkung 10.21. Die umgekehrten Implikationen gelten nicht. Der Ring $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ ist ein Hauptidealring, aber nicht euklidisch. Der Ring $\mathbb{Z}[X]$ ist ein faktorieller Ring, aber kein Hauptidealring.

11. Der Chinesische Restsatz

11.1. **Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches.** In Hauptidealringen kann man größte gemeinsame Teiler und kleinste gemeinsame Vielfache definieren.

Definition 11.1. Sei R ein Integritätsring und seien $a_1, \ldots, a_r \in R$.

(1) Ein **größter gemeinsamer Teiler (ggT)** von $a_1, \ldots, a_r$ ist ein $d \in R$ mit
   (i) $d \mid a_i$ für alle $i = 1, \ldots, r$, und
   (ii) für jedes $t \in R$ mit $t \mid a_i$ für alle $i = 1, \ldots, r$ gilt $t \mid d$.
   Wir notieren den ggT als
   $$\mathrm{ggT}(a_1, \ldots, a_r).$$

(2) Ein **kleinstes gemeinsames Vielfaches (kgV)** von $a_1, \ldots, a_r$ ist ein $v \in R$ mit
   (i) $a_i \mid v$ für alle $i = 1, \ldots, r$, und
   (ii) für jedes $w \in R$ mit $a_i \mid w$ für alle $i = 1, \ldots, r$ gilt $v \mid w$.
   Wir notieren das kgV als
   $$\mathrm{kgV}(a_1, \ldots, a_r).$$

Proposition 11.2. *Sei R ein Integritätsring und seien $a_1, \ldots, a_r \in R$.*

(1) Wenn ein größter gemeinsamer Teiler d der $a_1, \ldots, a_r$ existiert, dann ist $d' \in R$ ein größter gemeinsamer Teiler $\iff d \sim d'$.

(2) Wenn ein kleinstes gemeinsames Vielfaches v der $a_1, \ldots, a_r$ existiert, dann ist $v' \in R$ ein kleinstes gemeinsames Vielfaches $\iff v \sim v'$.

Mit andern Worten: existierende ggT und kgV sind eindeutig bis auf Multiplikation mit einer Einheit.

[11] Diese praktische Annahme erleichtert die Notation, sorgt aber eventuell für die irrige Annahme, daß in der gesuchten Permutation $\sigma(n) = n$ gilt. Dies haben wir in diesem Moment so organisiert. In der Ausgangsfaktorisierung gilt dies nicht. Wir verwenden hier die Gruppenstruktur der Permutationsgruppe S_n, indem wir zwei Permutationen hintereinander ausführen. Oder, wir verwenden, daß die Behauptung offensichtlich nach beliebiger Permutation der Faktoren bewiesen werden darf.

Beweis. (1) Weil d' ein gemeinsamer Teiler ist, folgt $d \mid d'$. Analog gilt $d' \mid d$. Aus Proposition 10.3 (8) folgt dann $d \sim d'$.

Wenn umgekehrt $d \sim d'$, dann haben d und d' die gleichen Teilbarkeitseigenschaften nach Proposition 10.3 (7).

(2) beweist man genauso wie (1). □

Proposition 11.3. *In einem Hauptidealring R existieren zu beliebigen Elementen $a_1, \ldots, a_r \in R$ der ggT und das kgV. Genauer gilt:*

(1) Ein $d \in R$ ist ein ggT von $a_1, \ldots, a_r$ genau dann, wenn

$$(d) = (a_1, \ldots, a_r).$$

(2) Ein $v \in R$ ist ein kgV von $a_1, \ldots, a_r$ genau dann, wenn

$$(v) = \bigcap_{i=1}^{r} (a_i).$$

Beweis. Weil R ein Hauptidealring ist, werden durch Erzeugnis und Schnitt Elemente $d, v \in R$ definiert, und zwar (wie zu erwarten) nur eindeutig bis auf assoziierte Elemente. Wir müssen zeigen, daß solche d ein ggT und solche v ein kgV sind. Aber das folgt sofort aus der Definition der Teilbarkeitsbeziehung:

(1) Es gilt $(a_i) \subseteq (d)$ für alle $i = 1, \ldots, r$, also $d \mid a_i$. Für jedes $t \in R$ mit $(a_i) \subseteq (t)$ für alle $i = 1, \ldots, r$, also $t \mid a_i$, folgt

$$(d) = (a_1, \ldots, a_r) \subseteq (t), \qquad \text{also} \quad t \mid d.$$

(2) Es gilt $(v) \subseteq (a_i)$ für alle $i = 1, \ldots, r$, also $a_i \mid v$. Für jedes $w \in R$ mit $(w) \subseteq (a_i)$ für alle $i = 1, \ldots, r$, also $a_i \mid w$, folgt

$$(w) \subseteq \bigcap_{i=1}^{r} (a_i) = (v), \qquad \text{also} \quad v \mid w.$$ □

Bemerkung 11.4. Man kann ggT und kgV als Ideale in jedem Ring durch die rechte Seite der Formeln aus Proposition 11.3 definieren. Der Übergang zu Elementen bei Hauptidealringen führt zu Unbestimmtheit bis auf eine Einheit, siehe Proposition 10.1.

Korollar 11.5. *Sei R ein Hauptidealring und $a_1, \ldots, a_n \in R$. Für alle $1 \leq r \leq n$ gilt*

$$\begin{aligned} \mathrm{ggT}(a_1, \ldots, a_n) &= \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_r), a_{r+1}, \ldots, a_n), \\ \mathrm{kgV}(a_1, \ldots, a_n) &= \mathrm{kgV}(\mathrm{kgV}(a_1, \ldots, a_r), a_{r+1}, \ldots, a_n). \end{aligned}$$

Beweis. Das folgt sofort aus den Formeln aus Proposition 11.3 wegen der Idealgleichungen

$$\begin{aligned} (a_1, \ldots, a_n) &= ((a_1, \ldots, a_r), a_{r+1}, \ldots, a_n), \\ \bigcap_{i=1}^{n} (a_i) &= \bigcap_{i=1}^{r} (a_i) \ \cap (a_{r+1}) \cap \ldots \cap (a_n). \end{aligned}$$ □

Korollar 11.6 (Lemma von Bézout)**.** *Sei R ein Hauptidealring und $d = \mathrm{ggT}(a_1, \ldots, a_r)$. Dann ist d eine R-Linearkombination der a_i, d.h.*

$$d = x_1 a_1 + \ldots + x_r a_r$$

für geeignete Elemente $x_i \in R$ für $1 \leq i \leq r$.

Beweis. Das ist nach der Formel aus Proposition 11.3 klar. □

Die Eindeutigkeit der Primfaktorzerlegung in einem Hauptidealring erlaubt es, den ggT und das kgV mit Hilfe der Primfaktorzerlegung auszudrücken.

Korollar 11.7. *Seien $p_i \in R$ für $1 \leq i \leq n$ paarweise nicht-assoziierte Primelemente eines Hauptidealrings R.*

(1) *Sei $a = u \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$ mit $u \in R^\times$. Dann gilt für $b \in R$:*

$$b \mid a \iff \text{es gibt } 0 \leq f_i \leq e_i \text{ für } 1 \leq i \leq n \text{ und } v \in R^\times \text{ mit } b = v \cdot p_1^{f_1} \cdot \ldots \cdot p_n^{f_n}.$$

(2) *Sei $a_j = u_j \cdot \prod_{i=1}^n p_i^{e_{ij}}$ mit $u_j \in R^\times$ und mit $e_{ij} \in \mathbb{N}_0$ für alle $1 \leq i \leq n$ und $1 \leq j \leq r$. Sei*

$$m_i = \min_{1 \leq j \leq r} \{e_{ij}\} \qquad \text{und} \qquad M_i = \max_{1 \leq j \leq r} \{e_{ij}\}.$$

Dann gilt:

$$\operatorname{ggT}(a_1, \ldots, a_r) = \prod_{i=1}^n p_i^{m_i}$$
$$\operatorname{kgV}(a_1, \ldots, a_r) = \prod_{i=1}^n p_i^{M_i}.$$

Beweis. (1) Wir schreiben $a = bc$. Die Primfaktorzerlegungen von b und c legen wegen der Eindeutigkeit die Primfaktorzerlegung von a fest: man multipliziere beide Zerlegungen. Aussage (2) folgt sofort aus Aussage (1). □

Korollar 11.8. *Sei R ein Hauptidealring und seien $a, b \in R$. Dann gilt*

$$(\operatorname{ggT}(a, b) \cdot \operatorname{kgV}(a, b)) = (ab).$$

Beweis. Das folgt wegen

$$m + M = \min\{m, M\} + \max\{m, M\}$$

sofort aus den Formeln von Korollar 11.7. Der Übergang zu Hauptidealen ist nötig, weil ggT und kgV nur eindeutig bis auf assoziierte Elemente definiert sind. □

11.2. **Der euklidische Algorithmus in euklidischen Ringen.** Seien $a, b \in R$ Elemente eines Hauptidealrings und $d = \operatorname{ggT}(a, b)$. Es ist besonders interessant, den ggT „algorithmisch“ als R-Linearkombination

$$d = s \cdot a + t \cdot b$$

bestimmen zu können. Dies funktioniert für euklidische Ringe, sofern die Division mit Rest algorithmisch ist, wie etwa bei $\mathbb{Z}$ oder bei Polynomringen $K[X]$ über einem Körper K. Dies setzt natürlich voraus, daß auch das Rechnen in K algorithmisch ist.

Sei δ eine euklidische Gradfunktion auf R. Wir berechnen für $a, b \in R$

$$d = \operatorname{ggT}(a, b) \quad \text{ und } s, t \in R \text{ mit } \quad d = s \cdot a + t \cdot b.$$

Initialisierung: Wir nehmen ohne Einschränkung an, daß $\delta(a) \geq \delta(b)$. Wir setzen

$$r_0 = a, \quad r_1 = b \quad \text{und} \quad \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Wir starten mit $i = 1$.

Rekursion: Solange $r_i \neq 0$ gilt, berechnen wir per Division mit Rest q_i und r_{i+1} mit $\delta(r_{i+1}) < \delta(r_i)$ oder $r_{i+1} = 0$, so daß $r_{i-1} = q_i \cdot r_i + r_{i+1}$, und setzen dann:

$$s_{i+1} := s_{i-1} - q_i s_i$$
$$t_{i+1} := t_{i-1} - q_i t_i.$$

Wenn $r_i = 0$, dann STOP:

$$d = r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b.$$

Zur Korrektheit des Algorithmus betrachten wir zunächst die Folge $r_0, r_1, r_2, \ldots$. Die Folge $\delta(r_0), \delta(r_1), \delta(r_2), \ldots$ ist streng monoton fallend in $\mathbb{N}_0$ und damit endlich. Wir erreichen daher nach endlich vielen Iterationen ein n mit $r_n = 0$. Wegen

$$(\mathrm{ggT}(r_{i-1}, r_i)) = (r_{i-1}, r_i) = (r_{i-1} - q_i r_i, r_i) = (r_i, r_{i+1}) = (\mathrm{ggT}(r_i, r_{i+1}))$$

berechnet der Algorithmus, was er vorgibt zu berechnen (eigentlich nur bis auf ‚assoziiert'):

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(r_0, r_1) = \ldots = \mathrm{ggT}(r_{i-1}, r_i) = \ldots = \mathrm{ggT}(r_{n-1}, r_n) = \mathrm{ggT}(d, 0) = d.$$

Nun beweisen wir per Induktion für alle i

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} s_{i-1} & t_{i-1} \\ s_i & t_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Dies gilt für $i = 1$ aufgrund der Initialisierung des Algortihmus

$$\begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Wenn es für i gilt, dann auch für $i + 1$:

$$\begin{aligned} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} &= \begin{pmatrix} r_i \\ r_{i-1} - q_i r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} s_{i-1} & t_{i-1} \\ s_i & t_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \begin{pmatrix} s_i & t_i \\ s_{i-1} - q_i s_i & t_{i-1} - q_i t_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \end{aligned}$$

Werten wir dies für $i = n$ in der ersten Zeile aus, dann erhalten wir

$$d = r_{n-1} = s_{n-1} \cdot a + t_{n-1} \cdot b.$$

Zur konkreten Durchführung benutzt man am besten eine Tabelle der Form (aus den blau unterlegten Einträgen werden im Iterationsschritt die rot unterlegten berechnet):

i	r_i	q_i	s_i	t_i
0	a	$-$	1	0
1	b	q_1	0	1
2	r_2	q_2	s_2	t_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i-1$	r_{i-1}	$\vdots$	s_{i-1}	t_{i-1}
i	r_i	q_i	s_i	t_i
$i+1$	r_{i+1}	$\vdots$	s_{i+1}	t_{i+1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	d	q_{n-1}	s_{n-1}	t_{n-1}
n	0	$-$	s_n	t_n

Beispiel 11.9. Wir rechnen in $R = \mathbb{Z}$ den ggT von $a = 2016$ und $b = 512$ aus.

i	r_i	q_i	s_i	t_i
0	2016	$-$	1	0
1	512	3	0	1
2	480	1	1	-3
3	32	15	-1	4
4	0	$-$	16	-63

In der Tat ist

$$512 = 2^9 = 32 \cdot 16, \quad 2016 = 32 \cdot 63, \qquad 32 = -1 \cdot 2016 + 4 \cdot 512.$$

Bemerkung 11.10. Den ggT von mehr als zwei Elementen in einem euklidischen Ring bestimmt man rekursiv mit dem euklidischen Algorithmus für jeweils zwei Elemente und der Formel aus Korollar 11.5:

$$\mathrm{ggT}(a_1, a_2, a_3, \ldots, a_r) = \mathrm{ggT}(\mathrm{ggT}(a_1, a_2), a_3, \ldots, a_r) = \ldots$$

Definition 11.11. Elemente $a_1, \ldots, a_r$ eines Hauptidealrings R heißen **teilerfremd**, wenn ihr ggT eine Einheit ist:

$$(1) = (a_1, \ldots, a_r).$$

Sie heißen **paarweise teilerfremd**, wenn für alle $1 \leq i < j \leq r$ das Paar a_i, a_j teilerfremd ist.

Korollar 11.12. *Elemente $a_1, \ldots, a_r$ eines Hauptidealrings R sind teilerfremd genau dann, wenn*

$$1 = x_1 a_1 + \ldots + x_r a_r$$

für geeignete Elemente $x_i \in R$ für $1 \leq i \leq r$. □

Lemma 11.13. *Sei R ein Hauptidealring und a, b teilerfremde Elemente von R. Dann gilt*

$$(ab) = (a) \cap (b).$$

Beweis. Nach Korollar 11.8 gilt wegen $\mathrm{ggT}(a, b) = 1$

$$(a) \cap (b) = (\mathrm{kgV}(a, b)) = (\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b)) = (ab).$$ □

Satz 11.14 (Chinesischer Restsatz)**.** *Seien $a, b \in R$ teilerfremde Elemente des Hauptidealrings R. Dann definieren die kanonischen Projektionen $\mathrm{pr}_a : R \to R/(a)$ und $\mathrm{pr}_b : R \to R/(b)$ die Komponentenabbildungen eines Ringisomorphismus*

$$R/(ab) \simeq R/(a) \times R/(b), \qquad x + (ab) \mapsto (x + (a), x + (b)).$$

Beweis. Die kanonischen Projektionen definieren einen Ringhomomorphismus

$$\begin{aligned} \mathrm{pr} : R &\to R/(a) \times R/(b) \\ x &\mapsto (x + (a), x + (b)). \end{aligned}$$

Da a, b teilerfremd sind, gibt es nach Korollar 11.6 $s, t \in R$ mit

$$1 = sa + tb.$$

Seien $x, y \in R$ beliebig und $z = xtb + ysa$. Damit gilt (mit leicht mißbräuchlicher Notation mit Vertretern statt Nebenklassen)

$$\mathrm{pr}(z) = (z, z) = (x(1 - sa) + ysa, y(1 - tb) + xtb) = (x + sa(y - x), y + tb(x - y)) = (x, y),$$

und somit ist pr surjektiv. Lemma 11.13 berechnet den Kern als

$$\ker(\mathrm{pr}) = \ker(\mathrm{pr}_a) \cap \ker(\mathrm{pr}_b) = (a) \cap (b) = (ab).$$

Die Behauptung folgt nun aus dem Homomorphiesatz für Ringe, Satz 8.20. □

Korollar 11.15. *Sei R ein Hauptidealring und $a_1, \ldots, a_n$ seien paarweise teilerfremde Elemente. Dann definieren die kanonischen Projektionen $\mathrm{pr}_i : R \to R/(a_i)$ für $1 \leq i \leq n$ die Komponentenabbildungen eines Ringisomorphismus*

$$R/(\prod_{i=1}^{n} a_i) \simeq \prod_{i=1}^{n} R/(a_i).$$

Beweis. Wir zeigen die Aussage per Induktion nach n. Für $n = 1$ ist dies trivial. Wir nehmen an, daß die Aussage bewiesen ist für $n - 1$ Elemente.

Die Elemente a_1 und $b = a_2 a_3 \dots a_n$ sind teilerfremd. Andernfalls hätte nach Satz 10.16 der ggT (a_1, b) einen Primteiler p. Aus $p \mid a_2 a_3 \dots a_n$ folgt (Induktion nach Anzahl der Faktoren), daß es ein $2 \leq i \leq n$ geben muß mit $p \mid a_i$. Dann ist p ein nicht-trivialer gemeinsamer Teiler von a_1 und a_i im Widerspruch zur Annahme der paarweisen Teilerfremdheit.

Nach Satz 11.14 und Induktionsvoraussetzung gilt dann

$$R/(\prod_{i=1}^{n} a_i) = R/(a_1 b) \simeq R/(a_1) \times R/(b) \simeq R/(a_1) \times \left(\prod_{i=2}^{n} R/(a_i) \right) = \prod_{i=1}^{n} R/(a_i).$$

Man verifiziert leicht, daß dieser Isomorphismus aus den kanonischen Projektionen zusammengesetzt ist und so die behauptete Form hat. □

Beispiel 11.16. Sei $R = K[X]$ und $f = \prod_{i=1}^{n} p_i^{e_i}$ die Primfaktorisierung in (paarweise verschiedene) normierte irreduzible Polynome p_i. Verschiedene normierte irreduzible Polynome sind automatisch auch nicht assoziiert, weil Einheiten $K[X]^\times = K^\times$ nur konstante Polynome sind. Dann ergibt der Chinesische Restsatz einen kanonischen Ringisomorphismus

$$K[X]/(f) \cong \prod_{i=1}^{n} K[X]/(p_i^{e_i}).$$

Beispiel 11.17. Für $R = \mathbb{Z}$ besagt Korollar 11.15 folgendes. Seien $n_1, \dots, n_r$ paarweise teilerfremde positive natürliche Zahlen und $N = \prod_{i=1}^{r} n_i$ das Produkt. Dann ist die natürliche Abbildung

$$\varphi : \mathbb{Z}/N\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}, \qquad \varphi(a + N\mathbb{Z}) = (a + n_i\mathbb{Z})_{i=1,\dots,r}$$

ein Isomorphismus von Ringen. Diese Aussage ist auch für die Struktur der zugrundeliegenden abelschen Gruppen interessant. Ein Erzeuger des Produkts ist $\varphi(1) = (1, \dots, 1)$, wie man leicht durch Bestimmen der Ordnung herausfindet.

Der Chinesische Restsatz kann als Aussage über das Lösen von Systemen von Kongruenzen verstanden werden. Für beliebige ganze Zahlen $a_i \in \mathbb{Z}$ für $1 \leq i \leq r$ hat das System der Kongruenzen

$$x \equiv a_i \pmod{n_i} \quad \text{für alle } 1 \leq i \leq r$$

eine Lösung $x \in \mathbb{Z}$, die als Lösung $x \pmod N$ sogar eindeutig ist. Es ist $x \in \mathbb{Z}/N\mathbb{Z}$ Lösung genau dann, wenn $\varphi(x) = (a_1, \dots, a_r)$.

Der folgende Algorithmus beschreibt, wie man die Lösung x findet.

Schritt 1: Für jedes $1 \leq i \leq r$ sei $N_i = \prod_{j=1,\ j\neq i}^{r} n_j$. Dann ist $1 = \mathrm{ggT}(n_i, N_i)$. Wir suchen ein $e_i \in \mathbb{Z}$ mit

$$e_i \equiv 1 \pmod{n_i} \quad \text{und} \quad e_i \equiv 0 \pmod{N_i}.$$

Das ist ein Spezialfall des zu behandelnden Problems mit nur zwei Kongruenzgleichungen und speziellen Inhomogenitäten.

Schritt 2: Mittels des euklidischen Algorithmus aus Abschnitt 11.2 finden wir $x_i, y_i \in \mathbb{Z}$ mit

$$x_i N_i + y_i n_i = 1.$$

Dann erfüllt $e_i = x_i N_i \pmod N$ die geforderten Kongruenzen.

Schritt 3: Die gesuchte Lösung ist

$$x = \sum_{i=1}^{r} a_i e_i \pmod N,$$

denn $x \equiv \sum_{i=1}^{r} a_i e_i \equiv a_i e_i \equiv a_i \pmod{n_i}$.

Dieses Vorgehen hat den Vorteil, daß die hauptsächlichen Rechenkosten bei der Berechnung der e_i entstehen. Diese Rechnung ist von den spezifischen a_i unabhängig und kann bei variierenden a_i wiederverwendet werden. Es fällt dann nur noch der billige Schritt 3 an.

11.3. **Jordan–Chevalley–Zerlegung.** Sei K ein Körper und $A \in \mathrm{M}_n(K)$ eine quadratische Matrix. Die Menge der Polynome in A

$$R_A := \{P(A)\ ;\ P(X) \in K[X]\}$$

ist das Bild des Auswertungshomomorphismus

$$\mathrm{ev}_A : K[X] \twoheadrightarrow R_A \subseteq \mathrm{M}_n(K).$$

Der Auswertungshomomorphismus ist definiert, weil $K \simeq K \cdot \mathbf{1} = Z(\mathrm{M}_n(K))$ mit allen Matrizen kommutiert, siehe Satz 7.25. Als Bild ist $R_A = \mathrm{ev}_A(K[X])$ ein Unterring von $\mathrm{M}_n(K)$. Der Kern ist

$$\ker(\mathrm{ev}_A) = (m_A(X))$$

vom Minimalpolynom von A erzeugt, und der Homomorphiesatz beschreibt R_A als

$$K[X]/(m_A(X)) \simeq R_A.$$

Damit ist R_A bereits ganz gut beschrieben. Sei gemäß Theorem 10.18

$$m_A(X) = \prod_{i=1}^{r} p_i(X)^{n_i}$$

die Primfaktorzerlegung von $m_A(X)$. Das Minimalpolynom von A ist per Definition normiert, und wir nehmen dasselbe von den paarweise verschiedenen ($\iff$ nicht assoziierten, weil normiert) irreduziblen Polynomen $p_i(X)$ an. Nach dem Chinesischen Restsatz, genauer Korollar 11.15, folgt

$$R_A \simeq K[X]/(m_A(X)) \simeq \prod_{i=1}^{r} K[X]/(p_i(X)^{n_i}).$$

Verfolgt man die Definition der Isomorphismen, so findet man

$$A \leftrightarrow X \leftrightarrow (X, \dots, X).$$

Wir nehmen nun an, daß das charakteristische Polynom $\chi_A(X)$ und damit auch $m_A(X)$ vollständig in Linearfaktoren zerfällt:

$$p_i(X) = X - \lambda_i.$$

Wir übersetzen nun die additive Zerlegung

$$(X, \dots, X) = (\lambda_1, \dots, \lambda_r) + (X - \lambda_1, \dots, X - \lambda_r)$$

in den Ring R_A und finden $S, N \in K[X]$ mit entsprechend

$$A = S(A) + N(A)$$

also

$$S(A) \leftrightarrow (\lambda_1, \dots, \lambda_r) \quad \text{und} \quad N(A) \leftrightarrow (X - \lambda_1, \dots, X - \lambda_r).$$

Weil $A_{\mathrm{ss}} := S(A)$ und $A_{\mathrm{n}} := N(A)$ in R_A liegen, kommutieren A_{ss} und A_{n} mit allen Matrizen, die mit A kommutieren[12] nach dem folgenden Lemma.

Lemma 11.18. *Sei B eine Matrix mit $AB = BA$. Dann gilt für alle $C \in R_A$*

$$BC = CB.$$

Beweis. Weil $C \in R_A$ liegt, gibt es ein $P(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $C = P(A)$. Dann ist

$$BC = B \sum_{i=0}^{n} a_i A^i = \sum_{i=0}^{n} a_i B A^i = \sum_{i=0}^{n} a_i A^i B = \Big(\sum_{i=0}^{n} a_i A^i\Big) \cdot B = CB. \qquad \square$$

[12] Das ss steht für semisimple (halbeinfach) und n für nilpotent.

Insbesondere kommutieren A_{ss} und A_n.

Lemma 11.19. *A_{ss} ist diagonalisierbar und A_n ist nilpotent.*

Beweis. Die Matrix A_{ss} ist Nullstelle von $P(T) = \prod_{i=1}^{r} T - \lambda_i$, hat daher ein Minimalpolynom ohne doppelte Nullstelle und ist demnach diagonalisierbar. Den Wert $P(A_{\mathrm{ss}})$ können wir in R_A ausrechnen und genauer in

$$\prod_{i=1}^{r} K[X]/((X-\lambda_i)^{n_i}),$$

und dort auch komponentenweise. In der i-ten Komponente haben wir λ_i für A_{ss} und das annulliert $P(T)$ wegen $P(\lambda_i) = 0$.

Die Nilpotenz von A_n berechnen wir ebenfalls in den Komponenten $K[X]/((X-\lambda_i)^{n_i})$. Dort ist A_n gegeben durch $X - \lambda_i$, somit offensichtlich nilpotent. □

Bevor wir die zwei Theoreme dieses Abschnitts beweisen können, müssen wir noch einen Satz über simultanes Diagonalisieren nachliefern.

Satz 11.20. *Seien $B, C \in \mathrm{M}_n(K)$. Dann sind äquivalent:*

(a) Die Matrizen B und C sind simultan diagonalisierbar: Es gibt $S \in \mathrm{GL}_n(K)$ und Diagonalmatrizen D und E mit

$$B = SDS^{-1} \qquad \text{und} \qquad C = SES^{-1}.$$

(b) Es gibt eine Basis von K^n, deren Vektoren gleichzeitig Eigenvektoren von B und von C sind.

(c) B und C sind diagonalisierbar und

$$CB = BC.$$

Wenn diese äquivalenten Bedingungen gelten, dann ist auch jede Linearkombination von B und C diagonalisierbar.

Beweis. (a) $\Longrightarrow$ (b): Die Spaltenvektoren von S sind eine Basis, weil $S \in \mathrm{GL}_n(K)$. Außerdem sind diese Spalten Eigenvektoren zu B, der Eigenwert ist der entsprechende Diagonaleintrag von D, und zu C, der Eigenwert ist der entsprechende Diagonaleintrag von E.

(b) $\Longrightarrow$ (a): Aus einer Basis von Eigenvektoren zu B und gleichzeitig C machen wir eine Matrix S. Diese ist dann in $\mathrm{GL}_n(K)$, weil wir eine Basis benutzt haben. Dann sind

$$D = S^{-1}BS \qquad \text{und} \qquad E = S^{-1}CS$$

Diagonalmatrizen, und (a) folgt.

(b) $\Longrightarrow$ (c): Sei $\mathscr{B} = (b_1, \ldots, b_n)$ eine Basis aus Eigenvektoren zu B und C: mit $Bb_i = \lambda_i b_i$ und $Cb_i = \mu_i b_i$ für die Eigenwerte $\lambda_i, \mu_i \in K$. Dann gilt für alle $1 \le i \le n$

$$BCb_i = B(\mu_i b_i) = \mu_i B b_i = \mu_i \lambda_i b_i = \lambda_i \mu_i b_i = \lambda_i C b_i = C(\lambda_i b_i) = CBb_i.$$

Damit gilt $BC = CB$, denn es reicht, die zugehörige lineare Abbildung auf einer Basis zu vergleichen.

(c) $\Longrightarrow$ (b): Da B diagonalisierbar ist, gibt es eine Eigenraumzerlegung $K^n = \bigoplus_\lambda V_\lambda(B)$. Wenn $v \in V_\lambda(B)$ ein Eigenvektor zum Eigenwert λ ist, dann ist auch $w = Cv$ ein solcher:

$$Bw = BCv = CBv = C(\lambda v) = \lambda Cv = \lambda w.$$

Weil C diagonalisierbar ist, hat das Minimalpolynom $m_C(X)$ von C keine doppelten Nullstellen und zerfällt in Linearfaktoren. Das Minimalpolynom von C eingeschränkt zu einer linearen Abbildung $V_\lambda(B) \to V_\lambda(B)$ ist ein Teiler von $m_C(X)$. Damit hat auch dieses keine doppelten Nullstellen und zerfällt in Linearfaktoren. Daher ist auch jeder der Blöcke diagonalisierbar, der C in einer zur Zerlegung $K^n = \bigoplus_\lambda V_\lambda(B)$ angepaßten Basis beschreibt. Das heißt, der Raum

$V_\lambda(B)$ hat eine Basis aus Eigenvektoren von C. Vereinigt über alle λ erhalten wir so eine Basis aus Eigenvektoren für gleichzeitig B und C.

Beweisen wir noch den Zusatz: für $x, y \in K$ und S, D und E wie in (a) gilt

$$xB + yC = S(xD + yE)S^{-1}. \qquad \square$$

Lemma 11.21. *Seien $N, M \in \mathrm{M}_n(K)$ kommutierende nilpotente Matrizen. Dann ist auch jede Linearkombination von N und M nilpotent.*

Beweis. Seien $x, y \in K$ und $n \in \mathbb{N}$ so groß, daß $N^n = M^n = 0$. Weil N und M kommutieren, gilt die binomische Formel. Dann ist

$$(xN + yM)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} x^k y^{2n-k} N^k M^{2n-k}.$$

In der Summe ist jeder Summand 0, weil jeweils N^k oder M^{2n-k} die Nullmatrix ist. $\square$

Theorem 11.22 (Additive Jordan–Chevalley–Zerlegung)**.** *Sei $A \in \mathrm{M}_n(K)$ mit zerfallendem charakterstischen Polynom. Dann gibt es eindeutige miteinander kommutierende Matrizen*

- *$A_{\mathrm{ss}} \in \mathrm{M}_n(K)$ mit $AA_{\mathrm{ss}} = A_{\mathrm{ss}}A$ und A_{ss} diagonalisierbar,*
- *$A_n \in \mathrm{M}_n(K)$ mit $AA_n = A_nA$ und A_n nilpotent und*

$$A = A_{\mathrm{ss}} + A_n.$$

Zusatz: es gibt Polynome $S(X), N(X) \in K[X]$ mit $A_{\mathrm{ss}} = S(A)$ und $A_n = N(A)$.

Beweis. Die Existenz haben wir bereits gesehen, sogar mit dem Zusatz. Diese Zerlegung bezeichnen wir wie oben und im Theorem mit $A = A_{\mathrm{ss}} + A_n$.

Sei also $A = S + N$ eine weitere solche Zerlegung. Aufgrund des Zusatzes kommutieren A_{ss} und S sowie A_n und N. Aus den beiden Summenzerlegungen erhalten wir

$$A_{\mathrm{ss}} - S = N - A_n$$

Weil A_{ss} und S kommutieren und diagonalisierbar sind, sind sie sogar simultan diagonalisierbar, siehe Satz 11.20. Es gibt dann eine Basis aus Eigenvektoren für S und A_{ss} gleichzeitig. Deshalb ist $A_{\mathrm{ss}} - S$ diagonalisierbar, durch dieselbe Basis, siehe Satz 11.20.

Weil A_n und N kommutieren und nilpotent sind, ist $N - A_n$ auch nilpotent, siehe Lemma 11.21. Damit ist nun $A_{\mathrm{ss}} - S = N - A_n$ gleichzeitig diagonalisierbar und nilpotent. Nilpotente Matrizen haben nur den Eigenwert 0. Dieser Eigenwert steht auf der Diagonale beim Diagonalisieren, folglich ist

$$0 = A_{\mathrm{ss}} - S = N - A_n.$$

Dies zeigt die Eindeutigkeit. $\square$

Sei nun $A \in \mathrm{GL}_n(K)$. Dann sind alle Eigenwerte $\lambda_i \in K^\times$ und $A_{\mathrm{ss}} \in \mathrm{GL}_n(K)$. Sei $U(X)$ ein Polynom, das

$$U(A) \leftrightarrow (\lambda_1^{-1}X, \dots, \lambda_r^{-1}X) = \mathbf{1} + (\lambda_1^{-1}(X - \lambda_1), \dots, \lambda_r^{-1}(X - \lambda_r)) = \mathbf{1} + A_{\mathrm{ss}}^{-1}A_n =: A_u$$

entspricht. Durch die Beschreibung in R_A komponentenweise ist klar, daß A_u eine unipotente Matrix ist. Außerdem gilt

$$A_{\mathrm{ss}} \cdot A_u = A_{\mathrm{ss}} + A_n = A.$$

Als Summe einer invertierbaren Matrix $\mathbf{1}$ und einer damit kommutierenden nilpotenten Matrix $A_{\mathrm{ss}}^{-1}A_n$ ist A_u auch invertierbar.

Lemma 11.23. *Seien $U, V \in \mathrm{GL}_n(K)$ kommutierende unipotente Matrizen. Dann ist auch UV unipotent.*

Beweis. Sei $U = \mathbf{1} + N$ und $V = \mathbf{1} + M$. Dann sind $N, M \in \mathrm{M}_n(K)$ nilpotent per Definition von unipotent. Außerdem kommutieren N und M:

$$NM = (U - \mathbf{1})(V - \mathbf{1}) = UV - V - U + \mathbf{1} = VU - V - U + \mathbf{1} = (V - \mathbf{1})(U - \mathbf{1}) = MN.$$

Dann ist

$$UV = \mathbf{1} + N + M + NM.$$

Es bleibt zu zeigen, daß $N + M + NM$ nilpotent ist. Das folgt aus Lemma 11.21. □

Theorem 11.24 (Multiplikative Jordan–Chevalley–Zerlegung)**.** *Sei $A \in \mathrm{GL}_n(K)$ mit zerfallendem charakteristischen Polynom. Dann gibt es eindeutige miteinander kommutierende Matrizen*

- $A_{\mathrm{ss}} \in \mathrm{GL}_n(K)$ *mit* $AA_{\mathrm{ss}} = A_{\mathrm{ss}}A$ *und* A_{ss} *diagonalisierbar,*
- $A_u \in \mathrm{GL}_n(K)$ *mit* $AA_u = A_uA$ *und* A_u *unipotent und*

$$A = A_{\mathrm{ss}} \cdot A_u.$$

Zusatz: es gibt Polynome $S(X), U(X) \in K[X]$ mit $A_{\mathrm{ss}} = S(A)$ und $A_u = U(A)$.

Beweis. Die Existenz haben wir bereits gesehen, sogar mit dem Zusatz. Diese Zerlegung bezeichnen wir wie oben und im Theorem mit $A = A_{\mathrm{ss}} \cdot A_u$.

Sei also $A = S \cdot U$ eine weitere solche Zerlegung. Aufgrund des Zusatzes kommutieren A_{ss} und S sowie A_u und U. Aus den beiden Produktzerlegungen erhalten wir

$$S^{-1}A_{\mathrm{ss}} = UA_u^{-1}.$$

Weil A_{ss} und S kommutieren und diagonalisierbar sind, sind sie sogar simultan diagonalisierbar: es gibt eine Basis aus Eigenvektoren für S und A_{ss} gleichzeitig. Deshalb ist $S^{-1}A_{\mathrm{ss}}$ diagonalisierbar (selbe Basis).

Weil A_u und U kommutieren und unipotent sind, ist UA_u^{-1} auch unipotent, siehe Lemma 11.23. Damit ist nun $S^{-1}A_{\mathrm{ss}} = UA_u^{-1}$ gleichzeitig diagonalisierbar und unipotent. Unipotente Matrizen haben nur den Eigenwert 1. Dieser Eigenwert steht auf der Diagonale beim Diagonalisieren, folglich ist

$$\mathbf{1} = S^{-1}A_{\mathrm{ss}} = UA_u^{-1}.$$

Dies zeigt die Eindeutigkeit. □

Von den Jordan-Chevalley–Zerlegungen ist es nicht weit zum einen zu einer Verallgemeinerung für Matrizen ohne die Voraussetzung eines zerfallenden charakteristischen Polynoms, zum andern ist die Jordan-Normalform in Reichweite, und diese auch im allgemeinen Fall.

Übungsaufgaben zu §11

Übungsaufgabe 11.1. Seien $a_1, \ldots, a_n$ Elemente eines Hauptidealrings R. Zeigen Sie, daß das kgV der $a_1, \ldots, a_n$ das Produkt $a_1 \cdot \ldots \cdot a_n$ teilt.

Übungsaufgabe 11.2. Seien p ein Primelement in einem Hauptidealring R und $a_1, \ldots, a_n \in R$ Elemente. Zeigen Sie, daß aus

$$p \mid a_1 \cdot \ldots \cdot a_n$$

folgt, daß für ein i mit $1 \leq i \leq n$ schon $p \mid a_i$.

Übungsaufgabe 11.3. Sei K ein Körper. Bestimmen Sie die primen Elemente in $K[[X]]$ bis auf Einheiten.

Übungsaufgabe 11.4. Ist $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ eine zyklische Gruppe? Was ist mit $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$?

Übungsaufgabe 11.5. Sei K ein Körper, über dem jedes Polynom $f \in K[X]$ vom Grad $\deg(f) > 0$ eine Nullstelle hat (ein **algebraisch abgeschlossener Körper**). Zeigen Sie, daß jedes irreduzible Polynom in $K[X]$ linear, also vom Grad 1, ist.

Übungsaufgabe 11.6. Seien R ein Ring und $x, y, q, r \in R$ mit $x = qy + r$. Dann gilt

$$(x, y) = (r, y).$$

Teil 3. Mehr über Gruppen

12. Fixpunkte

12.1. **Das Lemma von Burnside.** Das Lemma von Burnside ist gar nicht von Burnside, sondern von Cauchy.

Definition 12.1. Sei $G \times X \to X$ eine Gruppenoperation. Ein Element $x \in X$ heißt **Fixpunkt** der Operation, wenn $G_x = G$, also $g.x = x$ für alle $g \in G$ gilt. Die Menge aller Fixpunkte bezeichnen wir mit

$$X^G = \mathrm{Fix}(G, X).$$

Die Fixpunkte eines $g \in G$ sind die $x \in X$ mit $g.x = x$. Ihre Menge wird mit

$$X^g = \mathrm{Fix}(g, X)$$

bezeichnet.

Bemerkung 12.2. Es gilt $X^g = X^{\langle g \rangle}$ und

$$X^G = \bigcap_{g \in G} X^g.$$

Satz 12.3 (Burnside–Lemma)**.** *Sei G eine endliche Gruppe, die auf einer endlichen Menge X operiert. Dann gilt für die Anzahl der Bahnen die Formel*

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Beweis. Wir zählen die Menge der Lösungen der Fixpunktgleichung

$$F = \{(g, x) \in G \times X \ ; \ g.x = x\}$$

auf zwei Weisen. Wir summieren entweder zuerst über jedes g die Anzahl $|X^g|$ der passenden x oder aber zuerst über jedes x die Anzahl $|G_x|$ der passenden g:

$$\sum_{g \in G} |X^g| = |F| = \sum_{x \in X} |G_x|.$$

Nach der Bahnenformel gilt $|G_x| = |G|/|G.x|$. Daraus folgt

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{1}{|G.x|}.$$

Zählen wir nun zuerst über den Bahnenraum und dann über die Elemente einer Bahn, so folgt

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \sum_{x \in X} \frac{1}{|G.x|} = \sum_{B \in G\backslash X} \sum_{x \in B} \frac{1}{|B|} = \sum_{B \in G\backslash X} 1 = |G\backslash X|. \qquad \square$$

12.2. **Der Fixpunktsatz.**

Definition 12.4. Sei p eine Primzahl. Eine **p-Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

Satz 12.5 (Fixpunktsatz)**.** *Sei G eine endliche p-Gruppe, die auf einer endlichen Menge X operiert. Dann gilt*

$$|X| \equiv |\mathrm{Fix}(G, X)| \pmod{p}.$$

Beweis. Die Bahnen der Länge 1 bestehen genau aus den Fixpunkten. Die Bahnen der Länge > 1 haben nach der Orbit–Stabilisator–Formel eine Länge, die durch p teilbar ist. Aus der Bahnenformel folgt daher.

$$|X| = \sum_{B \in G\backslash X} |B| = |\mathrm{Fix}(G, X)| + \sum_{B \in G\backslash X,\ |B|>1} |B| \equiv |\mathrm{Fix}(G, X)| \pmod{p}. \qquad \square$$

Um die Kraft der Gruppenoperationen für die Strukturanalyse zu demonstrieren, beweisen wir den Satz von Cauchy[13].

Satz 12.6 (Satz von Cauchy 1845)**.** *Sei G eine endliche Gruppe und p eine Primzahl, welche die Ordnung von G teilt. Dann existiert ein $g \in G$ mit der Ordnung* $\operatorname{ord}(g) = p$.

Beweis. Sei $Z = \langle (1,2,3,\ldots,p) \rangle \subseteq S_p$ die vom p-Zykel $\sigma = (1,2,3,\ldots,p)$ erzeugte Untergruppe in der symmetrischen Gruppe S_p. Nach Proposition 5.13 hat σ die Ordnung p und Z besteht aus den verschiedenen Elementen

$$\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{p-1},$$

hat also auch die Ordnung $|Z| = p$.

Wir lassen die Gruppe Z auf der Menge

$$X = \{(g_1,\ldots,g_p) \in G^p \;;\; g_1 g_2 \ldots g_p = 1\}$$

in natürlicher Weise durch zyklische Vertauschung operieren:

$$Z \times X \to X$$
$$\big(\sigma^n, (g_1,\ldots,g_p)\big) \mapsto (g_{\sigma^n(1)},\ldots,g_{\sigma^n(p)}),$$

dabei ist für $0 \le n < p$ explizit

$$(g_{\sigma^n(1)},\ldots,g_{\sigma^n(p)}) = (g_{1+n}, g_{2+n}, \ldots, g_p, g_1, \ldots, g_n).$$

Klar ist, daß wir so eine Operation von Z auf X definieren, sofern die Abbildung wohldefiniert ist, also Werte wieder in X angenommen werden. Dazu müssen wir zeigen, daß aus $g_1 g_2 \ldots g_p = 1$ auch $g_{r+1} \ldots g_p g_1 \ldots g_r = 1$ folgt. Mit $a = g_1 \ldots g_r$ und $b = g_{r+1} \ldots g_p$ müssen wir

$$ab = 1 \quad \Longrightarrow \quad ba = 1$$

zeigen. Das ist gerade die Behauptung, daß das Rechtsinverse von a, nämlich b, auch ein Linksinverses ist, also längst bekannt.

Nach dem Bahnensatz haben die Bahnen von Z auf X eine Länge, welche die Ordnung $p = |Z|$ teilt. Da p eine Primzahl ist, sind die Bahnen entweder der Länge p oder der Länge 1. Bahnen der Länge 1, also Fixpunkte, sind von der Form

$$(g,\ldots,g)$$

mit $g \in G$ und $g^p = 1$. Wir müssen also zeigen, daß es Bahnen der Länge 1 gibt, die von $(1,\ldots,1)$ verschieden sind. Dann nämlich hat $g \neq 1$ mit $g^p = 1$ die Ordnung p, weil p eine Primzahl ist: wegen $g \neq 1$ ist $\operatorname{ord}(g) > 1$ und wegen $g^p = 1$ gilt $\operatorname{ord}(g) \mid p$.

Jetzt zählen wir auf zwei Arten. Die Menge X hat $|G|^{p-1}$ Elemente, denn man kann die ersten $g_1,\ldots,g_{p-1}$ frei wählen und

$$g_p = (g_1 \ldots g_{p-1})^{-1}$$

ist dann eindeutig festgelegt und existiert. Damit ist $|X|$ durch p teilbar. Satz 12.5 besagt dann

$$|\mathrm{Fix}(Z,X)| \equiv |X| \equiv 0 \pmod{p}.$$

Jetzt kommt die Pointe. Aus dem unbrauchbaren Fixpunkt $(1,\ldots,1)$ folgt, daß

$$|\mathrm{Fix}(Z,X)| \ge 1$$

und da $|\mathrm{Fix}(Z,X)|$ durch p teilbar ist, folgt sogar $|\mathrm{Fix}(Z,X)| \ge p > 1$. Es muß also mindestens einen anderen Fixpunkt

$$(g,\ldots,g) \in \mathrm{Fix}(Z,X)$$

mit $g \neq 1$ geben! Dieses g ist das gesuchte Element der Ordnung p. □

[13] Augustin-Louis Cauchy, 1789–1857, französischer Mathematiker.

Bemerkung 12.7. Der Satz von Lagrange spricht eine Bedingung aus, die Untergruppen erfüllen müssen, wodurch die möglichen Untergruppen stark eingeschränkt werden. In Form des Korollars 4.16 wird daraus eine Bedingung an die Ordnung der Gruppenelemente. So gibt es in der S_6 beispielsweise kein Element der Ordnung 7, weil die davon erzeugte Untergruppe 7 Elemente hätte und $7 \nmid 6!$.

Der Satz von Cauchy, siehe Satz 12.6 spricht umgekehrt aus, daß zumindest für die Existenz von Gruppenelementen von Primzahlordnung die Bedingung aus dem Satz von Lagrange die einzige ist.

Beispiel 12.8. Satz 12.6 gilt nicht für Teiler der Gruppenordung, die keine Primzahl sind. Das einfachste Gegenbeispiel ist die kleinsche Vierergruppe $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Diese hat die Ordnung 4, aber kein Element der Ordnung 4. Für alle $g \in V_4$ gilt $2g = 0$, somit ist die Ordnung 1 oder 2, aber niemals 4.

Satz 12.9. *Jede p-Gruppe hat nichttriviales Zentrum.*

Beweis. Das Zentrum ist die Menge der Fixpunkte der Konjugationsoperation. Satz 12.5 besagt dann

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p}.$$

Jetzt kommt dieselbe Pointe wie im Beweis des Satzes von Cauchy, Satz 12.6. Das neutrale Element gehört zum Zentrum $Z(G)$, also ist $|Z(G)| \geq 1$. Da es sich um ein Vielfaches von p handelt, gilt sogar $|Z(G)| \geq p > 1$, und somit ist das Zentrum nicht trivial. □

12.3. **Gruppen der Ordnung p^2.** In Satz 4.22 haben wir alle Gruppen von Primzahlordnung bis auf Isomorphie bestimmt. Das sind genau die zyklischen Gruppen, also $\mathbb{Z}/p\mathbb{Z}$ bis auf Isomorphie.

Proposition 12.10. *Sei G eine Gruppe, so daß $G/Z(G)$ eine zyklische Gruppe ist. Dann ist G abelsch.*

Beweis. Sei g ein Vertreter der erzeugenden Nebenklasse von $G/Z(G)$. Dann erzeugen $Z(G)$ und g die Gruppe G. Allerdings kommutieren $Z(G)$ und g, so daß G abelsch sein muß:

Zwei beliebige Elemente von G haben die Form $x = g^n a$ und $y = g^m b$ mit $n, m \in \mathbb{Z}$ und $a, b \in Z(G)$. Dann gilt

$$xy = (g^n a)(g^m b) = g^n g^m ab = g^m g^n ba = g^m b g^n a = yx.$$ □

Korollar 12.11. *Sei p eine Primzahl. Eine Gruppe G der Ordnung p^2 ist abelsch.*

Beweis. Als p-Gruppe hat G nach Satz 12.9 nichttriviales Zentrum $Z(G) \neq 1$. Wenn $Z(G) = G$ sind wir fertig. Nach dem Satz von Lagrange, Satz 4.13, kann andernfalls nur noch $|Z(G)| = p$ sein. Aber dann hat $G/Z(G)$ auch p Elemente und ist somit zyklisch wegen Satz 4.22. Das ist ein Widerspruch zu Proposition 12.10. □

Korollar 12.12. *Sei p eine Primzahl. Eine Gruppe G der Ordnung p^2 ist isomorph zu entweder*

$$\mathbb{Z}/p^2\mathbb{Z} \qquad \text{oder} \qquad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Beweis. Korollar 12.11 besagt, daß G abelsch ist. Wir verwenden daher additive Notation. Die Elemente $g \in G$, $g \neq 0$ haben Ordnung p oder p^2 nach Korollar 4.16. Wenn $g \in G$ die Ordnung p^2 hat, dann ist

$$\mathbb{Z}/p^2\mathbb{Z} \simeq \langle g \rangle = G,$$

nach Satz 2.32.

Wir nehmen nun an, daß alle $x \in G$, $x \neq 0$ die Ordnung p haben. Sei $x \in G$, $x \neq 0$. Dann ist $\langle x \rangle$ eine zyklische Untergruppe der Ordnung p, und es gibt $y \in G \setminus \langle x \rangle$. Dann gilt

$$\langle x \rangle \subsetneq \langle x, y \rangle \subseteq G$$

und nach dem Satz von Lagrange, Satz 4.13, ist $|\langle x,y\rangle|$ ein Teiler von p^2, aber $> p = |\langle x\rangle|$. Daher ist $G = \langle x,y\rangle$. Die Abbildung

$$f : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G, \qquad f(n,m) = nx + my$$

ist ein Gruppenhomomorphismus, weil G abelsch ist. Das Bild enthält x, y, also $\langle x,y\rangle = G$ und f ist surjektiv. Da $|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}| = |G|$ gilt, muß f bijektiv sein. Daher ist f ein Gruppenisomorphismus. □

Beispiel 12.13. Gruppen der Ordnung p^3 sind nicht zwingend abelsch. Die Gruppe der unipotenten oberen Dreiecksmatrizen in $\mathrm{GL}_3(\mathbb{F}_p)$

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \; ; \; x,y,z \in \mathbb{F}_p \right\} \subseteq \mathrm{GL}_3(\mathbb{F}_p)$$

hat Ordnung p^3 und ist nicht kommutativ:

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

führt zu

$$AB = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = BA.$$

13. Sylow-Sätze

Fundamental für die Strukturtheorie endlicher Gruppen sind die Sylow-Sätze[14]. Wir folgen den Beweisen von Wielandt[15] aus dem Jahr 1959 (Publikationsdatum), deren zentrales Hilfsmittel Gruppenoperationen sind.

Definition 13.1. Eine **Sylow-(Unter)gruppe** ist eine Untergruppe $P \subseteq G$ einer endlichen Gruppe G, deren Ordnung eine Primzahlpotenz $|P| = p^r$ ist, so daß $|G| = p^r m$ mit $p \nmid m$, also eine maximale p-Untergrupe von G. Wenn man die Primzahl betonen möchte, spricht man von einer **p-Sylow-(Unter)gruppe** von G.

Theorem 13.2 (Sylow–Sätze, 1872)**.** *Sei G eine endliche Gruppe der Ordnung N und p ein Primteiler von N. Sei $N = p^r m$ mit $p \nmid m$.*

(1) Es gibt eine p-Sylow-Untergruppe in G.
(2) Jede p-Untergruppe von G ist in einer p-Sylow-Untergruppe enthalten.
(3) Je zwei p-Sylow-Untergruppen von G sind konjugiert.
(4) Sei $a_p = a_p(G)$ die Anzahl der p-Sylow-Untergruppen von G. Dann gilt
  (i) $a_p \mid |G|$,
  (ii) $a_p \equiv 1 \pmod p$.

Bevor wir in den Beweis einsteigen, benötigen wir ein paar Lemmata.

Lemma 13.3. *Sei R ein Ring mit $p \cdot 1 = 0$. Dann ist für alle $a, b \in R$*

$$(a+b)^p = a^p + b^p.$$

Beweis. Nach dem binomischen Lehrsatz reicht es, für alle $1 \le k \le p-1$ zu zeigen, daß

$$p \mid \binom{p}{k}.$$

[14] Peter Ludwig Mejdell Sylow, 1832–1918, norwegischer Mathematiker.
[15] Helmut Wielandt, 1910–2001, deutscher Mathematiker.

Dies folgt aber auch aus dem Spezialfall für $a = X$ und $b = 1$ im Polynomring $\mathbb{F}_p[X]$ wieder aus dem binomischen Lehrsatz: zu zeigen ist also in $\mathbb{F}_p[X]$

$$(X+1)^p = X^p + 1.$$

Wir schreiben $f(X) = (X+1)^p - X^p - 1$, ein Polynom vom Grad $\leq p-1$. Nach dem kleinen Fermat gilt für alle $n \in \mathbb{Z}$

$$(n+1)^p \equiv n + 1 \equiv n^p + 1 \pmod{p}.$$

Daher hat $f(X)$ die p-vielen verschiedenen Nullstellen der Reste $0, 1, \ldots, p-1$ modulo p. Das geht für ein Polynom vom Grad $< p$ nur, wenn es das Nullpolynom $f(X) = 0$ ist. □

Proposition 13.4. *Sei $n = p^r \cdot m$ mit $p \nmid m$. Dann gilt*

$$\binom{n}{p^r} \equiv m \pmod{p}.$$

Beweis. Wir müssen den Koeffizienten von X^{p^r} in $(X+1)^n \in \mathbb{F}_p[X]$ ausrechnen. Das geht mit Lemma 13.3 so:

$$(X+1)^n = \big((X+1)^{p^r}\big)^m = (X^{p^r}+1)^m = 1 + \binom{m}{1} X^{p^r} + \binom{m}{2} X^{2p^r} + \ldots = 1 + mX^{p^r} + \ldots \quad \square$$

13.1. **Der Beweis der Sylow-Sätze.**

Beweis von Theorem 13.2. (1) Wir zeigen nun die Existenz einer p-Sylow-Untergruppe. Sei G eine endliche Gruppe der Ordnung N, sei p eine Primzahl und $N = p^r m$ mit $p \nmid m$. Wenn $r = 0$ ist, so ist nichts zu tun. Sei daher $r \geq 1$. Sei

$$X = \{M \ ; \ M \subseteq G \text{ und } |M| = p^r\}$$

die Menge der p^r-elementigen Teilmengen. Da Translation eine freie Operation ist, gilt für jedes $g \in G$ und $M \in X$, daß

$$|gM| = |M|.$$

Daher operiert G auf X durch (Links-)Translation:

$$G \times X \to X$$
$$(g, M) \mapsto gM.$$

Behauptung: Sei $M \in X$ beliebig. Der Stabilisator G_M hat höchstens p^r Elemente.

Wir fixieren ein $x \in M$. Ein $g \in G_M$ ist dann eindeutig durch $gx \in M$ festgelegt als $g = (gx)x^{-1}$. Daher ist

$$|G_M| \leq |M| = p^r.$$

Wir suchen also ein $M \in X$ mit maximal möglichem Stabilisator. Wir arbeiten durch Widerspruch und nehmen an, daß alle Stabilisatoren G_M weniger als p^r Elemente haben. Es gilt nach dem Bahnensatz

$$p^r \mid |G| = |G_M| \cdot |G.M|.$$

Da $|G_M| < p^r$, gilt $p^r \nmid |G_M|$ und daher $p \mid |G.M|$. Es sind also alle Bahnenlängen durch p teilbar. Damit gilt

$$p \mid |X| = \binom{N}{p^r}$$

im Widerspruch zu Proposition 13.4. Also gibt es einen Stabilisator $P = G_M$ der Ordnung p^r. Dies ist die gesuchte p-Sylow-Untergruppe.

(2) Sei P eine p-Sylow-Untergruppe von G, die es nach (1) gibt. Sei Q eine beliebige p-Untergruppe. Wir lassen Q auf G/P durch Linkstranslation operieren. Nach Satz 12.5 gilt

$$|\operatorname{Fix}(Q, G/P)| \equiv |G/P| = |G|/|P| = m \not\equiv 0 \pmod{p}$$

und $|\operatorname{Fix}(Q, G/P)|$ ist daher nicht durch p teilbar. Es muß also einen Fixpunkt geben. Wenn gP von Q fixiert wird, dann ist

$$QgP = gP$$

oder äquivalent (Satz 4.38 bestimmt den Stabilisator von gP als Konjugierten des Stabilisators von P, also P)

$$Q \subseteq gPg^{-1}.$$

Mit P hat auch gPg^{-1} genau p^r Elemente und ist eine p-Sylow-Untergruppe. Damit ist Q in einer p-Sylow-Untergruppe enthalten.

(3) Sei P eine p-Sylow-Untergruppe von G, die es nach (1) gibt. Sei Q eine beliebige p-Sylow-Untergruppe. Der Beweis von (2) liefert ein $g \in G$ mit

$$Q \subseteq gPg^{-1}.$$

Da $|Q| = p^r = |gPg^{-1}|$, folgt Gleichheit. Je zwei p-Sylow-Untergruppen sind also konjugiert.

(4) Wir lassen nun G durch Konjugation auf der Menge der p-Sylow-Untergruppen

$$\mathfrak{P} = \{P \ ; \ P \text{ ist } p\text{-Sylow-Untergruppe von } G\}$$

operieren. Diese Operation ist wohldefiniert, denn konjugierte Untergruppen haben die gleiche Ordnung. Nach (2) ist diese Operation transitiv. Sei $P \in \mathfrak{P}$ und $N_G(P)$ der Stabilisator von P unter Konjugation mit G. Nach dem Satz von Lagrange, Satz 4.13,

$$a_p = |\mathfrak{P}| = (G : N_G(P) \mid |G|.$$

Dies zeigt (i).

Nun sei Q eine beliebige p-Sylow-Untergruppe. Wir lassen Q auf $\mathfrak{P}$ durch Konjugation operieren. Dann gilt nach Satz 12.5

$$a_p \equiv |\operatorname{Fix}(Q, \mathfrak{P})| = |\{P \in \mathfrak{P} \ ; \ Q \subseteq N_G(P)\}|.$$

Der Stabilisator $N_G(P)$ von P enthält P als normale Untergruppe. Eine p-Sylow-Untergruppe Q von G mit $Q \subseteq N_G(P)$ ist auch p-Sylow-Untergruppe von $N_G(P)$, denn $|N_G(P)|$ teilt $|G|$ und wird daher nicht durch mehr p-Faktoren geteilt als $|G|$. Daher sind nach (3) angewandt auf $N_G(P)$ die Gruppen P und Q durch ein $g \in N_G(P)$ konjugiert! Dann gilt

$$Q = gPg^{-1} = P.$$

Die p-Sylow-Untergruppe Q ist also der einzige Fixpunkt, somit zeigt Satz 12.5 die Kongruenz

$$a_p \equiv 1 \mod p,$$

und das ist Aussage (ii). □

13.2. **Anwendungen der Sylow-Sätze.**

Korollar 13.5. *Je zwei p-Sylow-Gruppen von G sind zueinander isomorph.*

Beweis: Aus Theorem 13.2 (3) folgt: sind S_1 und S_2 zwei p-Sylow-Gruppen von G, dann gibt es ein $g \in G$ so daß

$$S_2 = gS_1g^{-1}. \tag{13.1}$$

Somit definiert die Abbildung

$$g(-)g^{-1} : S_1 \to S_2$$
$$h \mapsto ghg^{-1}$$

einen Isomorphismus von S_1 mit S_2. In der Tat ist $g(-)g^{-1}$ als Einschränkung eines inneren Automorphismus von G injektiv und wegen (13.1) auch surjektiv. □

Korollar 13.6. *Eine p-Sylow-Gruppe von G ist ein Normalteiler von G genau dann, wenn $a_p(G) = 1$.*

Beweis: Ganz allgemein ist eine Untergruppe $H \leq G$ ein Normalteiler genau dann, wenn für alle $g \in G$ gilt

$$gHg^{-1} = H,$$

also wenn die Menge der zu H konjugierten Untergruppen nur aus H selbst besteht. Für eine p-Sylow-Gruppe $S \leq G$ besteht diese Menge nach Theorem 13.2 (3) genau aus der Menge aller p-Sylow-Gruppen von G. Somit ist S Normalteiler genau dann, wenn $a_p(G) = 1$. □

Als Anwendung der Sylow–Sätze beweisen wir den folgenden Struktursatz. Für den Begriff des semi-direkten Produkts verweisen wir auf [MK13] Beispiel 4.8 und auf Abschnitt 4.5.

Satz 13.7. *Seien $p \neq q$ Primzahlen und G eine Gruppe der Ordnung $|G| = p^2q$.*

(1) Eine p-Sylowuntergruppe oder eine q-Sylowuntergruppe ist ein Normalteiler.

(2) Sei N eine normale Sylowuntergruppe und H eine Sylowuntergruppe zum anderen Primteiler. Dann ist

$$G = N \rtimes H$$

ein semi-direktes Produkt bezüglich der Gruppenwirkung

$$\alpha : H \subseteq G \xrightarrow{g \mapsto g(-)g^{-1}|_N} \mathrm{Aut}(N).$$

Beweis. (1) Wenn es nur eine p-Sylowuntergruppe gibt, ist diese Normalteiler und (1) gilt. Ansonsten folgt aus den Sylow-Sätzen für die Anzahl der p-Sylowuntergruppen $a_p(G) = q$ und $q \equiv 1 \pmod{p}$. Insbesondere ist dann $q > p$.

Die Anzahl $a_q(G)$ der q-Sylowunterguppen ist $\equiv 1 \pmod{q}$ und als Teiler von p^2 eine der Möglichkeiten $1, p, p^2$. Weil $q > p$, kommt $a_q(G) = p$ nicht in Frage. Bei $a_q(G) = 1$ ist die q-Sylowuntergruppe normal. Es bleibt, $a_q(G) = p^2$ zu behandeln.

Die q-Sylowuntergruppe hat q Elemente und ist daher zyklisch nach Satz 4.22. Zwei verschiedene q-Sylowuntergruppen schneiden sich daher nur in 1: der Schnitt ist eine Untergruppe und hat nach dem Satz von Lagrange entweder 1 oder q Elemente, da q eine Primzahl ist.

Wir zählen nun die Elemente von Ordnung q in G. Diese Elemente erzeugen jeweils eine zyklische Gruppe der Ordnung q, eine q-Sylowuntergruppe. Daher

$$|\{g \in G \,;\, \mathrm{ord}(g) = q\}| = \Big|\bigcup_{U \subseteq G,\ q\text{-Sylow}} U \setminus \{0\}\Big| = a_q(G) \cdot (q-1) = p^2(q-1) = |G| - p^2.$$

Jede p-Sylowuntergruppe von G ist enthalten im Komplement aller q-Sylowuntergruppen. Da ist nur Platz für genau p^2-viele Elemente, also eine p-Sylowuntergruppe. Folglich ist $a_p(G) = 1$ im Widerspruch zur anfänglichen Annahme.

(2) Seien N und H wie im Satz. Die induzierte Abbildung $f : H \to G/N$ ist injektiv, weil $\ker(f) = N \cap H$ als Schnitt von Gruppen teilerfremder Ordnung $= 1$ ist und weil $|H| = |G/N|$. Daher ist

$$NH = G.$$

Die Abbildung

$$\varphi : N \rtimes_\alpha H \to G, \qquad \varphi(n, h) = nh$$

liefert einen Gruppenhomorphismus, wie man leicht aus der Definition von α und dem semi-direkten Produkt nachrechnet:

$$\varphi(n,h)\varphi(m,g) = nhmg = n(hmh^{-1})hg = n\alpha_h(m)hg = \varphi(n\alpha_h(m), hg) = \varphi((n,h)(m,g)).$$

Wegen $NH = G$ ist φ surjektiv und ein Isomorphismus wegen $|N \rtimes_\alpha H| = |N| \cdot |H| = |G|$. □

Übungsaufgaben zu §13

Übungsaufgabe 13.1. Zeigen Sie, daß jede Gruppe der Ordnung 15 zyklisch ist.

Übungsaufgabe 13.2. Seien p, q zwei verschiedene Primzahlen. Zeigen Sie, daß jede Gruppe der Ordnung pq einen Normalteiler hat.

Übungsaufgabe 13.3. Seien $p < q$ zwei Primzahlen mit $p \nmid q - 1$. Zeigen Sie, daß jede Gruppe der Ordnung pq zyklisch ist.

Übungsaufgabe 13.4. Welche $n \leq 100$ haben die Eigenschaft: alle Gruppen der Ordnung n sind zyklisch?

Teil 4. Appendix

Anhang A. Der Quotientenkörper

Satz A.1. *Ein Ring R ist ein Integritätsring genau dann, wenn es einen Körper K gibt, so daß R isomorph ist zu einem Unterring von K.*

Beweis. Offensichtlich erbt ein Ring, der isomorph zu einem Teilring eines Körpers ist, von diesem die Kürzungsregel und ist demnach auch ein Integritätsring.

Sei also umgekehrt R ein Integritätsring. Wir müssen einen Körper konstruieren, der einen zu R isomorphen Teilring enthält. Dies ist die gleiche Konstruktion wie die von $\mathbb{Q}$ aus $\mathbb{Z}$. Auf der Menge

$$R \times (R \setminus \{0\})$$

definieren wir eine Äquivalenzrelation durch

$$(a, b) \sim (c, d) \iff ad - bc = 0.$$

Diese Relation ist offensichtlich symmetrisch und reflexiv. Zur Transitivität nehmen wir $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$, also $ad = bc$ und $cf = de$. Dann folgt

$$d(af) = (ad)f = (bc)f = b(cf) = b(de) = d(be).$$

Aufgrund der Kürzungsregel folgt dann $af = be$, also $(a, b) \sim (e, f)$. Wir schreiben für die Äquivalenzklasse von (a, b) suggestiv

$$\frac{a}{b},$$

denn die Äquivalenzrelation entspricht dann durch Erweitern und Kürzen sich entsprechenden Brüchen: für $(a, b) \sim (c, d)$

$$\frac{a}{b} = \frac{ac}{bc} = \frac{ac}{ad} = \frac{c}{d}.$$

Die Menge der Äquivalenzklassen bezeichnen wir als **Quotientenkörper** von R

$$\mathrm{Quot}(R) = \left\{ \frac{a}{b} \;;\; a, b \in R, b \neq 0 \right\}.$$

Diese Terminologie rechtferigen wir dadurch, daß wir auf $\mathrm{Quot}(R)$ eine Ringstruktur definieren, die ein Körper ist und die einen zu R isomorphen Teilring hat.

Die Addition auf $\mathrm{Quot}(R)$ ist definiert durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}.$$

Die Multiplikation auf $\mathrm{Quot}(R)$ ist definiert durch

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Wohldefiniertheit und Ringaxiome werden mit einfachen, aber umfangreichen Rechnungen bewiesen. Diese lassen wir zur Übung. Der Ring $\mathrm{Quot}(R)$ ist ein Körper, da $\frac{a}{b} = 0 = \frac{0}{1}$ genau wenn $a = 0$, und für $a, b \in R \setminus \{0\}$ folgt

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

Die Abbildung

$$R \to \mathrm{Quot}(R), \qquad a \mapsto \frac{a}{1}$$

ist ein Ringhomomorphismus. Dieser ist injektiv und damit R isomorph zum Bild (Homomorphiesatz), einem Teilring im Körper $\mathrm{Quot}(R)$. □

Anhang B. Euklidische und nicht-euklidische Hauptidealringe

Beispiel B.1. Der Unterring von $\mathbb{C}$

$$\mathbb{Z}[i] = \{a + bi \ ; \ a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

ist ein euklidischer Ring, insbesondere ein Hauptidealring. Als euklidische Gradfunktion dient

$$N(a + bi) = a^2 + b^2 = (a + bi)(a - bi).$$

Diese **Norm** ist multiplikativ:

$$N(zw) = zw \cdot \overline{zw} = z\bar{z} \cdot w\bar{w} = N(z)N(w).$$

Beim Nachweis der Division mit Rest bezüglich $N(-)$ hilft die geometrische Vorstellung: $\mathbb{C}$ als Ebene $\mathbb{R}^2$ und $\mathbb{Z}[i] \subseteq \mathbb{C}$ als Menge der Gitterpunkte mit ganzzahligen Koeffizienten $\mathbb{Z}^2 \subseteq \mathbb{R}^2$. Die Norm $N(z)$ ist dann nichts anderes als das Quadrat des komplexen Absolutbetrags, also das Quadrat der euklidischen Länge von z: des Abstands von z und 0.

Sei $x \in \mathbb{Z}[i]$ und $0 \neq d \in \mathbb{Z}[i]$. In $\mathbb{C}$ können wir x/d betrachten. Dazu gibt es einen „nächsten Nachbarn“ $q \in \mathbb{Z}[i]$ mit $|x/d - q|^2 \leq 1/2$, das Quadrat der Länge der halben Diagonale eines Einheitsquadrats. Nach Multiplikation mit d ergibt sich für $r = d(x/d - q) = x - dq \in \mathbb{Z}[i]$

$$N(r) = |x - dq|^2 = |d|^2 \cdot |x/d - q|^2 \leq N(d)/2 < N(d),$$

bei $x = qd + r$. Dies etabliert Division mit Rest bezüglich der euklidischen Gradfunktion $N(-)$.

Beispiel B.2. Sei R ein euklidischer Ring mit euklidischer Gradfunktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$. Sei n_0 der kleinste Wert im Bild von δ. Dann ist

$$\delta^{-1}(n_0) \subseteq R^\times,$$

denn bei Division mit Rest von 1 durch u mit $\delta(u) = n_0$

$$1 = qu + r$$

gilt $\delta(u) > \delta(r) \geq n_0 = \delta(u)$, falls $r \neq 0$. Dies geht nicht, also muß $r = 0$ sein. Damit ist $1 = qu$ und u eine Einheit.

Sei R kein Körper und $x \in R \setminus R^\times$, $x \neq 0$ mit $\delta(x)$ minimal unter den Werten von δ auf Nichteinheiten. So ein x gibt es, da R kein Körper ist und weil jede nichtleere Teilmenge von $\mathbb{N}_0$ ein minimales Element hat.

Für dieses x ist $(x) \subseteq R$ ein echtes Ideal. Wir betrachten den Faktorring $R/(x)$. Jedes Element $0 \neq \alpha \in R/(x)$ darin hat einen Repräsentanten aus $R^\times$. In der Tat, für $\alpha = a + (x)$ macht man Division mit Rest

$$a = qx + r$$

und

$$a + (x) = r + (x).$$

Wegen $r = 0$ oder $\delta(r) < \delta(x) =: n_1$ ist $\alpha = 0$ oder mit Repräsentant r, einer Einheit nach Wahl von n_1. Damit gilt

$$|R^\times| + 1 \geq |R/(x)|. \tag{B.1}$$

Wir suchen nun einen Hauptidealring, der nicht euklidisch ist. Sei

$$R = \{a + b\frac{1 + \sqrt{-19}}{2} \ ; \ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Man rechnet leicht nach, daß dies ein Unterring von $\mathbb{C}$ ist. Schwieriger sind die restlichen Behauptungen, für die wir auf eine Zahlentheorievorlesung verweisen:

(a) R ist ein Hauptidealring.
(b) $R^\times = \{\pm 1\}$.

Wir führen nun die Annahme zu einem Widerspruch, R sei euklidisch. Dazu reicht es nach (B.1) aus nachzuweisen, daß R keinen Faktorring $R/(x)$ mit ≤ 3 Elementen hat. Ein Ring mit 2 Elementen ist notwendigerweise isomorph zu $\mathbb{Z}/2\mathbb{Z}$ und einer mit 3 Elementen notwendigerweise isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Im ersten Fall ist $2 \in (x)$ und damit

$$R/(2) \twoheadrightarrow R/(x).$$

Aber $R/(2)$ ist ein Körper mit 4 Elementen und hat demnach keinen Faktorring mit 2 Elementen. Genauso folgt im zweiten Fall $3 \in (x)$ und

$$R/(3) \twoheadrightarrow R/(x).$$

Aber $R/(3)$ ist ein Körper mit 9 Elementen und hat demnach keinen Faktorring mit 3 Elementen. Dies ist der gesuchte Widerspruch zur Existenz einer euklidischen Gradfunktion.

Jakob Stix, Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Str. 6–8, 60325 Frankfurt am Main, Germany
E-mail address: stix@math.uni-frankfurt.de