Grundlagen der Algebra

für Bachelor und L3 — Sommersemester 2014

GOETHE–UNIVERSITÄT FRANKFURT

JAKOB STIX

Zusammenfassung. — Die Vorlesung behandelt die grundlegende Theorie zu den algebraischen Grundbegriffen Gruppe, Ring und Körper. Thema sind insbesondere die Isomorphiesätze, Quotientenstrukturen, Gruppenoperationen, euklidsche Ringe, und endliche Körper. Als Anwendung beweisen wir die Jordannormalform für lineare Abbildungen.

Dieses Skript zur Vorlesung Grundlagen der Algebra befindet sich noch in der Entstehung und wird fortlaufend aktualisiert. Es muß davon ausgegangen werden, daß es noch einige Zeit dauern wird, bis eine stabile Version entstanden ist und die gröbsten Fehler korrigiert sind. Sie lesen das Skript **auf eigene Gefahr!**

Bitte teilen Sie mir Korrekturvorschläge per Email oder persönlich nach der Vorlesung mit.

Das Bonusmaterial in Kleindruck enthält historische Bezüge, weitere Kommentare, oder Vorgriffe zur Einordnung in der breiteren/höheren Kontext. Es ist nicht klausurrelevant.

Inhaltsverzeichnis

Danksagung 2
Einführung 3
Literatur 6

Teil 1. Gruppen und Gruppenoperationen 7
1. Gruppen 7
1.1. Definition und erste Beispiele 7
1.2. Erste Folgerungen 8
1.3. Untergruppen 9
1.4. Ordnung 11
1.5. Erzeugende 12
2. Operationen 14
2.1. Definition und erste Beispiele 14
2.2. Stabilisator und Orbit 15
2.3. Die Bahnenformel und Anwendungen 16
2.4. Zur symmetrischen Gruppe 19
2.5. Elemente von Primzahlordnung 21
3. Operationen von Gruppen auf Gruppen 23
3.1. Translation 23
3.2. Gruppenhomomorphismen 28
3.3. Konjugation 33
4. Quotienten und Isomorphiesätze 36
4.1. Konjugation von Untergruppen 36
4.2. Quotienten 37
4.3. Die Isomorphiesätze 41
5. Beispiele und Konstruktionen mit Gruppen 44
5.1. Zyklische Gruppen 44

5.2. Produkte 47
5.3. Semidirekte Produkte 49
5.4. Das Zentrum 50
5.5. Kommutatoren und abelsche Quotienten 50

Teil 2. Ringe 52
6. Ringe 52
6.1. Definition und Beispiele 52
6.2. Einheiten 55
6.3. Homomorphismen 55
6.4. Ideale und Faktorringe 58
6.5. Quotienten und Isomorphiesätze 59
7. Hauptidealringe 62
7.1. Integritätsringe und Hauptidealringe 62
7.2. Euklidische Ringe 64
7.3. Das Minimalpolynom 66
7.4. Primideale und maximale Ideale 67
8. Arithmetik in Hauptidealringen 69
8.1. Teilbarkeit in Integritätsringen 69
8.2. Der ggT und das kgV 70
8.3. Der euklidische Algorithmus in euklidischen Ringen 71
8.4. Primelemente und irreduzible Elemente 72
8.5. Die Eindeutigkeit der Primzerlegung in Hauptidealringen 75
8.6. Das Minimalpolynom und Teilbarkeit 77
8.7. Der Chinesische Restsatz 79
9. Die Jordannormalform 81
9.1. Invariante Unterräume 81
9.2. Begleitmatrix und Jordanblock 83
9.3. Die Jordannormalform im zerfallenden Fall 87
9.4. Was im nicht-zerfallenden Fall passiert 90

Danksagung. Ich möchte mich gerne bei allen bedanken, insbesondere bei den Studierenden Adrian Baumann, Sebastian Groß, Simone Jablonski, Theresa Kumpitsch, Denise Melchin, Carolin Müller, Phuong Bao Pham 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.

Das Bonusmaterial in Kleindruck enthält historische Bezüge, weitere Kommentare, oder Vorgriffe zur Einordnung in der breiteren/höheren Kontext.

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 bildet 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 Gefand über C*-Algebren, das jede solche C*-Algebra A mit dem Ring der stetigen Funktionen auf dem Spektrum von A identifiziert.

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

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

[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 $M = \mathbb{N}$.

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 $n \mod p$. 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 angenommen werden, so zum Beispiel die 0.

Quadratische Gleichunge wie etwa

$$X^2 + 1 = 0$$

haben keine relle 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 eine einzige Zahl i wird aus $\mathbb{R}$ ein Körper, der immer noch vollständig bezüglich Cauchy–Folgen zum natürlich erweiterten Abstandsbegriffs 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 im vorherigen Abschnitt 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-kommutative 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 Transformation 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.

[Me75] Kurt Meyberg, *Algebra, Teil 1*, Mathematische Grundlagen für Mathematiker, Physiker und Ingenieure, Carl Hanser Verlag, München–Wien, 1975, 192 Seiten.

[Me76] Kurt Meyberg, *Algebra, Teil 2*, Mathematische Grundlagen für Mathematiker, Physiker und Ingenieure, Carl Hanser Verlag, München–Wien, 1976, 182 Seiten.

Teil 1. Gruppen und Gruppenoperationen

1. Gruppen

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

Definition 1.1. Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung

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

mit den folgenden Eigenschaften.

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

$$g(hk) = (gh)k,$$

wobei die Klammerung die Reihenfolge festlegt, in der die Verknüpfungen auszuführen sind.

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

$$ge = g = eg.$$

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

$$gh = e = hg.$$

Notation 1.2. Um die Verknüpfung zweier Gruppenelemente zu bezeichenen, sind verschiedenste Notationen gebräuchlich, etwa

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

Bemerkung 1.3. (1) Strenggenommen ist eine Gruppe ein Paar $(G, \circ)$, wobei G eine Menge und $\circ : G \times G \to G$ eine Verknüpfung wie in der Definition 1.1 ist. Die verkürzte Notation G für das Paar $(G, \circ)$ entspringt dem Versuch, die Notation knapp und damit übersichtlicher zu halten.

(2) 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*[3] sind, bewiesen werden. Das gelingt durch vollständige Induktion nach der Länge r, aber damit wollen wir uns nicht aufhalten.

(3) Man kann die Axiome einer Gruppe abschwächen und zu einem äquivalenten Begriff kommen. Es reicht zum Beispiel, nur die Existenz eines linksneutralen Elements und eines Linksinversen zu verlangen, siehe [Me75] §1.3. 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. (1) Die kleinste Gruppe ist $G = \{e\}$ mit der einzig möglichen Verknüpfung

$$ee = e.$$

Diese Gruppe nennt man die triviale Gruppe.

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

[3] Es gibt das geflügelte Wort unter Mathematikern, daß man den Fehler in einem Beweis dadurch findet, daß man sich die Stellen genauer anschaut, in dem Beweisschritte durch Worte wie 'offensichtlich', 'trivialerweise gilt', 'wie man leicht sieht' oder ähnliches begründet werden.

(3) Sei $n \geq 1$ eine natürliche Zahl. Die symmetrische Gruppe S_n der Menge aller Permutationen (bijektiven Selbstabbildungen) der Menge $\{1, \ldots, n\}$ ist aus der linearen Algebra bekannt. Die Verknüpfung ist die Komposition der Permutationen. Die symmetrische Gruppe ist nichts weiter als die volle Gruppe der Symmetrien der unstrukturierten Menge von n Elementen.

(4) Sei K ein Körper und V ein K-Vektorraum. Dann ist die Menge $\mathrm{GL}(V)$ der bijketiven linearen Abbildungen $f : V \to V$ die **allgemeine**[4] **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.

(5) Speziell für $V = K^n$ setzen wir $\mathrm{GL}_n(K) = \mathrm{GL}(K^n)$. Und weiter für $n = 1$ erhalten wir

$$K^\times = \mathrm{GL}_1(K)$$

die Teilmenge $K^\times = K \setminus \{0\}$ des Körpers, welche mit der Multiplikation als Verknüpfung eine Gruppe bildet. Diese wird **multiplikative Gruppe** von K genannt. Körpermultiplikation und Matrixmultiplikation in $\mathrm{GL}_1(K)$ entsprechen sich.

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. 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 der Gruppe.

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**[5] Gruppe.

Bemerkung 1.7. 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.

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

Proposition 1.8. *In jeder Gruppe ist das neutrale Element eindeutig.*

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

$$e = ee' = e'.$$

□

Notation 1.9. Das nach Proposition 1.8 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.

[4] Englisch: general linear group, daher GL

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

Proposition 1.10. *In jeder Gruppe ist das Inverse eines Elements eindeutig. Genauer: sei $g \in G$ ein Element einer Gruppe G und $h, h' \in G$ mit*

$$hg = e = h'g,$$

dann gilt $h = h'$ und h ist Inverses von g.

Beweis. Sei k ein Inverses zu g. Dann gilt

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

Da dieselbe Schlußfolgerung auch mit h' gilt, folgt $h = k = h'$. □

Notation 1.11. Das nach Proposition 1.10 eindeutige Inverse zu einem Element $g \in G$ wird mit

$$g^{-1}$$

bezeichnet, sofern die Verknüpfung multiplikativ geschrieben wird.

Proposition 1.12. *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 1.10, 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 1.10 zeigt $g = (g^{-1})^{-1}$. □

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

Definition 1.13. 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 1.14. (1) 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.

(2) Eine Untergruppe ist insbesondere mit der geerbten Verknüpfung selbst eine Gruppe.

Notation 1.15. (1) Wir werden eine Untergruppe U einer Gruppe G oft durch $U < G$ oder $U \leq G$ bezeichnen. Diese Notation ist aber nicht allgemeingültiger Standard.

(2) Für Teilmengen $A, B \subseteq G$ einer Gruppe G und ein Element $g \in G$ vereinbaren wir die Notationen

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

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

Proposition 1.16. *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) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a).

(a) $\Longrightarrow$ (b): Es gelte Aussage (a). Dann enthält U ein neutrales Element, ist also nicht leer, und per Defintion gilt $UU \subseteq U$. Es bleibt zu zeigen, daß auch $U^{-1} \subseteq U$. Hierfür beweisen wir zunächst, daß neutrales Element und das Inverse für $u \in U$ in G und U die gleichen sind.

Sei $\varepsilon \in U$ neutrales Element für die Gruppe U und ε^{-1} das Inverse von ε aufgefaßt als Element von G. Sei e das neutrale Element von G. Aus

$$e = \varepsilon^{-1}\varepsilon = \varepsilon^{-1}(\varepsilon\varepsilon) = (\varepsilon^{-1}\varepsilon)\varepsilon = e\varepsilon = \varepsilon$$

folgt, daß U das gleiche neutrale Element hat wie G.

Sein nun $u \in U$ beliebig, u^{-1} das Inverse Element in G und $v \in U$ das Inverse Element in U. Dann gilt

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

Dies zeigt zum einen, daß die Inversen von u in U und in G die gleichen sind, und zum andern bereits $U^{-1} \subseteq U$.

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

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

also gilt Aussage (c).

(c) $\Longrightarrow$ (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 und Aussage (a) gilt. □

Beispiel 1.17. (1) In jeder Gruppe G sind die triviale Gruppe $\{e\}$ und die ganze Gruppe G Untergruppen.
(2) Die Teilmenge $\{\pm 1\} \subset \mathbb{Q}^*$ ist eine Untergruppe (das ist gerade $\mathbb{Z}^\times$, vgl Kapitel §6).
(3) Der Einheitskreis $\mathrm{S}^1 = \{z \in \mathbb{C}^\times \ ; \ |z| = 1\} \subseteq \mathbb{C}^\times$.
(4) Sei $n \geq 1$ eine natürliche Zahl. Die alternierende Gruppe A_n ist eine Untergruppe von S_n, nämlich die Teilmenge derjenigen Permuationen mit Signum 1. Bezüglich des Signums einer Permutation verweisen wir auf die Lineare Algebra 1.

Bemerkung 1.18. Bei den Beispielen S^1 und A_n handelt es sich jeweils um das Urbild eines Wertes einer Abbildung, nämlich $z \mapsto |z|$ oder $\sigma \mapsto \mathrm{sign}(\sigma)$. Dies ist kein Zufall, aber hier besonders natürlich. Wir sehen später, daß beide Beispiele Kerne von Homomorphismen sind.

Beispiel 1.19. (4) $\mathrm{GL}_n(\mathbb{Q}) \subseteq \mathrm{GL}_n(\mathbb{R})$, oder allgemeiner für eine Körpererweiterung $K \subseteq L$ die Untergruppe

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

Wir erinnern nun an die Beschreibung aller Untergruppen von $\mathbb{Z}$ aus der Linearen Algebra 1.

Satz 1.20. *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 1.16, 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 $U = P \cup \{0\} \cup -P$, 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 $n = \min P$ Element in P.

Damit ist sicher $n\mathbb{Z} \subseteq U$. Nehmen wir an, daß es ein Element $g \in U \setminus n\mathbb{Z}$ gibt. Dann gibt[7] es ein $a \in \mathbb{Z}$ mit

$$na < g < (a + 1)n.$$

Mit g ist auch $h = g - an \notin U$, da sonst $g = h + an \in U$ wäre. Für h gilt aber die Abschätzung

$$0 < h < n,$$

also $h \in P$, was der Konstruktion von n als Minimum von P widerspricht. Es muß also $n\mathbb{Z} = U$ gelten. □

1.4. **Ordnung.** In multiplikativer Schreibweise kann man Gruppenelemente potenzieren.

Definition 1.21. Sei $g \in G$ ein Element einer Gruppe G mit neutralem Element e. Für $m \in \mathbb{Z}$ definieren wir

$$g^m = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{m\text{-mal}} & m \geq 1, \\ e & m = 0, \\ (g^{-1})^{-m} & m \leq -1. \end{cases}$$

Bemerkung 1.22. Die dritte Zeile ist wohldefiniert, da hier die erste Zeile Anwendung findet. Darüber hinaus ist nun der Ausdruck g^{-1} doppelt definiert. Das macht nichts, denn in beiden Varianten bedeutet g^{-1} das gleiche: das Inverse zu g.

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

Lemma 1.23. *Sei $g \in G$ ein Gruppenelement und $n, m \in \mathbb{Z}$. Dann gelten*

$$g^n \cdot g^m = g^{n+m},$$
$$(g^n)^m = g^{nm}.$$

Beweis. Trivial. □

Bemerkung 1.24. Man beachte hingegen, daß in der Regel für $g, h \in G$ und $n \in \mathbb{Z}$

$$(gh)^n \neq g^n h^n.$$

Lemma–Definition 1.25. *Sei $g \in G$ ein Gruppenelement. Dann ist*

$$\{a \in \mathbb{Z} \ ; \ g^a = e\}$$

*eine Untergruppe von $\mathbb{Z}$. Die **Ordnung** von g ist*

$$\operatorname{ord}(g) = \begin{cases} n & \text{wenn } n\mathbb{Z} = \{a \in \mathbb{Z} \ ; \ g^a = e\} \text{ und } n > 0, \\ \infty & \text{wenn } 0\mathbb{Z} = \{a \in \mathbb{Z} \ ; \ g^a = e\}. \end{cases}$$

[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.

[7] Das ist wieder nicht so einfach, wie es scheint.

Beweis. Man verifiziert sofort für $U = \{a \in \mathbb{Z} \;;\; g^a = e\}$ die Bedingung $UU \subseteq U$ und $U^{-1} \subseteq U$ aus Proposition 1.16(c): für $a, b \in U$ gilt $g^a = g^b = e$ also nach Lemma 1.23

$$g^{a-b} = g^a g^{-b} = e(g^b)^{-1} = ee^{-1} = e$$

und somit $a - b \in U$.

Die Beschreibung der Untergruppen von $\mathbb{Z}$ in Satz 1.20 zeigt, daß die Ordnung von g wohldefiniert ist. □

Bemerkung 1.26. Die angegebene Definition der Ordnung eines Elements ist elegant, aber nur zusammen mit dem Beweis von Satz 1.20 hilfreich. Ein Gruppenelement $g \in G$ von endlicher Ordnung hat die Ordnung

$$\operatorname{ord}(g) = \min\{m \;;\; m \in \mathbb{N}, m > 0, g^m = e\}$$

und für jedes $n \in \mathbb{Z}$ mit $g^n = e$ folgt $n \in \operatorname{ord}(g)\mathbb{Z}$, also

$$\operatorname{ord}(g) \mid n$$

($\operatorname{ord}(g)$ ist Teiler von n).

Beispiel 1.27. 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

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

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.

Definition 1.28. Die **Ordnung** einer Gruppe G ist die Mächtigkeit (die Anzahl der Elemente) $|G|$ der zugrundeliegenden Menge G.

1.5. **Erzeugende.** Untergruppen verhalten sich wohl bezüglich Schnitt.

Lemma 1.29. *Sei G eine Gruppe, I eine Menge und für jedes $i \in I$ eine Untergruppe $U_i \leq G$ gegeben. Dann ist*

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

eine Untergruppe von G.

Beweis. Wir weisen Proposition 1.16(c) nach. Für $u, v \in U$ gilt $u, v \in U_i$ für alle i. Damit nach Proposition 1.16(c) auch $uv^{-1} \in U_i$, und somit $uv^{-1} \in U$. □

Lemma–Definition 1.30. *Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Die **von S erzeugte Untergruppe** ist die kleinste Untergruppe von G, die S enthält. Als Notation verwenden wir*

$$\langle S \rangle \subseteq G.$$

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

Beweis. Wir müssen zeigen, daß es eine solche minimale Untergruppe gibt. Dazu betrachten wir den Schnitt aller Kandidaten und behaupten:

$$\langle S\rangle = \bigcap_{S\subseteq U,\ U\leq G} U.$$

Der Schnitt ist nicht leer, denn mindestens $U = G$ gibt es. Nach Lemma 1.29 ist der Schnitt selbst wieder eine Untergruppe und enthält per Konstruktion S. Weiter ist der Schnitt in jeder Untergruppe, die S enthält, selbst enthalten, also minimal mit dieser Eigenschaft. □

Definition 1.31. Ein **Erzeugendensystem** für eine Gruppe G ist eine Teilmenge $S \subseteq G$ mit

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

Bemerkung 1.32. Ist $S \neq \emptyset$, so kann man $\langle S\rangle$ auch konstruktiv beschreiben als die Menge aller endlichen Verknüpfungen von Elementen von $T = S \cup S^{-1}$, genauer

$$\langle S\rangle = \bigcup_{n\geq 1} \underbrace{T\cdot\ldots\cdot T}_{n\text{-mal}}$$

Offensichtlich ist die so erhaltene Menge in $\langle S\rangle$ enthalten und ist abgeschlossen unter der Gruppenverknüpfung. Um eine Untergruppe zu sein, und damit minimale S enthaltende Untergruppe zu sein, bedarf es nun der Abgeschlossenheit bezüglich des Inversennehmens. Die Verifikation dieser Behauptung überlassen wir zur Übung.

Bemerkung 1.33. 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[8] (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.

Übungsaufgaben zu §1

Übungsaufgabe 1.1. Sei $G = \{e, g\}$ eine Gruppe mit genau zwei Elementen: mit neutralem Element e und $g \neq e$. Zeigen Sie, daß dann $gg = e$ gelten muß.

Übungsaufgabe 1.2 (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. Zeige, daß $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$ eine Untergruppe von $\mathrm{GL}_2(\mathbb{C})$ ist.

Übungsaufgabe 1.3 (Quaternionengruppe). Wir betrachte 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 $z \in \{\pm 1, \pm i\}$ ist. Zeige, daß Q_8 eine Untergruppe aus 8 Elementen ist, von Elementen

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

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

erzeugt wird, wobei

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

und

$$ij = k.$$

Bestimme die Ordnung der Elemente von Q_8.

Übungsaufgabe 1.4. In der Regel gilt für Elemente $g, h \in G$ und $n \in \mathbb{Z}$ gilt 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. Zeigen Sie: eine Gruppe in der jedes nichttriviale Element die Ordnung 2 hat, ist eine abelsche Gruppe.

Übungsaufgabe 1.6. Sei g ein Gruppenelement der Ordnung n und $m \in \mathbb{Z}$. Bestimmen Sie die Ordnung von g^m.

Übungsaufgabe 1.7. 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 1.8. Weisen Sie nach, daß die Konstruktion von $\langle S \rangle$ aus Bemerkung 1.32 abgeschlossen ist unter dem Übergang zum inversen Element.

2. Operationen

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

2.1. Definition und erste Beispiele.

Definition 2.1. Eine Gruppenoperation (genauer Linksoperationen oder Operation von links) einer Gruppe G auf einer Menge X ist eine Abbildung

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g.x \end{aligned}$$

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 festlegt, in der die Verknüpfungen auszuführen sind.

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

$$e.x = x$$

Bemerkung 2.2. Man kann auch analog eine Operation von rechts definieren als eine Abbildung

$$\begin{aligned} X \times G &\to X, \\ (x, g) &\mapsto x.g \end{aligned}$$

mit den entsprechenden Eigenschaften. Man kann zwischen Links- und Rechtsoperationen übersetzen, indem man ein 'Vorzeichen spendiert', siehe Aufgabe 2.1.

Es folgen einige natürliche Beispiele.

Beispiel 2.3. (1) Die $\mathrm{GL}(V)$ operiert auf V vermöge Matrixmultiplikation von Matrix und Vektor.
(2) Die symmetrische Gruppe operiert auf $\{1,\dots,n\}$ qua Definition.
(3) Die Gruppe S^1 operiert auf $\mathbb{C} \simeq \mathbb{R}^2$ durch Multiplikation komplexer Zahlen.
(4) Die 3-dimensionale Drehgruppe $\mathrm{SO}(3)$ operiert auf der 2-Sphäre

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

Dazu später mehr in der Vorlesung Geometrie.
(5) Man vergleiche die formale Ähnlichkeit von Definition 2.1 mit der Definition einer Gruppe. Insbesondere operiert G auf $X = G$ vermöge der Gruppenmultiplikation.

2.2. **Stabilisator und Orbit.**

Satz–Definition 2.4. *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*

$$G_x = \{g \in G \; ; \; g.x = x\}$$

von 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 1.16, daß $G_x \subseteq G$ eine Untergruppe ist. □

Beispiel 2.5. (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 des Elements n für die definierende Operation von S_n auf $X = \{1,\dots,n\}$ besteht aus eindeutigen Fortsetzungen der Permutationen $\sigma \in S_{n-1}$ zu $\tilde{\sigma} \in S_n$ durch

$$\tilde{\sigma}(i) = \begin{cases} \sigma(i) & i < n \\ n & i = n \end{cases}$$

Die Zuordnung $\sigma \mapsto \tilde{\sigma}$ ist verträglich mit Komposition (also ein Gruppenisomorphismus, vgl. Definition 3.28), also ist der Stabilisator von $n \in X$ eine Kopie (isomorph zu) von 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: $G_0 = \mathrm{S}^1$.

Definition 2.6. Sei $G \times X \to X$ eine Operation der Gruppe G auf der Menge X.
(1) Der **Orbit** (oder G-**Orbit**, oder die **Bahn**) eines Elements $x \in X$ ist die Teilmenge

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

(2) Der **Raum der Orbits** oder **Orbitraum** 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 2.7. Die Orbits 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.

Satz 2.8. *Sei $G \times X \to X$ eine Operation der Gruppe G auf der Menge X.*

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

(2) Die Orbits der Operation von G auf X definieren eine Partition von X, die Zerlegung in Äquivalenzklassen für die Äquivalenzrelation $\sim$ auf X:

$$x \sim y \iff \text{es gibt ein } g \in G \text{ mit } x = g.y$$

Beweis. (1) Seien $x, y \in X$ zwei Elemente. Wenn $G.x \cap G.y = \emptyset$, dann ist nichts zu tun. Sei also $z \in G.x \cap G.y$. Dann gibt es $g, h \in G$ mit $g.x = z = h.y$, woraus

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

folgt. Wir kürzen $k = g^{-1}h$ ab und sehen

$$G.x = G.(k.y) = (Gk).y = G.y$$

was zu beweisen war.

Aussage (2) ist nur eine Umformulierung von Aussage (1), angewandt auf alle Orbits. □

Definition 2.9. Eine **transitive Operation** ist eine Operation mit nur einem Orbit, d.h. eine Operation $G \times X \to X$ so daß für alle $x, y \in X$ ein $g \in G$ existiert mit $g.x = y$.

Bemerkung 2.10. 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.

2.3. **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 2.11 (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

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

(2) Sind X und G endlich, so gilt

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

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

Beweis. (1) Für jedes $y \in G.x$ definieren wir die Transportermenge

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

Dann ist $G_{x,x} = G_x$ und

$$G = \bigcup_{y \in G.x} G_{y,x}, \tag{2.1}$$

denn jedes $g \in G$ liegt in einem der $G_{y,x}$, nämlich für $y = g.x$ und offensichtlich ist dieses y in der Bahn $G.x$. Wir müssen nun zeigen,

(i) daß die Vereinigung in (2.1) aus disjunkten Mengen besteht, und

(ii) daß die $G_{y,x}$ unabhängig von y alle gleich groß sind,

nämlich $|G_{y,x}| = |G_{x,x}| = |G_x|$. Dann zählen wir

$$|G| = \sum_{y \in G.x} |G_{y,x}| = \sum_{y \in G.x} |G_x| = |G.x| \cdot |G_x|. \tag{2.2}$$

Die Inklusion $G_x \subseteq$G und die Surjektion $G \twoheadrightarrow G.x$ definiert durch $g \mapsto g.x$ zeigen, daß mit $|G|$ auch $|G_x|$ und $|G.x|$ endlich sind. Umgekehrt folgt aus (2.1), daß mit $|G_x|$ und $|G.x|$ endlich die Gruppe G in endlich viele endliche Mengen partitioniert ist, also endliche Ordnung hat.

Behautung (i) ist klar, denn für $g \in G_{y,x} \cap G_{z,x}$ gilt

$$y = g.x = z$$

per Definition. Um Behauptung (ii) zu zeigen wählen wir $y \in G.x$ und $h \in G_{y,x}$ (so ein h gibt es, denn y liegt ja im Orbit von x!). Dann ist die Abbildung

$$\begin{aligned} G_x &\to G_{y,x} \\ g &\mapsto hg \end{aligned}$$

bijektiv. Zunächst ist $hg.x = h.x = y$, also $hg \in G_{y,x}$ und die Abbildung wohldefiniert. Aus $hg_1 = hg_2$ folgt durch Linksmultiplikation mit h^{-1} schon $g_1 = g_2$, also ist die Abbildung injektiv.

Jetzt zeigen wir noch, daß jedes beliebige $k \in G_{y,x}$ im Bild liegt. Für $g = h^{-1}k$ gilt

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

also $g \in G_x$ und $k = hg$ liegt im Bild. Damit ist alles gezeigt.

Für Aussage (2) zerlegen wir X nach Satz 2.8 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. □

Anwendung 2.12. In Beispiel 2.5 (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 idenitfizieren ist. Die Operation ist transitiv, besteht also aus nur einer 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 2.13. 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.

Wir bestimmen die Ordnung von $\mathrm{GL}_n(\mathbb{F})$ mittels der definierenden Operation $\mathbb{F}^n$ und Sätzen aus der Linearen Algebra 1. Ein $A \in \mathrm{GL}_n(\mathbb{F})$ bildet eine linear unabhängige Menge von Vektoren $v_1, \ldots, v_r$ auf eine linear unabhängige Menge $w_1 = Av_1, \ldots, w_r = Av_r$ ab. Der Basisergänzungssatz und die Tatsache, daß man lineare Abbildungen auf einer Basis beliebig vorgeben kann, zeigt, daß jede linear unabhängige Menge $w_1, \ldots, w_r$ für ein geeignetes $A \in \mathrm{GL}_n(\mathbb{F})$ erhalten wird, sogar inklusive der Anordnung.

Wir starten mit dem Standardbasisvektor e_1. Sein Orbit besteht demnach aus jedem linear unabhängigen Vektor, also jedem beliebigen $v \in \mathbb{F}^n \setminus \{0\}$. Sei G_1 der Stabilisator von e_1. Dann zeigt der Bahnensatz

$$|\,\mathrm{GL}_n(\mathbb{F})| = |G_1| \cdot |\mathbb{F}^n \setminus \{0\}| = |G_1| \cdot (q^n - 1),$$

wobei wir verwenden, daß ein $\mathbb{F}$-Vektorraum der Dimension d genau q^d Elemente hat (beachte $\dim_{\mathbb{F}}\{0\} = 0$).

Nun arbeiten wir mit G_1 und dem Standardbasisvektor e_2 weiter. Der Orbit von e_2 unter der G_1-Operation besteht aus allen Vektoren w, so daß e_1, w linear unabhängig sind, also $w \in \mathbb{F}^n \setminus \langle e_1 \rangle$. Sei $G_2 \subseteq G_1$ der Stabilisator von e_2 für die G_1-Operation, also

$$G_2 = \{A \in \mathrm{GL}_n(\mathbb{F}) \; ; \; Ae_1 = e_1, Ae_2 = e_2\}.$$

Aus dem Bahnensatz folgt nun

$$|G_1| = |G_2| \cdot |\mathbb{F}^n \setminus \langle e_1 \rangle| = |G_2| \cdot (q^n - q^1).$$

Jetzt geht es immer so weiter: sei $W_r = \langle e_1, \ldots, e_r \rangle$ und

$$G_r = \{A \in \mathrm{GL}_n(\mathbb{F}) \; ; \; Ae_i = e_i \text{ für alle } i = 1, \ldots, r\}$$

die Stabilisatorgruppe aus dem vorherigen Schritt. Dann ist die Bahn von e_{r+1} unter G_r die Menge der Vektoren w, so daß $e_1, \ldots, e_r, w$ linear unabhängig sind, also $w \in \mathbb{F}^n \setminus W_r$. Der Bahnensatz zeigt

$$|G_r| = |G_{r+1}| \cdot |\mathbb{F}^n \setminus W_r| = |G_{r+1}| \cdot (q^n - q^r). \tag{2.3}$$

Multiplizieren wir (2.3) für alle r auf, und verwenden, daß $G_n = \{e\}$, so folgt

$$|\mathrm{GL}_n(\mathbb{F}) = (q^n - 1) \cdot (q^n - q) \cdot (q^n - q^{n-1}) = \prod_{r=0}^{n-1} (q^n - q^r).$$

Anwendung 2.14. Sei $n \geq 3$ 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 abbildet. Dies ist eine Gruppe mit Komposition von Abbildungen als Verknüpfung.

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 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 folgern, daß D_n von d und s erzeugt wird:

$$D_n = \langle d, s \rangle.$$

In der Tat operiert schon die Untergruppe $U = \langle d, s \rangle$ transitiv auf den Ecken von Δ_n. Und auch der Stabilisator ist gleich, denn s und die Identität (das neutrale Element von D_n) sind ja bereits in U enthalten. Aus der Bahnenformel folgt nun $|U| = 2n = |D_n|$, und somit muß $U = D_n$ sein.

Beispiel 2.15. 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}. Der Orbit von $0 \neq v \in K^{n+1}$ ist die **Geraden durch** v (ohne 0), also der eindimensionale Unterraum $\langle v \rangle$ (ohne 0), während der Orbit von 0 nur aus der 0 besteht. In der eingeschränkten Operation

$$\begin{aligned} K^\times \times (K^{n+1} \setminus \{0\}) &\to K^{n+1} \setminus \{0\} \\ \lambda, (x_0, \ldots, x_n) &\mapsto (\lambda x_0, \ldots, \lambda x_n) \end{aligned}$$

sind alle Stabilisatoren 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 Bahn des Vektors $(x_0, \ldots, x_n)$ bezeichnet man mit

$$[x_0 : \ldots : x_n]$$

und nennt die x_i **homogene Koordinaten** (die nur bis auf Skalieren mit λ bestimmt sind).

Anwendung 2.16. 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 $\mathbb{F}^{n+1}\backslash\{0\}$ 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

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

2.4. **Zur symmetrischen Gruppe.** Die symmetrische Gruppe ist aus der Linearen Algebra 1 bekannt, wo sie eine Rolle bei der Theorie der Determinante spielt.

Definition 2.17. Sei $n \in \mathbb{N}$ eine natürliche Zahl. Die **symmetrische Gruppe** S_n auf n Elementen ist die Gruppe

$$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \ ; \ \sigma \text{ ist eine Bijektion}\}$$

mit der Komposition als Gruppenverknüpfung.

Wir lassen ein Gruppenelement $\sigma \in S_n$ auf der Menge $\{1, \ldots, n\}$ iteriert operieren. Wir beginnen mit

$$a_1, a_2 = \sigma(a_1), a_3 = \sigma(a_2), \ldots, a_{i+1} = \sigma(a_i), \ldots$$

Da nur endlich viele Elemente zur Verfügung stehen, muß es ein erstes Mal eine Wiederholung geben: $1 \le s < r$ mit

$$a_s = a_r.$$

Wenn $s > 1$, dann ist

$$\sigma(a_{s-1}) = a_s = a_r = \sigma(a_{r-1})$$

und, weil σ bijektiv ist, auch

$$a_{s-1} = a_{r-1}.$$

Daraus schließen wir, daß die erste Wiederholung mit $s = 1$ beginnnt: es gibt kein vorperiodisches Verhalten. Das Element σ operiert also auf den Elementen

$$a_1, a_2, \ldots, a_r$$

durch zyklische Vertauschung in dieser Reihenfolge.

Definition 2.18. Ein **Zykel** in der Gruppe S_n ist eine Permutation $\sigma \in S_n$ der folgenden Form. Es gibt eine Teilmenge

$$A = \{a_1, \ldots, a_r\} \subseteq \{1, \ldots, n\}$$

mit $r \ge 2$ Elementen, so daß

$$\sigma(b) = \begin{cases} a_{i+1} & b = a_i, 1 \le i < r, \\ a_1 & b = a_r, \\ b & b \notin A. \end{cases}$$

Die Zahl $r = |A|$ heißt Länge des Zykels, und die Menge A nennen wir die **Trägermenge** des Zykels. Man sagt auch r**-Zykel**, wenn die Länge r ist. Als Notation verwenden wir

$$\sigma = (a_1, a_2, \ldots, a_r).$$

Haben mehrere Zykel disjunkte Trägermengen, so spricht man von **disjunkten Zykeln**.

Bemerkung 2.19. (1) Man beachte, daß die Elemente der Trägermenge im Zykel nicht der Größe nach geordnet sein müssen.
(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.
(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 2.20. 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 2.21. *(1) Ein Zykel der Länge r hat die Ordnung r.*
(2) Zwei disjunkte Zykel kommutieren miteinander.
(3) Jede Permutation $\sigma \in S_n$ ist bis auf die Reihenfolge auf eindeutige Art und Weise ein Produkt von disjunkten Zykeln.

Beweis. (1) Mit $\sigma = (a_1, a_2, \ldots, a_r)$ folgt für alle $i \in \mathbb{Z}$
$$\sigma^i(a_s) = a_{s+i},$$
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) Das ist klar: ein Zykel macht nur etwas Nichttriviales auf seiner Trägermenge. Sind diese disjunkt, so kommutieren (man sagt auch vertauschen) die Permutationen.

Seien $\sigma, \pi \in S_n$ disjunkte Zykel mit Trägermenge $A, B \subseteq \{1, \ldots, n\}$. Dann gilt
$$\sigma\pi(i) = \sigma(\begin{cases} \pi(i) & i \in B \\ i & i \notin B \end{cases}) = \begin{cases} \sigma(i) & i \in A \\ \pi(i) & i \in B \\ i & i \notin A \cup B \end{cases}$$
und genauso für $\pi\sigma$. Damit gilt $\sigma\pi = \pi\sigma$ wie behauptet.

(3) Sei $\sigma \in S_n$ eine Permutation. 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 $\sigma \neq \mathrm{id}$. Dann lassen wir die von σ erzeugte Untergruppe $\langle\sigma\rangle \subseteq S_n$ durch Einschränkung auf $\{1, \ldots, n\}$ operieren. Jeder Orbit der Länge $r \geq 2$ ist von der Form $A = \{a_1, \ldots, a_r\}$ mit $\sigma(a_i) = a_{i+1}$ für $i = 1, \ldots, r-1$ und $\sigma(a_r) = a_1$. Das Produkt über die Orbits der Länge ≥ 2 von den entsprecheden Zykeln ist offenbar identisch mit der Permutation σ. Dies zeigt die Existenz der Darstellung als Produkt von disjunkten Zykeln.

Die Eindeutigkeit der Darstellung sieht man wie folgt ein. Die Trägermengen der Zykel sind als Orbits von $\langle\sigma\rangle$ operierend auf $\{1, \ldots, n\}$ festgelegt. Die Reihenfolge der Elemente aus dem Orbit in den Zykeln wird durch die Wirkung von σ bis eben auf zyklische Permutation bestimmt. □

Proposition 2.22. *Sei $\sigma \in S_n$ ein Produkt von m disjunkten Zykeln der Längen $r_1, \ldots, r_m$. Dann gilt*
$$\mathrm{ord}(\sigma) = \operatorname*{kgV}_{1 \leq i \leq m} (r_i)$$

[9] Dies ist eine Konvention, die uns erspart, das neutrale Element von der Behauptung der Zerlegung in Zykel auszusparen.

Beweis. 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 $1 \leq i \leq m$ gilt $z_i^d = \mathrm{id}$, und damit $r_i = \mathrm{ord}(z_i) \mid d$. Daraus folgt sofort die Behauptung. □

Definition 2.23. Eine **Transposition** ist ein Zykel der Länge 2.

Satz 2.24. *Die symmetrische Gruppe S_n ist durch Transpositionen erzeugt.*

Beweis. Nach Proposition 2.21 reicht es, einen beliebigen Zykel $(a_1, a_2, \dots, a_r)$ als Produkt von Transpositionen zu erzeugen. Das ist leicht, denn

$$(a_1, a_2, \dots, a_r) = (a_1, a_r) \dots (a_1, a_3)(a_1, a_2)$$

was wir per vollständiger Induktion nach $r \geq 2$ nachweisen. Für $r = 2$ ist nichts zu tun. Nehmen wir also an, daß für $r - 1$ die Formel bereits gilt. Dann ist

$$(a_1, a_r) \dots (a_1, a_3)(a_1, a_2) = (a_1, a_r)(a_1, a_2, \dots, a_{r-1}) = (a_1, a_2, \dots, a_r)$$

wie man sofort nachrechnet. □

Alternativer Beweis. Wir zeigen die Behauptung mit vollständiger Induktion nach n. Für $n = 1$ ist nichts zu tun. Sei S_{n-1} durch Transpositionen erzeugt. Der Stabilisator des Elements n in der natürlichen Operation von S_n auf $\{1, \dots, n\}$ ist eine Kopie von S_{n-1} und die Transpositionen $(a, b) \in S_n$ mit $1 \leq a < b < n$ werden dabei genau mit den Transpositionen von S_{n-1} identifiziert.

Wir betrachten nun die von allen Transpositionen in S_n erzeugte Untergruppe $U \subseteq S_n$ und lassen diese per Einschränkung auf $\{1, \dots, n\}$ wirken. Der Stabilisator U_n ist gleich dem Stabilisator der gesamten S_n-Operation, denn alle Transpositionen sind per Definition in U und nach Induktionsannahme erzeugen diese den Stabilisator als Kopie von S_{n-1}.

Die Operation ist eingeschränkt auf U transitiv, denn Transpositionen reichen aus, um zwei beliebige Elemente zu vertauschen. Nach dem Bahnensatz gilt demnach

$$|U| = |\{1, \dots, n\}| \cdot |S_{n-1}| = n \cdot (n-1)! = |S_n|.$$

Die Untergruppe U hat gleich viele Elemente wie S_n, daher gilt $U = S_n$. □

2.5. **Elemente von Primzahlordnung.** Um die Kraft der Gruppenoperationen für die Strukturanalyse zu demonstrieren, beweisen wir nun noch den Satz von Cauchy[10].

Satz 2.25 (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 $\mathrm{ord}(g) = p$.*

Beweis. Sei $Z = \langle (1, 2, 3, \dots, p) \rangle \subseteq S_p$ die vom p-Zykel $\sigma = (1, 2, 3, \dots, p)$ erzeugte Untergruppe in der symmetrischen Gruppe S_p. Nach Proposition 2.21 hat σ die Ordnung p und Z besteht aus den verschiedenen Elementen

$$\mathrm{id}, \sigma, \sigma^2, \dots, \sigma^{p-1},$$

hat also auch die Ordnung $|Z| = p$.

Wir lassen die Gruppe Z auf der Menge

$$X = \{(g_1, \dots, g_p) \in G^p \ ; \ g_1 g_2 \dots g_p = 1\}$$

in natürlicher Weise durch zyklische Vertauschung operieren:

$$Z \times X \to X$$
$$\big(\sigma^n, (g_1, \dots, g_p)\big) \mapsto (g_{\sigma^n(1)}, \dots, g_{\sigma^n(p)}),$$

[10] Augustin-Louis Cauchy, 1789–1857, französischer Mathematiker.

dabei ist für $0 \leq n < p$ 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 $g_2 \ldots g_p g_1 = 1$ folgt. Mit $a = g_1$ und $b = g_2 \ldots g_p$ 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, die 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 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.

Sei $F \subseteq X$ die Menge der Fixpunkte der Operation, also die Vereinigung der Bahnen der Länge 1. Und sei weiter $P \subseteq X$ die Vereinigung der Bahnen der Länge p. Dann gilt nach dem Bahnensatz

$$|F| = |X| - |P|.$$

Da die rechte Seite durch p teilbar ist, gilt dies auch für $|F|$. Jetzt kommt die Pointe. Aus dem unbrauchbaren Element $(1, \ldots, 1) \in F$ folgt, daß $|F| \geq 1$ und da $|F|$ durch p teilbar ist, folgt sogar $|F| \geq p > 1$. Es muß also mindestens ein anderes Element

$$(g, \ldots, g) \in F$$

mit $g \neq 1$ geben! Dieses g ist das gesuchte Element der Ordnung p. □

Übungsaufgaben zu §2

Übungsaufgabe 2.1. Sei G eine Gruppe und X eine Menge. Definieren Sie, wann eine Abbildung

$$X \times G \to X$$

eine Rechtsoperation von G auf X genannt werden soll und zeigen Sie die Äquivalenz der Begriffe Linksoperation und Rechtsoperation: ist $G \times X \to X$ mit $g, x \mapsto g.x$ eine Linksoperation, dann definiert

$$x, g \mapsto g^{-1}.x$$

eine Rechtsoperation (und analog umgekehrt).

Übungsaufgabe 2.2. 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 2.3. 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 2.4. Bestimmen Sie die Orbits der Operation von $\mathrm{GL}_n(K)$ auf K^n durch Matrixmultiplikation.

Übungsaufgabe 2.5. Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen.

(1) Zeigen Sie, daß ein $\mathbb{F}$-Vektorraum V der Dimension d aus q^d Elementen besteht.
(2) Bestimmen Sie die Ordnung von $\mathrm{GL}_2(\mathbb{F})$.
(3) Bestimmen Sie die Ordnung von $\mathrm{GL}_n(\mathbb{F})$ für $n \geq 1$.

Tipp: Lassen Sie $\mathrm{GL}_2(\mathbb{F})$ auf $\mathbb{F}^2$ in natürlicher Weise operieren und benutzen Sie die Bahnenformel. Verallgemeinern Sie dies per vollständiger Induktion.

Übungsaufgabe 2.6. 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 2.7. In dieser Aufgabe analysieren wir die Operation von $G = \mathrm{GL}_2(K)$ auf $\mathbb{P}^1(K)$ aus Aufgabe 2.6.

(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 2.8. Sei G eine Gruppe. 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.

3. Operationen von Gruppen auf Gruppen

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

Definition 3.1. Sei $U \subseteq G$ eine Untergruppe.

(1) Die Untergruppe U operiert auf G von links durch **Translation (von links, oder Linkstranslation)** wie folgt:
$$\begin{aligned} U \times G &\to G \\ (u, g) &\mapsto ug. \end{aligned}$$
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.

Beispiel 3.2. (1) Die Bahn des neutralen Elements $e \in G$ unter der Translation mit der Untergruppe U (von links oder rechts!) ist gerade U selbst.

(2) 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

$$U = Ue = \{1, d, d^2, \ldots, d^{n-1}\},$$
$$Us = \{s, ds, d^2s, \ldots, d^{n-1}s\}.$$

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 $i \in \mathbb{Z}$)

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

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

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

gilt.

Definition 3.3. Der Orbitraum der Linkstranslation (bzw. Rechtstranslation) der Untergruppe U von G wird mit

$$U\backslash G \quad (\text{bzw. } G/U)$$

bezeichnet.

Satz–Definition 3.4. *Der **Index** $(G : U)$ einer Untergruppe U von G ist definiert als*

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

insbesondere haben beide Bahnenräume die gleiche Mächtigkeit.

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 3.5. (1) Falls G endlich ist, so folgt Satz-Definition 3.4 unmittelbar aus der Bahnenformel

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

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

(2) Die Notation $(G : U)$ für den Index der Untergruppe $U \subseteq G$ ist suggestiv und erinnert an die Konsequenz der Bahnenformel

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

sofern alle Größen endlich sind.

Beispiel 3.6. (1) In der Notation von Beispiel 3.2 hat die Untergruppe $\langle d \rangle \subseteq D_n$ den Index 2 und $\langle s \rangle \subseteq D_n$ den Index n.

(2) Sei K ein Körper. Die Gruppe $\mathrm{GL}_2(K)$ hat die Untergruppe der oberen Dreiecksmatrizen

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

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

$$gB = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K) \; ; \; K \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = K \begin{pmatrix} a \\ c \end{pmatrix} \right\} \tag{3.1}$$

und bestehen aus allen Elementen von $\mathrm{GL}_2(K)$, deren erste Spalte die gleiche Gerade in K^2 aufspannen. In der Tat, rechnen wir

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda & x \\ 0 & \mu \end{pmatrix} = \begin{pmatrix} \lambda a & xa + \mu b \\ \lambda c & xc + \mu d \end{pmatrix},$$

so daß die erste Spalte nur Werte in $K \begin{pmatrix} a \\ c \end{pmatrix}$ annehmen kann. Dies zeigt $\subseteq$ in (3.1).

Wir zeigen nun $\supseteq$ in (3.1). Sei $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ ein beliebiges Element der rechten Seite. Dann gibt es $\lambda \in K^\times$ mit

$$\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \lambda \begin{pmatrix} a \\ c \end{pmatrix}.$$

Da $g \in \mathrm{GL}_2(K)$ ist, sind die Spalten $\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}$ eine Basis von K^2 und die Linearkombinationen

$$x \begin{pmatrix} a \\ c \end{pmatrix} + \mu \begin{pmatrix} b \\ d \end{pmatrix} \tag{3.2}$$

mit $x \in K$ und $\mu \in K^\times$, nehmen als Werte alle Vektoren an, so daß

$$\lambda \begin{pmatrix} a \\ c \end{pmatrix}, x \begin{pmatrix} a \\ c \end{pmatrix} + \mu \begin{pmatrix} b \\ d \end{pmatrix}$$

eine Basis von K^2 ist, also zum Beispiel die Spalten von $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Der Raum der Linksnebenklasse 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

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

(3) 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.

Wir zeigen nun, daß jede Untergruppe der Stabilisator eines Elements bei einer geeigneten Gruppenoperation ist.

Proposition 3.7. *Sei U eine Untergruppe der Gruppe G. Dann operiert G auf G/U vermöge der durch Linkstranslation induzierten Abbildung*

$$\begin{aligned} G \times G/U &\to G/U, \\ (g, hU) &\mapsto ghU. \end{aligned}$$

Die Operation ist transitiv und der Stabilisator von der Nebenklasse U ist U.

Beweis. Wir müssen zunächst zeigen, daß die Operation wohldefiniert ist, daß also für eine Linksnebenklasse $B = hU$ das Bild $gB = ghU$

(i) erstens eine Linksnebenklasse ist, und
(ii) zweitens nur von B (und g) und nicht von der Wahl von h abhängt.

Das ist beides trivial, denn ghU ist eine Linksnebenklasse und in der Form gB hängt diese nur von B und nicht von h ab.

Sodann müssen wir Assoziativität nachweisen: für $g, h, k \in G$ gilt

$$g(h(kU)) = g(hkU) = ghkU = (gh)(kU).$$

Und mit dem neutralen Element $e \in G$ gilt $eB = B$ für jedes $B \in G/U$.

Offensichtlich ist G/U der Orbit der Nebenklasse $U \in G/U$. Sei $g \in G$ im Stabilisator von U. Dann gilt

$$gU = U$$

also wegen $e \in U$ auch $g = ge \in U$. Umgekehrt, wenn $g \in U$ gilt, dann ist gU eine Linksnebenklasse, die sich mit U in g schneidet, also mit dieser identisch sein muß: $gU = U$. Dies zeigt, daß der Stabilisator von U gleich U ist. □

Definition 3.8. Sei G eine Gruppe. Eine **Abbildung von Mengen mit G-Operation** (oder **G-äquivariante Abbildung**) ist eine Abbildung

$$f : X \to Y$$

von Mengen X und Y mit G-Operation, so daß für alle $x \in X$ und $g \in G$ gilt:

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

Satz 3.9. *Sei X eine transitive G-Menge und $x \in X$ ein Element mit Stabilisator G_x. Dann ist die Abbildung*

$$\begin{aligned} f : G/G_x &\to X \\ gG_x &\mapsto g.x \end{aligned}$$

eine bijektive G-äquivariante Abbildung. Es gilt insbesondere

$$(G : G_x) = |X|.$$

Beweis. Da aus $gG_x = hG_x$ schon

$$g.x = g.(G_x.x) = (gG_x).x = (hG_x).x = h.(G_x.x) = h.x$$

folgt, ist die Abbildung f wohldefiniert. Die Abbildung f ist surjektiv, da nach Voraussetzung X nur aus einem Orbit besteht, also $X = G.x$ ist.

Wenn $g.x = h.x$, so folgt

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

also $h^{-1}g \in G_x$ und $hG_x = h(h^1g)G_x = gG_x$. Also ist f auch injektiv.

Für alle $g, h \in G$ gilt

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

und zeigt die G-Äquivarianz von f.

Die Gleichheit von Index $(G : G_x)$ und $|X|$ folgt nun aus der Definition des Index. □

Satz 3.10 (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 2.11 (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 3.11. Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Dann hat die Gruppe der oberen Dreiecksmatrizen B, 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 3.6) ist zu $\mathbb{P}^1(\mathbb{F})$ mit $|\mathbb{P}^1(\mathbb{F})| = q + 1$ Elementen (siehe Anwendung 2.16), folgt aus dem Satz von Lagrange

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

Satz 3.12. *Sei $g \in G$ ein Gruppenelement von endlicher Ordnung $\operatorname{ord}(g) = N$. Dann besteht die von g erzeugte Untergruppe $\langle g \rangle \subseteq G$ aus den N Elementen*

$$1, g, g^2, \ldots, g^{N-1},$$

insbesondere hat $\langle g \rangle$ die Ordnung $|\langle g \rangle| = \operatorname{ord}(g) = N$.

Beweis. Die Potenzen g^a mit $a \in \mathbb{Z}$ sind in jeder Untergruppe $U \subseteq G$ enthalten, sobald $g \in U$ gilt. Außerdem ist

$$\{g^a \ ; \ a \in \mathbb{Z}\} \subseteq G$$

eine Untergruppe, denn $g^a g^b = g^{a+b}$ und $(g^a)^{-1} = g^{-a}$ zeigen die Abgeschlossenheit unter Multiplikation und Inversennehmen. Daher gilt

$$\langle g \rangle = \{g^a \ ; \ a \in \mathbb{Z}\}.$$

Da weiter per Annahme $g^N = 1$, ist als Teilmengen von G

$$\langle g \rangle = \{g^a \ ; \ a \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{N-1}\},$$

denn mittels

$$g^{a \pm N} = g^a g^{\pm N} = g^a$$

kann man die Exponenten von g^a stets in $0 \leq a \leq N-1$ wählen. Wenn $g^a = g^b$, dann ist $g^{a-b} = 1$ und so $N \mid a - b$. Also sind die Elemente

$$1, g, g^2, \ldots, g^{N-1}$$

paarweise verschieden und alles bewiesen. □

Korollar 3.13. *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 dem Satz von Lagrange: $\operatorname{ord}(g) = |U|$ teilt $|U| \cdot (G : U) = |G|$. □

Bemerkung 3.14. Der Satz von Lagrange spricht eine Bedingung aus, die Untergruppen erfüllen müssen, wodurch die möglichen Untergruppen stark eingeschränkt werden. In Form des Korollars 3.13 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 spricht umgekehrt aus, daß zumindest für die Existenz von Gruppenelementen von Primzahlordnung die Bedingung aus dem Satz von Lagrange die einzige ist.

Korollar 3.15 (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 3.13. □

Beispiel 3.16. Sei p eine Primzahl. Der endliche Körper $\mathbb{F}_P$ hat p Elemente, die Restklassen von ganzen Zahlen modulo $p\mathbb{Z}$. Seine multiplikative Gruppe $\mathbb{F}_p^\times$ hat $p-1$ Elemente, die nicht durch p teilbaren Restklassen. Korollar 3.15 besagt in diesem Spezialfall, daß für alle $x \in \mathbb{Z}$ mit $p \nmid x$ gilt

$$p \mid x^{p-1} - 1.$$

Definition 3.17. Der **Exponent** $\exp(G)$ einer endlichen Gruppe G ist die kleinste positive natürliche Zahl $N \geq 1$, so daß

$$g^N = 1$$

für alle $g \in G$ gilt.

Bemerkung 3.18. Es gilt offensichtlich per Definition

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

Nach dem kleinen Fermat gilt $\exp(G) \mid |G|$, aber Gleichheit muß hier nicht gelten. Als Beispiel dient die S_4. Hier sind die Ordnungen das kgV der Zykellängen, in die man ein gegebenes Element zerlegen kann. Es geht also um das kgV über Partitionen von 4. Das sind 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$; entsprechend die Ordnungen 4, 3, 2, 2 und 1. Somit gilt

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

3.2. **Gruppenhomomorphismen.** Um Gruppen besser zu verstehen, braucht man einen Begriffsapparat um Gruppen zu vergleichen: strukturerhaltende Abbildungen.

Definition 3.19. 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 3.20. (1) Die Determinante ist ein Gruppenhomomorphismus

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

(2) Das aus der Linearen Algebra 1 bekannte Signum $\operatorname{sign} : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus.

Zur Erinnerung: Das Signum $\operatorname{sign} : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus, und zwar eindeutig dadurch charakterisiert, daß für Transpositionen $\tau \in S_n$ gilt:

$$\operatorname{sign}(\tau) = -1.$$

Die Eindeutigkeit folgt dadurch, daß offensichtlich ein Gruppenhomomorphismus eindeutig durch seine Werte auf einem Erzeugendensystem festgelegt ist und nach Satz 2.24 die Transpositionen S_n erzeugen. Die Existenz des Signum ist eine nichttriviale Sache.

Am einfachsten[11] 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

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

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

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

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

und die Zuordnung

$$\rho : S_n \to \mathrm{GL}_n(\mathbb{Q})$$
$$\sigma \mapsto \rho(\sigma) = P_\sigma$$

ist ein Gruppenhomomrphismus. Dann definiert

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

den Signum-Homomorphismus. In der Tat ist dies wohldefiniert und nimmt auf Transpositionen nach Eigenschaft der Determinante den Wert -1 an.

Lemma 3.21. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt $f(e) = e$ und*

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

für alle $g \in G$, wobei e das neutrale Element in G und (mißbräuchlich) auch in H bezeichne.

Beweis. Aus $f(e) = f(ee) = f(e)f(e)$ folgt durch Multiplikation mit $f(e)^{-1}$ die Behauptung $f(e) = e$. Weiter gilt für $g \in G$

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

und somit die zweite Behauptung. □

Proposition 3.22. *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. Aus $a, b \in f^{-1}(V)$ folgt $f(ab) = f(a)f(b) \in V$, also $ab \in f^{-1}(V)$. Und weiter $f(a^{-1}) = f(a)^{-1} \in V$, also $a^{-1} \in f^{-1}(V)$. Damit ist $f^{-1}(V)$ eine Untergruppe von G.

Aus $a, b \in f(U)$ folgt die Existenz von Elementen $x, y \in U$ mit $a = f(x)$ und $b = f(y)$. Dannn gilt $ab = f(x)f(y) = f(xy) \in f(U)$ und $a^{-1} = f(x)^{-1} = f(x^{-1}) \in f(U)$, so daß $f(U)$ eine Untergruppe in H ist. □

Definition 3.23. 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 3.24. Sei K ein Körper und $n \in \mathbb{N}$. Die spezielle lineare Gruppe

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

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

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

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

Proposition 3.25. *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 3.26. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Das Bild $\operatorname{im}(f)$ ist endlich genau dann, wenn $\ker(f)$ endlichen Index hat. In diesem Fall gilt*

$$|\operatorname{im}(f)| = (G : \ker(f)).$$

Proposition 3.27. *Wir setzen $N = \ker(f)$. Die Abbildung von Mengen $G/N \to \operatorname{im}(f)$, welche gN auf $f(g)$ abbildet, ist wohldefiniert. Aus $gN = hN$ folgt*

$$\{f(g)\} = f(g)f(N) = f(gN) = f(hN) = f(h)f(N) = \{f(h)\}.$$

Außerdem ist die Abbildung offensichtlich surjektiv.

Wenn $f(g) = f(h)$ für $g, h \in G$, dann ist $f(h^{-1}g) = f(h)^{-1}f(g) = 1$, somit $h^{-1}g \in N$ oder äquivalent $g \in hN$. Damit ist $gN = hN$ (beide Nebenklassen sind nicht disjunkt) und damit f auch injektiv.

Definition 3.28. 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 $G \simeq H$.

Bemerkung 3.29. Im Kontext des Beweises von Proposition 3.26 sehen wir später in Satz 4.9, daß G/N eine Gruppenstruktur trägt, und in Satz 4.20 sehen wir, daß die Abbildung $G/N \to \operatorname{im}(f)$ ein Gruppenisomorphismus ist.

Beispiel 3.30. (1) Die Exponentialfunktion

$$\exp : \mathbb{R} \to \mathbb{R}^\times$$

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

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

Da $\ker(\exp) = \{0\}$, ist exp injektiv. Das Bild von $\exp(-)$ ist die Untergruppe $\mathbb{R}_{>0} \subseteq \mathbb{R}^\times$ der positiven reellen Zahlen. Wir erhalten einen Isomorphismus $(\mathbb{R}, +) \simeq (\mathbb{R}_{>0}, \cdot)$. Die Umkehrabbildung ist der natürliche Logarithmus.

(2) Der Stabilisator von $n \in \{1, \ldots, n\}$ unter der natürlichen S_n-Operation ist isomorph zu S_{n-1} vermöge des injektiven Gruppenhomomorphismus

$$f : S_{n-1} \to S_n,$$

der eine Permutation von $\{1, \ldots, n-1\}$ durch $n \mapsto n$ fortsetzt:

$$f(\sigma) = \left(i \mapsto \begin{cases} \sigma(i) & 1 \leq i < n, \\ n & i = n. \end{cases} \right)$$

$\sigma \in S_{n-1}$ durch $\sigma(n) = n$ fortsetzt. Offensichtlich ist $\ker(f) = \{\mathrm{id}\}$, somit f injektiv, das Bild ist genau der Stabilisator von n und die Einschränkung auf das Bild ist ein Isomorphismus von Gruppen.

Proposition 3.31. *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 $f : H \to K$ Gruppenhomomorphimen. 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 3.32. *Die Menge* $\mathrm{Aut}(G)$ *aller Automorphismen einer Gruppe* G *ist bezüglich der Komposition eine Gruppe.* □

Beispiel 3.33. 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 Vekotor, 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 bedeutet, 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

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

Definition 3.34. Die **symmetrische Gruppe** auf einer Menge X ist die Gruppe

$$S_X = \{\sigma : X \to X \ ; \ \sigma \text{ ist eine Bijektion}\}$$

mit der Komposition als Gruppenverknüpfung.

Bemerkung 3.35. Sei $n \geq 1$ eine natürliche Zahl. Der Spezialfall

$$S_n := S_{\{1,\ldots,n\}}$$

liefert die bekannte symmetrische Gruppe auf n Elementen zurück. Für eine n-elementige Menge X liefert eine Bijektion

$$\varphi : X \xrightarrow{\sim} \{1, \ldots, n\}$$

einen Isomorphismus

$$\begin{aligned} S_X &\xrightarrow{\sim} S_n \\ \sigma &\mapsto \varphi\sigma\varphi^{-1}. \end{aligned}$$

In der Tat ist die Abbildung ein Homomorphismus, denn für alle $\sigma, \tau \in S_X$ gilt

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

und die Abbildung $\sigma \mapsto \varphi^{-1}\sigma\varphi$ ist der inverse Gruppenhomomorphismus.

Proposition 3.36. *Sei* G *eine Gruppe und* X *eine Menge. Die folgenden Daten sind äquivalent.*

(a) Eine Gruppenoperation $G \times X \to X$.

(b) Ein Gruppenhomomorphismus $\rho : G \to S_X$.

Genauer: für $g \in G$ *und* $x \in X$ *definiert* $\rho(g)(x) = g.x$ *eine bijektive Abbildung* $\rho(g) : X \to X$ *und so einen Gruppenhomomorphismus*

$$\rho : G \to S_X.$$

Sei umgekehrt $\rho : G \to S_X$ *ein Gruppenhomomorphismus. Dann definiert*

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g.x := \rho(g)(x) \end{aligned}$$

eine Gruppenoperation von G *auf* X.

Beweis. Sei $G \times X \to X$ eine Gruppenoperation von G auf X. Wir definieren $\rho(g) : X \to X$ durch $\rho(g)(x) = g.x$. Dann gilt für $g, h \in G$ und $x \in X$

$$\rho(g)(\rho(h)(x)) = g.(h.x) = (gh).x = \rho(gh)(x). \tag{3.3}$$

Mit dem neutralen Element $e \in G$ gilt

$$\rho(e)(x) = e.x = x$$

also $\rho(e) = \mathrm{id}_X$. Hieraus folgt, daß

$$\rho(g^{-1}) \circ \rho(g) = \rho(e) = \mathrm{id}_X = \rho(g) \circ \rho(g^{-1}),$$

also ist $\rho(g)$ bijektiv mit Inversem $\rho(g^{-1})$. Wir erhalten eine wohldefinierte Abbildung

$$\rho : G \to S_X,$$

und sogar ein Gruppenhomomorphismus nach (3.3).

Starten wir umgekehrt mit einem Gruppenhomomorphismus $\rho : G \to S_X$, so definiert man für $g \in G$ und $x \in X$ durch $g.x := \rho(g)(x)$ eine Abbildung $G \times X \to X$. Dies ist eine Gruppenoperation, wie man als Übung leicht nachrechnet.

Die beiden Konstruktionen sind offensichtlich invers zueinander. □

Beispiel 3.37. Sei T die Gruppe der Symmetrien eines Tetraeders, die **volle Tetraedergruppe**. 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 Proposition 3.36, also ein Gruppenhomomorphismus. Wir zeigen, daß die Tetraedergruppe T isomorph ist zu S_4, und zwar genauer, daß ρ ein Isomorphismus ist.

Die Symmetrien des Tetraeders sind durch ihre Wirkung auf den Ecken eindeutig bestimmt: ρ ist injektiv. 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.

Definition 3.38. Eine **freie Operation** ist eine Operation, bei der alle Stabilisatoren die triviale Gruppe $\{e\}$ sind, d.h. eine Operation $G \times X \to X$, so daß für $g \in G$ und $x \in X$ aus $g.x = x$ bereits $g = e$ folgt.

Lemma 3.39. *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: $u = e$ ist das neutrale Element von G, also von U. □

Satz 3.40 (Satz von Cayley)**.** *Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe. Eine Gruppe der Ordnung n ist isomorph zu einer Untergruppe der S_n.*

Beweis. Wir wählen zunächst eine Bijektion von Mengen $\varphi : G \to \{1, \ldots, n\}$ und erhalten daraus einen Gruppenisomorphismus

$$S_n \to S_G$$
$$\sigma \mapsto \varphi^{-1} \circ \sigma \circ \varphi.$$

Wir lassen nun die Gruppe G durch Translation von links auf sich selbst operieren. Dies übersetzt wie in Proposition 3.36 zu einem Gruppenhomomorphismus

$$\rho : G \to S_G \simeq S_n$$

in die symmetrische Gruppe der zugrundeliegenden Menge von G. Wir müssen zeigen, daß ρ injektiv ist, und dann ist ρ ein Isomorphismus auf das Bild.

Nach Proposition 3.25 müssen wir zeigen, daß $\ker(\rho) = \{1\}$. Aber per Definition

$$\ker(\rho) = \bigcap_{h\in G} \text{Stabilisator von } h,$$

und dies ist $\{1\}$, denn die Operation durch Translation ist frei nach Lemma 3.39. □

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

Definition 3.41. Sei G eine Gruppe und $g, h \in G$ Gruppenelemente. Man nennt

$$ghg^{-1}$$

das zu h (mittels g) **konjugierte Element**. Die Abbildung $\varphi_g : G \to G$ definiert durch

$$\varphi_g(h) = ghg^{-1}$$

nennt man **Konjugation mit** g.

Notation 3.42. 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.

Beispiel 3.43. Als Beispiel beschreiben wir die Konjugation in der symmetrischen Gruppe S_n.

Sei $\sigma \in S_n$ beliebig und

$$\pi = (a_1, \dots, a_r)$$

ein Zykel der Länge r. Dann ist

$$\sigma\pi\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_r)) \tag{3.4}$$

auch ein Zykel der Länge r.

Wir zeigen (3.4), indem wir beide Seiten auf $\{1, \dots, n\}$ auswerten und vergleichen. Dazu benutzen wir, daß σ eine Permutation ist und werten aus auf $i = \sigma(b)$ für alle $b = 1, \dots, n$. Dann gilt

$$\begin{aligned}\sigma\pi\sigma^{-1}(i) = \sigma\pi(b) = \sigma\Big(&\begin{cases} a_{s+1} & \text{falls } b = a_s \text{ für ein } 1 \le s < r \\ a_1 & \text{falls } b = a_r \\ b & \text{falls } b \notin \{a_1, \dots, a_r\} \end{cases}\Big) \\ &= \begin{cases} \sigma(a_{s+1}) & \text{falls } i = \sigma(a_s) \text{ für ein } 1 \le s < r \\ \sigma(a_1) & \text{falls } i = \sigma(a_r) \\ i & \text{falls } i \notin \{\sigma(a_1), \dots, \sigma(a_r)\} \end{cases}\end{aligned}$$

Es werden also genau die Elemente der Form $\sigma(a_s)$ bewegt, und zwar wie mit der rechten Seite von (3.4) beschrieben.

Proposition 3.44. *Die Konjugation mit $g \in G$ ist ein Gruppenautomorphimus $\varphi_g : G \to G$.*

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

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

Da $\varphi_e(a) = a$ 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 3.45. Die Rechnung in Proposition 3.44 zeigt, daß die Zuordung

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

ein Gruppenhomomorphismus ist.

Definition 3.46. Automorphismen der Form $\varphi_g : G \to G$ wie in Proposition 3.44 werden **innere Automorphismen** genannt.

Bemerkung 3.47. Die Formel (3.4) überträgt sich auf Produkte von Zykeln, weil Konjugation mit einem festen σ ein Gruppenhomomorphismus ist. Die Konjugationsklassen von S_n sind demnach durch Partitionen von n parametrisiert.

Korollar 3.48. *Konjugierte Elemente haben die gleiche Ordnung.*

Beweis. Seien $g, h \in G$. Dann gilt für alle $n \in \mathbb{Z}$

$$h^n = 1 \iff \varphi_g(h^n) = \varphi_g(1) \iff \varphi_g(h)^n = 1 \iff (ghg^{-1})^n = 1.$$

□

Lemma–Definition 3.49. *Sei G eine Gruppe. Die Abbildung*

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

beschreibt eine Operation von G auf sich selbst, die ***Operation durch Konjugation*** *(oder* ***Konjugationsoperation****).*

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

$$(ab).h = (ab)h(ab)^{-1} = abhb^{-1}a^{-1} = a(b(h)b^{-1})a^{-1} = a.(b.h), \tag{3.5}$$

was die Assoziativität zeigt. □

Bemerkung 3.50. Alternativ zum Beweis von Lemma-Definition 3.49 hätte man darauf verweisen können, daß

$$\mathrm{Aut}(G) \subseteq S_G$$

eine Untergruppe ist, und die Zuordnung $g \mapsto \varphi_g$ daher einen Gruppenhomomorphismus

$$G \to \mathrm{Aut}(G) \subseteq S_G$$

liefert, der nach Proposition 3.36 zu einer Gruppenoperation $G \times G \to G$ übersetzt werden kann. Man rechnet dann leicht nach, daß man die Konjugationsoperation erhält.

Definition 3.51. Sei G eine Gruppe.

(1) Die Bahnen der Konjugationsoperation heißen **Konjugationsklassen** von G. Die Konjugationsklasse von $h \in G$ bezeichnen wir mit

$$C_h := \{ghg^{-1} \ ; \ g \in G\}.$$

(2) Der **Zentralisator** eines Gruppenelements $h \in G$ ist der Stabilisator der Konjugationsoperation

$$Z_G(h) := \{g \in G \ ; \ ghg^{-1} = h\}.$$

Beispiel 3.52. (1) Der Zentralisator von $h \in G$ ist die Untergruppe von G bestehend aus allen Elementen $g \in G$, die mit h kommutieren, denn $ghg^{-1} = h$ ist äquivalent zu $gh = hg$. Insbesondere gilt stets

$$\langle h \rangle \subseteq Z_G(h).$$

(2) Die Mächtigkeit der Konjugationsklassse von h ist nach dem Bahnensatz

$$|C_h| = (G : Z_G(h))$$

der Index des Zentralisators.

(3) Sei $n \geq 3$ eine natürliche Zahl. Wir diskutieren die Begriffe am Beispiel der Diedergruppe D_n. Sei wie üblich d eine Drehung um den Winkel $2\pi/n$ und s eine Spiegelung. Da Drehungen miteinander kommutieren, gilt für alle $0 \leq i \leq n-1$

$$\langle d \rangle = \{1, d, d^2, \ldots, d^{n-1}\} \subseteq Z_{D_n}(d^i).$$

Die Zentralisatoren haben also Index 1 oder 2 in D_n. Dementsprechend bestehen die Konjugationsklassen aus einem oder zwei Elementen. Wegen

$$sd^i s^{-1} = \varphi_s(d^i) = \varphi_s(d)^i = (sds)^i = d^{-i}$$

sind die Konjugationsklassen für $0 \leq i < n$ genau

$$\{d^i, d^{-1}\}.$$

Dies ist 2-elementig, es sei denn $i = 0$ oder $i = n/2$ (sofern n gerade ist). In den Ausnahmefällen ist die Konjugationsklasse 1-elementig.

Für die Konjugationsklasse von sd^i berechnen wir

$$dsd^{-1} = ds(sds) = ds^2 ds = d^2 s,$$

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 $\{s, ds, d^2 s, \ldots, d^{n-1}s\}$ zyklisch um 2 Positionen. Damit sind für ungerades n alle $d^j s$ konjugiert (durch iteriertes Anwenden von d). Andererseits enthält der Stabilisator mindestens 2 Elemente, so daß die Konjugationsklasse C_s höchstens n Elemente haben kann. Im Fall n gerade spaltet die Menge der Spiegelungen in zwei Konjugationsklassen auf: je nach Parität von j in $d^j s$.

Übungsaufgaben zu §3

Übungsaufgabe 3.1. Betrachten Sie den Beweis der Bahnenformel in Satz 2.11. Zeigen Sie, daß die Zerlegung

$$G = \bigcup_{y \in G.x} G_{y,x}$$

in Transportermengen die Links-Nebenklassenzerlegung nach der Rechtstranslation des Stabilisators G_x auf G ist. Zeigen Sie damit erneut die Zwischenbehauptungen, daß die Zerlegung diskjunkt ist und alle Mengen $G_{y,x}$ gleich groß sind.

Übungsaufgabe 3.2. Seien $U_i < G$ für $i = 1, \ldots, r$ Untergruppen von endlichem Index in der Gruppe G. Zeigen Sie, daß die Untergruppe $U = \bigcap_{i=1}^r$ auch von endlichem Index ist und genauer

$$(G : U) \leq \prod_{i=1}^{r} (G : U_i)$$

gilt.

Übungsaufgabe 3.3. Sei G eine Gruppe und seien $U \subseteq G$ und $V \subseteq U$ Untergruppen. Zeigen Sie die folgenden Aussage.

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

Übungsaufgabe 3.5. 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 3.6. 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 3.7. Sei G eine Gruppe. Zeigen Sie, daß die Relation auf der Menge G definiert durch Konjugation, also

$$a \sim b \quad \iff \quad \text{es gibt ein } g \in G \text{ mit } b = gag^{-1}$$

eine Äquivalenzrelation ist.

Übungsaufgabe 3.8. 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 3.9. Bestimmen Sie die Anzahl der Konjugationsklassen in S_6.

Übungsaufgabe 3.10. Beschreiben Sie analog zum Beispiel 3.6 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 3.11. 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 $\mathrm{ord}(g) = n$.

4. Quotienten und Isomorphiesätze

4.1. **Konjugation von Untergruppen.**

Definition 4.1. Konjugierte Untergruppen sind Untergruppen $U, V \subseteq G$ einer Gruppe G, so daß es ein Element $g \in G$ gibt mit $gUg^{-1} = V$.

Bemerkung 4.2. Eine Gruppe G operiert vermöge Konjugation auf der Menge seiner Untergruppen. 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 3.22 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.

Satz 4.3. *Sei X eine Menge mit G-Operation und sei $B \subseteq X$ ein Orbit. Dann sind die Stabilisatoren G_a, G_b für $a, b \in B$ konjugiert zueinander.*

Beweis. Nach Voraussetzung gibt es ein $g \in G$ mit $g.a = b$. Dann gilt $gG_ag^{-1} = G_b$, denn

$$(gG_ag^{-1}).b = (gG_ag^{-1}).g.a = (gG_a).a = g.a = b$$

zeigt $gG_ag^{-1} \subseteq G_b$. Weiter folgt aus $g^{-1}.b = a$ wie eben $g^{-1}G_bg \subseteq G_a$. Darauf wenden wir φ_g an und erhalten die umgekehrte Inklusion $G_b \subseteq gG_ag^{-1}$. □

Kerne haben die bemerkenswerte Eigenschaft, als Untergruppe nur zu sich selbst konjugiert zu sein. Diese Eigenschaft bekommt einen Namen.

Definition 4.4. Ein **Normalteiler** ist eine Untergruppe N in einer Gruppe G, die nur zu sich selbst konjugiert ist.

Lemma 4.5. *Eine Untergruppe $N \subseteq G$ ist ein Normalteiler genau dann, wenn für alle $g \in G$ gilt*

$$N \subseteq gNg^{-1}.$$

Beweis. Normalteiler erfüllen $N = gNg^{-1}$ per Definition. Sei umgekehrt $N \subseteq G$ eine Untergruppe, so daß für alle $g \in G$ gilt $N \subseteq gNg^{-1}$. Dann gilt für g^{-1} als Gruppenelement auch $N \subseteq g^{-1}Ng$. Dies konjugieren wir mit g und erhalten

$$gNg^{-1} \subseteq g(g^{-1}Ng)g^{-1} = N.$$

Es gilt also $N = gNg^{-1}$ für alle $g \in G$. □

Proposition 4.6. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann ist $N = \ker(f)$ ein Normalteiler.*

Beweis. Sei $h \in N$. Dann gilt

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

und somit $ghg^{-1} \in N$. Dies zeigt $gNg^{-1} \subseteq N$. Wir schließen nun analog wie in Lemma 4.5. □

Beispiel 4.7. (1) Sein $n \geq 4$ und $\sigma \in S_n$ ein Zykel der Länge $r \geq 2$. Dann ist $U = \langle\sigma\rangle$ kein Normalteiler von S_n. Dies folgt sofort aus Beispiel 3.43.

Man beachte, daß die vom 3-Zykel in S_3 erzeugte Untergruppe gerade A_3 ist. Dies ist der Kern von $\operatorname{sign} : S_3 \to \{\pm 1\}$ und somit ein Normalteiler.

(2) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

4.2. **Quotienten.** Wir zeigen nun, daß Kerne von Gruppenhomomorphismen dasselbe sind wie Normalteiler. Die eine Richtung haben wir bereits in Proposition 4.6 eingesehen: Kerne sind Normalteiler.

Lemma 4.8. *Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ ist Normalteiler in G genau dann, wenn für alle $g \in G$ die von g repräsentierten Links- und Rechtsnebenklassen übereinstimmen:*

$$gN = Ng.$$

Beweis. Die definierende Eigenschaft $gNg^{-1} = N$ wird durch Rechtsmultiplikation mit g zur äquivalenten Eigenschaft $gN = Ng$. □

Satz 4.9 (Faktorgruppe)**.** *Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler.*

(1) Sei N Normalteiler. 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

$$p : G \to G/N$$
$$g \mapsto gN$$

ist ein surjektiver Gruppenhomomorphismus mit Kern $\ker(p) = N$.

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

$$g \in \ker(p) \iff p(g) = 1 \iff gN = N \iff g \in N.$$

Also gilt $N = \ker(p)$. □

Beispiel 4.10. Sei 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 3.6), während Rechtsnebenklassen aus Matrizen bestehen, deren untere Zeile Vielfache voneinander sind.

Definition 4.11. Zu einem Normalteiler N in einer Gruppe G heißt die in Satz 4.9 definierte Gruppe auf G/N die **Faktorgruppe** von G nach N.

Proposition 4.12. *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 dann das Komplement $G \setminus U$. □

Beispiel 4.13. Sei D_n die Diedergruppe, $d \in D_n$ eine Drehung um $2\pi/n$ und s eine Spiegelung. Dann ist $\langle d \rangle$ ein Normalteiler, aber für $n \geq 3$ die Untergruppe $\langle s \rangle$ nicht.

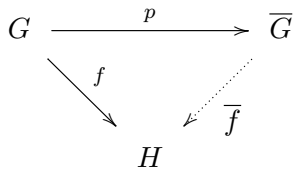
Satz 4.14 (Existenz des Quotienten nach einem Normalteiler)**.** *Sei N ein Normalteiler in der Gruppe G. Dann gibt es einen Gruppenhomomorphismus*

$$p : G \to \overline{G}$$

mit den folgenden Eigenschaften:

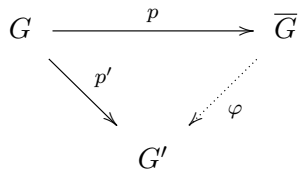
(i) $N \subseteq \ker(p)$.

(ii) *Für jeden Gruppenhomomorphismus $f : G \to H$ mit $N \subseteq \ker(f)$ gibt es einen Gruppenhomomorphismus $\overline{f} : \overline{G} \to H$, so daß $f = \overline{f} \circ p$, d.h. das Diagramm*



kommutiert, und $\overline{f}$ ist eindeutig mit dieser Eigenschaft.

Die Gruppe $\overline{G}$ zusammen mit dem Gruppenhomomorphismus $p : G \to \overline{G}$ ist eindeutig bis auf eindeutige Isomorphie: Wenn ein weiterer Gruppenhomomorphismus $p' : G \to G'$ mit denselben Eigenschaften existiert, dann gibt es einen eindeutigen Isomorphismus $\varphi : \overline{G} \xrightarrow{\sim} G'$, so daß $p' = \varphi \circ p$, d.h. das Diagramm



kommutiert.

Beweis. Zur Existenz benutzen wir die Konstruktion $\overline{G} = G/N$ mit der Abbildung

$$\begin{aligned} p : G &\to G/N \\ g &\mapsto gN. \end{aligned}$$

Dies ist in der Tat ein Gruppenhomomorphismus, denn für alle $g, h \in G$ gilt

$$p(gh) = ghN = gNhN = p(g)p(h).$$

Weiter gilt $p(g) = 1$ genau dann, wenn $gN = N$ also wenn $g \in N$. Es gilt somit (i).

Sei $f : G \to H$ ein Gruppenhomomorphismus mit $f(N) = 1$. Dann ist f konstant auf Nebenklassen von N, denn $f(gN) = f(g)f(N) = f(g)$, und

$$\begin{aligned} \varphi : G/N &\to H \\ gN &\mapsto f(gN) \end{aligned}$$

ist ein wohldefinierter Gruppenhomomorphismus:

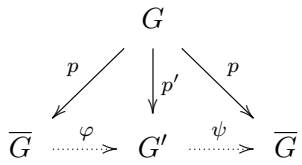
$$\varphi(gNhN) = \varphi(ghN) = f(ghN) = f(gNhN) = f(gN)f(hN) = \varphi(gN)\varphi(hN).$$

Es gilt

$$f(g) = \varphi(gN) = \varphi(p(g)),$$

und ein solches φ ist eindeutig durch f bestimmt, denn $\varphi(gN) = f(g)$.

Zur Eindeutigkeit nehmen wir an, es gibt mit $p' : G \twoheadrightarrow G'$ einen zweiten Kandidaten. Aus Eigenschaft (ii) erhalten wir $\varphi : \overline{G} \to G'$ und $\psi : G' \to \overline{G}$, so daß



kommutiert. Damit löst $\varphi \circ \psi$ das Fortsetzungsproblem für $f = p$, genauso wie $\mathrm{id} : \overline{G} \to \overline{G}$. Die geforderte Eindeutigkeit erzwingt $\varphi \circ \psi = \mathrm{id}$. Aus Symmetrie folgt $\psi \circ \varphi = \mathrm{id}$ und dies zeigt die Eindeutigkeit des Quotienten. □

Definition 4.15. Ein $\overline{G}$ mit $p : G \to \overline{G}$ wie in Satz 4.14 heißt **Quotient** und p heißt **Quotientenabbildung** oder genauer **Quotientenhomomorphismus**.

Bemerkung 4.16. Aus dem Beweis von Satz 4.14 folgt, daß Faktorgruppen G/N zusammen mit der natürlichen Abbildung $G \to G/N$ Quotienten sind. Wegen der Eindeutigkeit sind Quotientenabbildungen 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.

Der Existenzsatz für Quotienten illustriert ein wiederkehrendes Motiv in der Mathematik:

Konstruktion konkret, explizit	$\leftrightarrow$	**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.

Beispiel 4.17 (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.

Proposition 4.18. *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. □

Bemerkung 4.19. Man kann in Proposition 4.18 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

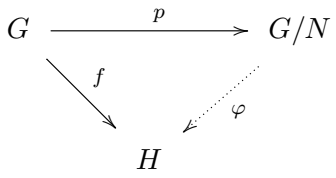
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \notin N.$$

4.3. **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 von Quotienten nach Normalteilern zusammen mit der dort gezeigten Eindeutigkeit.

Satz 4.20 (Homomorphiesatz)**.** *Sei $f : G \to H$ ein surjektiver Homomorphismus mit Kern $N = \ker(f)$. Dann gibt es einen eindeutigen Isomorphismus*

$$\varphi : G/N \xrightarrow{\sim} H,$$

so daß $f = \varphi \circ p$ mit der Quotientenabbildung $p : G \to G/N$. Mit andern Worten kommutiert das folgende Diagramm.



Beweis. Die Existenz und Eindeutigkeit eines Gruppenhomomorphismus

$$\varphi : G/N \to H$$

mit $f = \varphi \circ p$ folgt aus der Quotienteneigenschaft der Abbildung $p : G \to G/N$ aus dem Beweis von Satz 4.14. 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 φ hat trivialen Kern. Somit ist φ injektiv nach Proposition 3.25.

Die Abbildung φ ist surjektiv, denn für jedes $h \in H$ gibt es (f surjektiv) ein $g \in G$ mit $f(g) = h$, und dann gilt $\varphi(gN) = f(g) = h$. Damit ist φ sogar bijektiv und ein Isomorphismus. □

Satz 4.21 (Erster Isomorphiesatz)**.** *Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler. Dann ist*

$$H/(H \cap N) \xrightarrow{\sim} HN/N$$
$$h(H \cap N) \mapsto hN$$

ein Gruppenisomorphismus. Insbesondere gilt:

(1) Das naive Produkt 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. Wir können f als surjektiven Homomorphismus

$$F : H \twoheadrightarrow HN/N$$

auffassen. Der Homomorphiesatz, Satz 4.20, angewandt auf F liefert den gesuchten Isomorphismus

$$\varphi : H/(H \cap N) \xrightarrow{\sim} HN/N,$$

denn $\ker(F) = \ker(f) = H \cap N$. Beachten Sie, daß $\varphi(h(H \cap N)) = F(h) = hN$ nach Konstruktion von φ wie in Satz 4.20. □

Beispiel 4.22. (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 E 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

$$\begin{aligned} K^\times &\to D \\ \lambda &\mapsto \lambda E = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda \end{pmatrix} \end{aligned}$$

Ferner ist D ein Normalteiler in $\mathrm{GL}_n(K)$, denn für $\lambda \in K^\times$ und $A \in \mathrm{GL}_n(K)$ gilt

$$A(\lambda E)A^{-1} = \lambda(AEA^{-1}) = \lambda(AA^{-1}) = \lambda E.$$

Die Faktorgruppe ist

$$\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/D$$

genannte die **projektiv lineare Gruppe**.

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 4.23 (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 des Quotienten aus Satz 4.14 liefert einen eindeutigen Gruppenhomomorphismus

$$f : G/N \to G/K$$

mit $f(gN) = gK$. Die Abbildung φ ist offensichtlich surjektiv und $\ker(f) = K/N$, denn $gK = K$ bedeutet $g \in K$. Der Homomorphiesatz, Satz 4.20, angewandt auf f liefert den gesuchten Isomorphismus

$$\varphi : (G/N)/(K/N) \xrightarrow{\sim} G/K$$

und $\varphi(gN(G/K)) = f(gN) = gK$ wie behauptet. □

Beispiel 4.24. 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

$$(\mathbb{Z}/nm\mathbb{Z})/(m\mathbb{Z}/nm\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z}.$$

Übungsaufgaben zu §4

Übungsaufgabe 4.1. Zeigen Sie, daß die Operation aus Aufgabe 2.6 eine Operation von $\mathrm{PGL}_{n+1}(K)$ auf $\mathbb{P}^n(K)$ induziert.

Übungsaufgabe 4.2. Sei $\mathbb{F}$ ein endlicher Körper mit q Elementen. Berechnen Sie die Ordnung der Gruppe $\mathrm{PGL}_n(\mathbb{F})$.

Übungsaufgabe 4.3. 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 $y \in X$ Dann gibt es einen eindeutigen Gruppenhomorphismus

$$\varphi : G \to H$$

mit der Eigenschaft

$$g.y = y.(\varphi(g)).$$

Wie ändert sich φ, wenn man ein anderes Element $y \in X$ wählt?

Übungsaufgabe 4.4. 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.

Übungsaufgabe 4.5. Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Der Normalisator $N_G(U)$ von U in G ist der Stabilisator von U bezüglich der Operation von G auf der Menge seiner Untergruppen durch Konjugation. Zeigen Sie, daß $U \subseteq N_G(U)$ und daß $N_G(U)$ die größte Untergruppe von G ist, in der U ein Normalteiler ist.

Übungsaufgabe 4.6. 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 als U identifizieren müssen.

Übungsaufgabe 4.7. 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 4.8. 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 Orthognonalraum 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 4.9 (Lineare Darstellung der Diedergruppe). Sei $n \geq 3$ eine natürliche Zahl und D_n die n-te Diedergruppe 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.

5. Beispiele und Konstruktionen mit Gruppen

5.1. **Zyklische Gruppen.** Die algebraisch einfachsten Gruppen sind die zyklischen Gruppen.

Definition 5.1. Eine Gruppe heißt **zyklisch**, wenn sie von einem Element erzeugt werden kann.

Beispiel 5.2. 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 der surjektiven Quotientenabbildung $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ auch das Bild von 1 ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$. Damit ist
$$\mathbb{Z}/n\mathbb{Z}$$
eine zyklische Gruppe, und zwar der Ordnung n.

Bemerkung 5.3. Sei $g \in G$ ein Gruppenelement. Dann definiert
$$\begin{aligned} \psi_g : \mathbb{Z} &\to G \\ i &\mapsto \psi_g(i) := g^i \end{aligned}$$
einen Gruppenhomomorphismus. Das Bild von ψ_g ist
$$\mathrm{im}(\psi_g) = \langle g \rangle.$$
Dies wurde im Beweis von Satz 3.12 als Zwischenschritt bewiesen. Der Kern von ψ_g ist per Definition erzeugt von $n = \mathrm{ord}(g)$, wenn die Ordnung endlich ist, oder eben $n = 0$, wenn

per Definition die Ordnung unendlich ist. Nach dem Homomorphiesatz 4.20 induziert ψ_g einen Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \simeq \langle g \rangle,$$

der die Nebenklasse $1 + n\mathbb{Z}$ auf g abbildet.

Satz 5.4. *Eine Gruppe G ist zyklisch genau dann, wenn es ein $n \in \mathbb{N}_0$ und einen Isomorphismus*

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

gibt.

Beweis. Ist G zyklisch, dann gibt es per Definition einen Erzeuger $g \in G$, also ein Element mit $G = \langle g \rangle$. Mit $n = 0$, falls g unenedliche Ordnung hat, oder $n = \operatorname{ord}(g)$, falls g endliche Ordnung hat, wurde in Bemerkung 5.3 der behauptete Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \simeq \langle g \rangle = G$$

konstruiert.

Sei umgekehrt G isomorph zu $\mathbb{Z}/n\mathbb{Z}$. Dann ist G zyklisch, denn das Bild eines Erzeugers von $\mathbb{Z}/n\mathbb{Z}$ erzeugt G. Nicht zu vergessen: solche Erzeuger gibt es, nämlich zum Beispiel die Restklasse der 1, siehe Beispiel 5.2. □

Satz 5.5. *Eine Gruppe G der endlichen Ordnung n ist zyklisch genau dann, wenn es ein Element der Ordnung n in G gibt.*

Beweis. Wenn G zyklisch ist, dann gibt es einen Erzeuger g und $\operatorname{ord}(g) = |\langle g \rangle| = |G|$ nach Satz 3.12.

Sei Umgekehrt $g \in G$ ein Element der Ordnung $\operatorname{ord}(g) = |G|$. Dann ist $\langle g \rangle \subseteq G$ eine Untergruppe der gleichen Ordnung, wieder nach Satz 3.12, und somit $\langle g \rangle = G$. Damit erzeugt g die Gruppe G, und G ist zyklisch. □

Satz 5.6. *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 $g \neq 1$ ein Element in G. Dann ist $\operatorname{ord}(g)$ ein Teiler von p aber nicht 1. Da p Primzahl ist, muß $\operatorname{ord}(g) = p$ sein. Dann hat die zyklische Untergruppe $\langle g \rangle$ genauso viele Elemente wie G. Daher gilt $G = \langle g \rangle$ und G ist zyklisch.

Nach obigem Beispiel gibt es (zu jedem Erzeuger von G) einen Isomorphismus $G \simeq \mathbb{Z}/p\mathbb{Z}$. Die Gruppe $\mathbb{Z}/p\mathbb{Z}$ ist in der Tat eine Gruppe der Ordnung p. Daher gibt es genau eine Gruppe von Primzahlordnung p. □

Satz 5.7. *Eine endliche zyklische Gruppe G der Ordnung N hat für jeden Teiler $d \mid N$ eine zyklische Untergruppe der Ordnung d. Dies sind alle Untergruppen von G.*

Beweis. Für jedes $n \in \mathbb{Z}$ ist die Abbildung $[n] : G \to G$ definiert durch $[n](g) = g^n$ für alle $g \in G$ ein Gruppenhomomorphismus. In der Tat, G ist abelsch und daher für alle $g, h \in G$

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

Sei $d \mid N$ ein Teiler der Gruppenordnung und $N = md$. Sei γ ein Erzeuger der Gruppe G. Dann hat γ^d die Ordnung m. In der Tat ist $(\gamma^d)^m = \gamma^N = 1$ und keine kleinere Potenz ist gleich 1, denn γ hat Ordnung N.

Aus Satz 3.12 folgt nun

$$\operatorname{im}([d]) = \{\gamma^{ad} \ ; \ a \in \mathbb{Z}\} = \langle \gamma^d \rangle = \{1, \gamma^d, \ldots, \gamma^{(m-1)d}\}.$$

Wir schließen aus dem Satz von Lagrange, Satz 3.10 und Proposition 3.26, daß

$$|\ker([d])| = \frac{|G|}{(G : \ker([d]))} = \frac{|G|}{|\operatorname{im}([d])|} = \frac{N}{m} = d.$$

Damit ist
$$\ker([d]) = \{g \in G \;;\; g^d = 1\}$$
eine Untergruppe von G der Ordnung d. Dies zeigt die Existenz der behaupteten Untergruppe der Ordnung d.

Der kleine Fermat, Korollar 3.15, zeigt $(g^m)^d = g^N = 1$ für alle $g \in G$. Daher gilt
$$\mathrm{im}([m]) \subseteq \ker([d]).$$
Beide Seiten bestehen aus d Elementen und sind daher gleich. Die Gruppe $\mathrm{im}([m])$ wird von γ^m erzeugt und ist zyklisch. Die gefundene Untergruppe der Ordnung d ist somit zyklisch.

Sei U eine Untergruppe der Ordnung $|U| = d$. Nach dem kleinen Fermat, Korollar 3.15, erfüllt jedes Element $g \in U$ die Gleichung $g^d = 1$. Es gilt also
$$U \subseteq \{g \in G \;;\; g^d = 1\}.$$
Da sowohl U als auch $\ker([d])$ aus d Elementen bestehen, muß $U = \ker([d])$ sein. Die Untergruppe der Ordnung d ist daher eindeutig.

Nach dem Satz von Lagrange, Satz 3.10, muß die Ordnung einer Untergruppe von G ein Teiler von $|G|$ sein. Dies zeigt, daß wir bereits sämtliche Untergruppen von G beschrieben haben. □

Proposition 5.8. *Sei G eine zyklische Gruppe mit Erzeuger $g \in G$ von endlicher Ordnung N. Dann ist g^a auch ein Erzeuger genau dann, wenn a und N teilerfremd sind, d.h., der größte gemeinsame Teiler von a und N gleich 1 ist.*

Beweis. Wenn $d \mid a$ und $d \mid N$, dann gilt mit $N' = N/d \in \mathbb{Z}$ und $a' = a/d \in \mathbb{Z}$
$$(g^a)^{N'} = g^{a'dN'} = g^{a'N} = (g^N)^{a'} = 1.$$
Also liegt g^a in einer Untergruppe der Ordnung N' in G. Wenn g^a die Gruppe G erzeugt, muß $N' = N$ und damit $d = 1$ sein. Es müssen also a und N teilerfremd sein.

Seien umgekehrt a und N teilerfremd und sei $h = g^a$. Die Abbildung
$$\psi_h : \mathbb{Z} \to G$$
aus Bemerkung 5.3 den Kern $N\mathbb{Z}$, denn
$$\psi_h(n) = 1 \iff h^n = 1 \iff g^{an} = 1 \iff N \mid an \iff N \mid n.$$
Nach dem Homomorphiesatz gilt $\mathbb{Z}/N\mathbb{Z} \simeq \mathrm{im}(\psi_h) = \langle g^a \rangle$. Diese Untergruppe von G hat also $|G|$-viele Elemente, also $\langle g^a \rangle = G$ und g^a ist ein Erzeuger. □

Definition 5.9. Die **Eulersche φ-Funktion** $\varphi : \mathbb{N} \to \mathbb{N}$ ist definiert als
$$\varphi(n) = |\{a \in \mathbb{N} \;;\; 1 \leq a \leq n,\ a \text{ und } n \text{ sind teilerfremd}\}|.$$

Korollar 5.10. *Für alle $n \in \mathbb{N}$ gilt*
$$\sum_{d \mid n} \varphi(d) = n.$$

Beweis. Wir betrachten die Abbildung
$$u : \mathbb{Z}/n\mathbb{Z} \to \{U \subseteq \mathbb{Z}/n\mathbb{Z} \;;\quad \text{Untergruppe}\}$$
$$g \mapsto u(g) := \langle g \rangle.$$
Die Menge der Untergruppen ist über die Teiler $d \mid n$ parameterisiert nach Satz 5.7: zu jedem d gibt es eine Untergruppe U_d der Ordnung d (nämlich $m\mathbb{Z}/n\mathbb{Z}$ mit $n = dm$). Die Faser der Abbildung u besteht aus der Menge der Erzeuger der jeweiligen Untergruppe. Die Untergruppe der Ordnung d hat $\varphi(d)$ Erzeuger nach Proposition 5.8. Jetzt summieren wir über die Fasern der Abbildung u und erhalten
$$\sum_{d \mid n} \varphi(d) = \sum_{d \mid n} |u^{-1}(U_d)| = |\mathbb{Z}/n\mathbb{Z}| = n.$$

□

Satz 5.11. *Eine endliche Gruppe der Ordnung N ist zyklisch genau dann, wenn es zu jedem Teiler $d \mid N$ höchstens d Elemente $g \in G$ gibt mit* $\mathrm{ord}(g) \mid d$.

Beweis. Sei G zyklisch von Ordnung N und $d \mid N$. Die Elemente mit $g^d = 1$ sind die d Elemente von $\ker([d])$, siehe Beweis von Satz 5.7. Dies zeigt, daß zyklische Gruppen die beschriebene Eigenschaft haben.

Sei nun umgekehrt G eine endliche Gruppe der Ordnung N und zu jedem Teiler $d \mid N$

$$|\{g \in G \ ; \ g^d = 1\}| \leq d.$$

Wenn es in G ein Element $x \in G$ der Ordnung d gibt, dann haben die d Elemente in $\langle x \rangle$ alle einen Teiler von d als Ordnung. Daher gilt dann

$$\{g \in G \ ; \ g^d = 1\} = \langle x \rangle.$$

Die Elemente in G von genau der Ordnung d liegen daher in $\langle x \rangle$ und sind Erzeuger dieser zyklischen Gruppe. Es gibt also in G entweder $r_d = 0$ oder $r_d = \varphi(d)$ viele Elemente der Ordnung d. Nach dem Satz von Lagrange, Satz 3.10, ist diese Anzahl 0 für alle $d \nmid N$. Wir schätzen nun die Anzahl der Elemente von Ordnung N ab, indem wir von allen Elementen aus G diejenigen mit Ordnung $< N$ abziehen, also mittels Korollar 5.10 durch

$$r_N = |G| - \sum_{d|N, d<N} r_d \geq N - \sum_{d|N, d<N} \varphi(d) = \varphi(N) > 0.$$

Daher gibt es in G ein Element der Ordnung N, sagen wir g. Dann hat die Untergruppe $\langle g \rangle \subseteq G$ schon N Elemente, die Inklusion ist also eine Gleichheit, und G ist zyklisch. □

Korollar 5.12. *Sei K ein Körper und $G \subseteq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Sei d ein Teiler der Gruppenordnung N. Dann ist

$$\{x \in G \ ; \ \mathrm{ord}(x) \mid d\} \subseteq \{x \in K \ ; \ x^d - 1\}$$

eine Teilmenge der Lösungen aus K eines Polynoms vom Grad d, also bestehend aus höchstens d Elementen. Nach Satz 5.11 muß G zyklisch sein. □

Korollar 5.13. *Die multiplikative Gruppe $\mathbb{F}^\times$ eines endlichen Körpers $\mathbb{F}$ ist zyklisch.*

Beweis. Die Gruppe $\mathbb{F}^\times$ ist endlich, so daß Korollar 5.12 auf $\mathbb{F}^\times$ anwendbar ist. □

Bemerkung 5.14. Sei $\mathbb{F}$ ein endlicher Körper und $\gamma \in \mathbb{F}^\times$ ein Erzeuger. Dann induziert ψ_γ einen Isomorphismus

$$\begin{aligned} \Psi_\gamma : \mathbb{Z}/(p-1)\mathbb{Z} &\to \mathbb{F}^\times \\ a &\mapsto \gamma^a. \end{aligned}$$

Von zentraler Bedeutung für Kryptographie mit RSA ist die Tatsache (Wette), daß Ψ_γ sehr viel schneller auszurechnen ist (also zu $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ den Wert γ^a zu ermitteln), also der **diskrete Logarithmus** zur Basis γ. Dies ist der Name des inversen Isomorphismus, der zu einem $x\mathbb{F}^\times$ den Exponenten zur Basis γ berechnet:

$$\log_\gamma(x) := a \iff \gamma^a = x.$$

5.2. **Produkte.**

Definition 5.15. (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 5.16. (1) 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

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

(2) Sei $n \in I$ ein Element. Die Projektion auf die n-te Koordinate ist der Gruppenhomomorphismus

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

mit $p_n((g_i)_{i\in I}) = g_n$.

Definition 5.17. Sei I eine Menge und für jedes $i \in I$ mit G_i eine Gruppe gegeben. Ein **Produkt** der Gruppen G_i für alle $i \in I$ ist eine Gruppe P zusammen Gruppenhomomorphismen

$$p_i : P \to G_i,$$

so daß die **universelle Eigenaschaft für Produkte** gilt: für jede Gruppe G und Gruppenhomomorphismen $f_i : G \to G_i$ für alle $i \in I$ ein eindeutiger Gruppenhomomorphismus

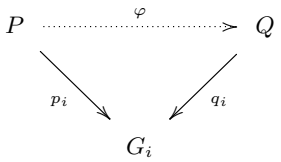
$$f : G \to P$$

existiert mit $p_i \circ f = f_i$.

Satz 5.18 (Existenz von Produkten)**.** *Produkte von Gruppen existieren und sind eindeutig bis auf eindeutigen Isomorphismus. Genauer: sei I eine Menge, G_i eine Gruppe für alle $i \in I$ und seien P mit $p_i : P \to G_i$ sowie Q mit $q_i : Q \to G_i$ für alle $i \in I$ Produkte. Dann gibt es einen eindeutigen Isomorphismus*

$$\varphi : P \xrightarrow{\sim} Q$$

mit $p_i = q_i \circ \varphi$, d.h. das Diagramm



kommutiert.

Beweis. Zuerst zeigen wir, daß $\prod_{i\in I} G_i$ zusammen mit den Projektionen p_i die geforderte Eigenschaft hat. Seien $f_i : G \to G_i$ Gruppenhomomorphismen. Dann definiert

$$\begin{aligned} f : G &\to \prod_{i\in I} G_i \\ g &\mapsto (f_i(g))_{i\in I} \end{aligned}$$

einen Gruppenhomomorphismus, so daß per Definition $p_n \circ f = f_n$ für alle $n \in I$:

$$f(g)_n = p_n(f(g)) = p_n((f_i(g))_{i\in I}) = f_n(g).$$

Sei $f' : G \to \prod_{i\in I} G_i$ ein weiterer solcher. Dann ist für alle $g \in G$ die n-te Komponente von $\varphi(g)$ genau

$$\varphi(g)_n = p_n(\varphi(g)) = (p_n\varphi)(g) = f_n(g).$$

Damit ist $\varphi(g) = (f_i(g))_{i\in I} = f(g)$ und f eindeutig mit der geforderten Eigenschaft.

Die Eindeutigkeitsaussage für das Produkt folgt genau wie im Beweis von Satz 4.14. Seien P mit $p_i : P \to G_i$ und Q mit $q_i : Q \to G_i$ für alle $i \in I$ Produkte für die Gruppen G_i, $i \in I$. Dann gehört nach der universellen Eigenschaft des Produkts Q zu den p_i ein Gruppenhomomorphismus $\varphi : P \to Q$ mit $q_i \circ \varphi = p_i$, und nach

der universellen Eigenschaft des Produkts P gehört zu den q_i ein Gruppenhomomorphismus $\psi : Q \to P$ mit $p_i \circ \psi = q_i$.

Nun erfüllen sowohl $\varphi \circ \psi$ als auch die Identität $\mathrm{id}_Q : Q \to Q$ die Bedingung aus der universellen Eigenschaft von Q für die Gruppenhomomrphismen q_i. Aus der Eindeutigkeit folgt $\varphi \circ \psi = \mathrm{id}_Q$. Analog folgt $\psi \circ \varphi = \mathrm{id}_P$. Damit sind φ und ψ zueinander inverse Isomorphismen, und eindeutig mit der Eigenschaft, mit den p_i bzw. q_i in der geforderten Weise kompatibel zu sein. □

Notation 5.19. Da nun einmal das direkte Produkt ein Produkt im Sinne von Satz 5.18 ist, verwendet man allgemein für Produkte die Notation

$$\prod_{i \in I} G_i$$

oder $G_1 \times G_2$, oder $G_1 \times \ldots\ldots \times G_n$, wenn $I = \{1, 2\}$ oder $I = \{1, \ldots, n\}$.

Bemerkung 5.20. (1) Sei $n \in I$ ein Element. Die Inklusion der n-ten Koordinate ist der Gruppenhomomorphismus

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

mit

$$\iota_n(g) = (1, \ldots, 1, \underset{\uparrow n}{g}, 1, \ldots, 1).$$

Dieser Gruppenhomomorphimus gehört nach Satz 5.18 zum System von Homomorphismen $f_i : G_n \to G_i$ mit $f_n = \mathrm{id}_{G_n}$ und $f_i(h) = 1 \in G_i$ für $i \neq n$ und alle $h \in G_n$.

(2) Seien H und K Untergruppen der Gruppe G. Wenn die Multiplikation

$$\begin{aligned} \mu : H \times K &\to G \\ (h, k) &\mapsto hk \end{aligned}$$

ein Gruppenisomorphismus ist, so nennt man G das **innere (direkte) Produkt** von H und K. Nun ist μ keinesfalls immer ein Gruppenhomomorphismus. Genauer ist μ ein Gruppenhomomorphismus genau dann, wenn H mit K kommutiert, d.h., für alle $h \in H$ und $k \in K$ gilt $hk = kh$. In der Tat, wenn μ Gruppenhomomorphismus ist, dann gilt

$$hk = \mu\big((h, k)\big) = \mu\big((1, k)(h, 1)\big) = \mu\big((1, k)\big)\mu\big((h, 1)\big) = kh.$$

Und umgekehrt, wenn H und K kommutieren, dann gilt für alle $h_1, h_2 \in H$ und $k_1, k_2 \in K$, daß

$$\mu\big((h_1, k_1)(h_2, k_2)\big) = \mu\big(h_1 h_2, k_1 k_2\big) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \mu\big((h_1, k_1)\big)\mu\big((h_2, k_2)\big).$$

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

(4) Das Bild der Inklusion $G \hookrightarrow G \times H$ ist ein Normalteiler. Wir bezeichnen es der Einfachheit halber auch mit G, genauso $H \subseteq G \times H$. Es gilt

$$H \simeq (G \times H)/G$$

wie man aus dem ersten Isomorphiesatz wegen $H \cap G = \{1\}$ und $H = H/\{1\}$ folgert.

5.3. **Semidirekte Produkte.** Die Konstruktion des Produkts läßt sich wie folgt verallgemeinern.

Lemma–Definition 5.21. *Das **semi-direkte Produkt** einer Gruppe N mit einer Gruppe Γ bezüglich des Gruppenhomomorphismus $\alpha : \Gamma \to \mathrm{Aut}(N)$ ist die Gruppe $G = N \rtimes_\alpha \Gamma$ definiert als Menge durch*

$$G = N \times \Gamma$$

mit der Verknüpfung definiert für $n, m \in N$ und $g, h \in \Gamma$ durch

$$(n, g)(m, h) := (n\alpha(g)(m), gh).$$

Beweis. Wr müssen zeigen, daß es in $N \rtimes_\alpha \Gamma$ ein neutrales Element gibt. Dies ist $e = (1, 1)$, denn für $n \in N$ und $g \in \Gamma$ gilt

$$(n, g)(1, 1) = (n, g) = (1, 1)(n, g).$$

Weiter müssen wir zeigen, daß die Komposition ein Inverses besitzt. Für $n \in N$ und $g \in \Gamma$ ist

$$(n, g)(\alpha(g^{-1})(n^{-1}), g^{-1}) = (n\alpha(g)\big(\alpha(g^{-1})(n^{-1})\big), gg^{-1}) = (nn^{-1}, 1) = (1, 1)$$

und

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

Daher ist $(\alpha(g^{-1})(n^{-1}), g^{-1})$ ein Inverses zu (n, g).

Jetzt fehlt noch die Assoziativität, die wir zur Übung überlassen. □

Bemerkung 5.22. 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 5.23. 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 Γ auf $N = \prod_{\gamma\in\Gamma} H$ durch

$$\alpha : \Gamma \to \mathrm{Aut}(N)$$

durch die folgende Permutation der Komponenten operiert. Für $g \in \Gamma$ und $n = (h_\gamma)_{\gamma\in\Gamma} \in N$ gilt

$$\alpha(g)(n) = (h_{\gamma g})_{\gamma\in\Gamma}.$$

In der Tat handelt es sich bei $\alpha(g) : N \to N$ um einen Automorphismus von N. Und die Zuordnung $g \mapsto \alpha(g)$ is ein Gruppenhomomorphismus, denn für $g_1, g_2 \in G$ und $n = (h_\gamma)_{\gamma\in\Gamma} \in N$ gilt

$$\alpha(g_1)\big(\alpha(g_2)(n)\big) = \alpha(g_1)\big((h_{\gamma g_2})_{\gamma\in\Gamma}\big) = (h_{\gamma g_1 g_2})_{\gamma\in\Gamma} = \alpha(g_1g_2)(n).$$

Man beachte die Reihenfolge der g_i. Es wird γ zu γg substituiert, also im zweiten Schritt γg_2 zu $(\gamma g_1)g_2$.

5.4. **Das Zentrum.**

Definition 5.24. Das **Zentrum** einer Gruppe G ist die Teilmenge

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

derjenigen Element, die mit allen Gruppenelementen kommutieren.

Proposition 5.25. *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. □

Definition 5.26. Sei p eine Primzahl. Eine **p-Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

Satz 5.27. *Jede p-Gruppe hat nichttriviales Zentrum.*

Beweis. Jeder Orbit für die Operation einer p-Gruppe G hat als Länge eine Potenz von p. Entweder der Orbit besteht aus nur einem Element, einem Fixpunkt der Operation, oder der Orbit hat durch p teilbare Länge. Wir zerlegen nun G in Bahnen bezüglich der Konjugationsoperation. Sei P die Vereinigung der Bahnen, welche Länge > 1 haben. Dann ist $|P|$ ein Vielfaches von p und nach dem Bahnensatz

$$|Z(G)| = |G| - |P|$$

auch ein Vielfaches von p. Jetzt kommt dieselbe Pointe, wie im Beweis des Satzes von Cauchy, Satz 2.25. Das neutrale Element gehört zum Zentrum $Z(G)$, also ist $|Z(G) > 0$. Da es sich um ein Vielfaches von p handelt, gilt sogar $|Z(G)| \geq p$, und somit ist das Zentrum nicht die triviale Untergruppe. □

5.5. **Kommutatoren und abelsche Quotienten.** Kommutatoren messen die Abweichung von Kommutativität.

Definition 5.28. Der **Kommutator** zweier Gruppenelemente $g, h \in G$ ist das Element

$$[g, h] = ghg^{-1}h^{-1} \in G.$$

Notation 5.29. 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 5.30. *Seien $g, h \in G$ Gruppenelemente. Dann kommutieren g und h genau dann, wenn $[g, h] = 1$ gilt.*

Beweis. Es gilt $gh = hg$ genau dann, wenn $[g, h] = ghg^{-1}h^{-1} = hg(g^{-1}h^{-1}) = 1$ gilt. □

Definition 5.31. 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 5.32. Als Notation für die Kommutatorgruppe zu G findet man auch $G' = [G, G]$.

Satz 5.33 (Abelisierung)**.** *Sei G eine Gruppe. Dann gilt:*

(1) Die Komutatorgruppe $[G, G]$ ist ein Normalteiler in G.

(2) Die Faktorgruppe $G/[G,G]$ ist abelsch.
(3) Die Quotientenabbildung $p : G \to G/[G,G]$ hat die folgende universelle Eigenschaft.
Ein Gruppenhomorphismus $f : G \to H$ faktorisiert über p, d.h. es gibt einen Gruppenhomomorphismus $\varphi : G/[G,G] \to H$ mit $f = \varphi \circ p$, genau dann, wenn $\mathrm{im}(f)$ eine abelsche Gruppe ist. Das φ ist dann eindeutig.

Beweis. (1) Seien $g, x, y \in G$ beliebige Gruppenelemente und $a = g^{-1}xg$ und $b = g^{-1}yg$. Dann ist

$$g[a,b]g^{-1} = \varphi_g(aba^{-1}b^{-1}) = \varphi_g(a)\varphi_g(b)\varphi_g(a)^{-1}\varphi_g(b)^{-1} = [x,y].$$

Alle Kommutatoren $[x,y]$ sind daher in der Untergruppe $\varphi_g([G,G])$ enthalten und daher

$$[G,G] \subseteq g[G,G]g^{-1}$$

für alle $g \in G$. Nach Lemma 4.5 ist damit $[G,G]$ ein Normalteiler in G.

(2) 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.

(3) Angenommen f faktorisiert wie im Satz. Für beliebige Elemente $x, y \in \mathrm{im}(f)$ gibt es dann $a, b \in G$ mit $f(a) = x$ und $f(b) = y$. Dann ist $[x,y]$ das Bild $f([a,b]) = \varphi(p([a,b])$, und weil $p([a,b]) = 1$ folgt $[x,y] = 1$. Es ist also $\mathrm{im}(f)$ kommutativ.

Sei umgekehrt $\mathrm{im}(f)$ kommutativ. Dann ist für alle $a, b \in G$

$$f([a,b]) = [f(a), f(b)] = 1,$$

denn $\mathrm{im}(f)$ ist kommutativ, und somit $[a,b] \in \ker(f)$. Der Kern enthält also alle Kommutatoren und damit auch die von den Kommutatoren erzeugte Untergruppe

$$[G,G] \subseteq \ker(f).$$

Der Rest folgt aus der universellen Eigenschaft des Quotienten nach Satz 4.14 zusammen damit, daß $p : G \to G/[G,G]$ eine Quotientenabbildung ist. □

Definition 5.34. Die **Kommutatorfaktorgruppe** (oder **Abelisierung**) einer Gruppe G ist die Gruppe $G^{\mathrm{ab}} = G/[G,G]$ zusammen mit der Quotientenabbildung $G \to G^{\mathrm{ab}}$.

Übungsaufgaben zu §5

Übungsaufgabe 5.1. Sei $n \geq 1$ eine natürliche Zahl. Bestimmen Sie das Zentrum von S_n.

Übungsaufgabe 5.2. Sei $n \geq 1$ eine natürliche Zahl und K ein Körper. Bestimmen Sie das Zentrum von $\mathrm{GL}_n(K)$.

Übungsaufgabe 5.3. Bestimmen Sie die Kommutatorfaktorgruppe von S_n.

Übungsaufgabe 5.4. Die Diedergruppe D_4 und die Quaternionengruppe Q_8 sind beides Gruppen der Ordnung 8. Bestimmen Sie für beide Gruppen die Ordnungsstatistik: die vorkommenden Ordnungen der Elemente und wieviele Elemente eine gegebene Ordnung haben. Zeigen Sie, daß D_4 und Q_8 nicht isomorph sind.

Teil 2. Ringe

6. Ringe

6.1. **Definition und Beispiele.** Ringe sind Strukturen mit Addition und Multiplikation.

Definition 6.1. (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 Element 1, das neutrales Element für die Multiplikation ist: für alle $a \in R$ gilt

$$1 \cdot a = a = a \cdot 1.$$

(2) Ein **kommutativer Ring** ist ein Ring dessen Multiplikation kommutativ ist: für alle $a, b \in R$ gilt

$$a \cdot b = b \cdot a.$$

Bemerkung 6.2. 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 6.3. Die Multiplikation kürzen wir ab durch

$$ab := a \cdot b.$$

Außerdem gilt 'Punkt vor Strich'. Diese Festlegung spart Klammern.

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 $a - b$.

Beispiel 6.4. (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

$$\mathrm{Abb}(X, R) := \{f \ ; \ f : X \to R\}$$

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.

Bemerkung 6.5. 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. Wären 1 und $1'$ Einsen, dann gilt

$$1 = 1 \cdot 1' = 1'.$$

Es gelten die üblichen Rechenregeln für $-$, insbesondere das Distributivgesetz mit $-$ statt $+$.

Lemma 6.6. *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 6.7. *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 6.8. 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 jeder Mathematikstudierender kennen.

Beispiel 6.9. 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. Sei $f = \sum_{i=0}^{\infty} a_i X^i$ und $g = \sum_{i=0}^{\infty} b_i X^i$, dann ist

$$f + g = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

und

$$fg = \sum_{i=0}^{\infty} \big(\sum_{j+k=i} a_j b_k \big) X^i.$$

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. Wir schreiben suggestiv

$$\sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 + \dots.$$

'Formale Variabe' 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. Die Ringaxiome verifiziert man leicht, etwa die Assoziativität

$$\begin{aligned}
\big(\sum_{i=0}^{\infty} a_i X^i \cdot \sum_{i=0}^{\infty} b_i X^i\big) \cdot \sum_{i=0}^{\infty} c_i X^i &= \sum_{i=0}^{\infty} \big(\sum_{j+k=i} a_j b_k \big) X^i \cdot \sum_{i=0}^{\infty} c_i X^i \\
&= \sum_{i=0}^{\infty} \big(\sum_{r+s=i} \big(\sum_{j+k=r} a_j b_k \big) c_s \big) X^i \\
&= \sum_{i=0}^{\infty} \big(\sum_{j+k+l=i} a_j b_k c_l \big) X^i \\
&= \dots \text{ rückwärts } \dots \\
&= \sum_{i=0}^{\infty} a_i X^i \cdot \big(\sum_{i=0}^{\infty} b_i X^i \cdot \sum_{i=0}^{\infty} c_i X^i \big).
\end{aligned}$$

Der Potenzreihenring hat Möglichkeiten, die der Polynomring nicht hat. Etwa hat das Polynom $1 - X \in R[[X]]$ als formale Potenzreihe ein multiplikatives Inverses, nämlich

$$\sum_{i=0}^{\infty} X^i.$$

Bemerkung 6.10. 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 Potenzreihe

$$X^i = 0 + \ldots + 0 \cdot X^{i-1} + 1 \cdot X^i + 0 \cdot X^{i+1} + \ldots$$

ist. 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

$$\sum_{i=0}^{\infty} a_i X^i.$$

Der Polynomring ist ein Unterring im formalen Potenzreihenring.

Definition 6.11. 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 6.12. Sei R ein Ring. Der **Polynomring** mit Koeffizienten in R ist der Unterring

$$R[X] \subseteq R[[X]]$$

derjenigen formalen Potenzreihen $f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ mit: es gibt ein $n \geq 0$ und $a_i = 0$ für alle $i > n$. Man schreibt dann für f (mit diesem n oder besser 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.

Beispiel 6.13. 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.

6.2. **Einheiten.**

Definition 6.14. Eine **Einheit** ist ein Ringelement $a \in R$ mit multiplikativem Inversen in R: es gibt ein $b \in R$ mit

$$ab = ba = 1.$$

Satz 6.15. *Für einen Ring R ist die Menge der Einheiten*

$$R^\times = \{a \in R \; ; \quad a \text{ ist Einheit}\}$$

eine Gruppe bezüglich Mutiplikation aus R. Diese Gruppe heißt ***Einheitengruppe*** *von R.*

Beweis. Übung. □

Beispiel 6.16. Die Einheiten von $\mathbb{Z}$ sind $\mathbb{Z}^\times = \{1, -1\}$, und als Gruppe isomorph zu $\mathbb{Z}/2\mathbb{Z}$.

Definition 6.17. Ein **Körper** ist ein Ring R mit $R^\times = R \setminus \{0\}$ und $0 \neq 1$.

6.3. **Homomorphismen.** Wir wollen algebraische Strukturen stets zusammen mit den strukturerhaltenden Abbildungen untersuchen.

Definition 6.18. Ein **Ringhomomorphismus** ist eine Abbildung $f : R \to S$ zwischen Ringen R und S, so daß für alle $a, b \in R$ gilt:

(i) $f(a+b) = f(a) + f(b)$, es ist also f ein Gruppenhomomorphismus der zugrundeliegenden abelschen Gruppen,
(ii) $f(ab) = f(a)f(b)$,
(iii) $f(1) = 1$.

Ein **Ringisomorphismus** ist ein bijektiver Ringhomomorphismus.

Beispiel 6.19. Sei R ein Ring und $\varphi : Y \to X$ eine Abbildung von Mengen. Dann definiert das folgende einen Ringhomomorphismus:

$$\begin{aligned} \varphi^* : \mathrm{Abb}(X, R) &\to \mathrm{Abb}(Y, R) \\ (f : X \to R) &\mapsto \varphi^* f = (f \circ \varphi : Y \to R), \end{aligned}$$

also $(\varphi^* f)(y) = f(\varphi(y))$ für alle $y \in Y$.

Für eine einpunktige Menge $Y = \{x\}$ ist $\mathrm{Abb}(Y, R) \simeq R$ indem wir eine Funktion $f : Y \to R$ durch ihren Funktionswert $f(x) \in R$ beschreiben. Die Abbildung $f \mapsto f(x)$ ist bijektiv und ein Ringisomorphismus.

Ein Spezialfall wird gegeben durch ein $x \in X$ und die Inklusion $i : Y = \{x\} \hookrightarrow X$. Dann ist

$$\begin{aligned} i^* : \mathrm{Abb}(X, R) &\to \mathrm{Abb}(\{x\}, R) \simeq R \\ f &\mapsto i^* f = f(x). \end{aligned}$$

Dies ist der Auswertungsringhomomorphismus der Funktionen auf X im Punkt $x \in X$.

Beispiel 6.20. 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 6.21. Sei K ein Körper. Dann ist

$$\begin{aligned} K &\to \mathrm{M}_2(K) \\ a &\mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

ist **kein** Ringhomomorphismus. Wohl aber ist mit der Einheitsmatrix $E \in \mathrm{M}_n(K)$ die Abbildung

$$\lambda \mapsto \lambda E = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

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 $K \to \mathrm{M}_n(K)$.

Bemerkung 6.22. Für jeden Ringhomomorphismus $f : R \to S$ und $a \in R$ gilt

$$f(-a) = -f(a).$$

Das ist klar, denn f ist ein Gruppenhomomorphismus der zugrundeliegenden additiven Gruppen.

Bemerkung 6.23. 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. Weiter

$$1 = f(1) \in \mathrm{im}(f)$$

und

$$xy = f(a)f(b) = f(ab) \in \mathrm{im}(f).$$

Beispiel 6.24. Sei R ein Ring. Die Abbildung

$$\begin{aligned} R &\to R[X] \\ a &\mapsto a = a + 0 \cdot X^1 + 0 \cdot X^2 + \dots, \end{aligned}$$

die jedes Element auf das konstante Polynom a abbildet, ist ein injektiver Ringhomomorphismus. Wir identifizieren R mit dem Unterring von $R[X]$, der durch das Bild gegeben ist.

Satz 6.25. *Sei R ein Ring und $f : R \to S$ ein Ringhomomorphismus. Sei $s \in S$ ein Element, das mit allen Elementen aus $f(R)$ kommutiert, d.h. für alle $a \in R$ gilt*

$$f(a)s = sf(a).$$

Dann gehört zu s, ein eindeutiger Ringhomomorphismus $\mathrm{ev}_s : R[X] \to S$, der Auswertungshomomorphismus in s:

$$\begin{aligned} \mathrm{ev}_s : R[X] &\to S \\ P(X) = \sum_{i=0}^{n} a_i X^i &\mapsto P(s) = \sum_{i=0}^{n} f(a_i) s^i, \end{aligned}$$

mit den Eigenschaften

(i) $\mathrm{ev}_s(a) = f(a)$ *für jedes a in $R \subseteq R[X]$.*
(ii) $\mathrm{ev}_s(X) = s$.

Beweis. Die Auswertung $P(X) \mapsto P(s)$ ist ein Ringhomomorphismus, denn für $P(X) = \sum_{i=0}^{n} a_i X^i$ und $Q(X) = \sum_{j=0}^{m} b_j X^j$ gilt

$$\begin{aligned} P(s)Q(s) &= \Big(\sum_{i=0}^{n} f(a_i)s^i\Big) \cdot \Big(\sum_{j=0}^{m} f(b_j)s^j\Big) && \text{(ziehe } s^i \text{ an } f(b_j) \text{ vorbei)} \\ &= \sum_{0 \le i \le n, 0 \le j \le m} f(a_i)f(b_j)s^i s^j \\ &= \sum_{0 \le i \le n, 0 \le j \le m} f(a_i b_j)s^{i+j} \\ &= \sum_{k=0}^{n+m} \sum_{i+j=k} f(a_i b_j)s^k \\ &= \sum_{k=0}^{n+m} f\Big(\sum_{i+j=k} a_i b_j\Big)s^k = (PQ)(s). \end{aligned}$$

und für die Addition analog. Weiter wird die Eins, also das konstante Polynom 1 zu $1 \in R$ 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

$$F(P) = F\Big(\sum_{i=0}^{n} a_i X^i\Big) = \sum_{i=0}^{n} F(a_i X^i) = \sum_{i=0}^{n} F(a_i) \cdot F(X)^i = \sum_{i=0}^{n} f(a_i)s^i = P(s) = \mathrm{ev}_s(P).$$

Dies zeigt die Eindeutigkeit. □

Man überlege sich zur Übung, wo im Satz 6.25 der Unterschied zwischen $R[X]$ und $R[[X]]$ wichtig ist.

Beispiel 6.26. 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 abbgebildet 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.

Ab jetzt betrachten wir nur noch kommutative Ringe mit Eins!

6.4. **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 6.27. 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 $ax \in I$.

Definition 6.28. Sei R ein Ring und $M \subseteq R$ eine Teilmenge. Das von M **erzeugte Ideal** ist

$$(M) = \{a_1x_1 + \ldots + a_nx_n \ ; \ n \in \mathbb{N}_0, a_i \in R, x_i \in M \text{ für } 1 \leq i \leq n\}.$$

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 $r \in R$. Multiplikation mit -1 führt zum additiven Inversen:

$$-(a_1x_1 + \ldots + a_nx_n) = (-1)(a_1x_1 + \ldots + a_nx_n) \in (M)$$

also ist (M) eine additive Untergruppe, und damit dann sogar ein Ideal. Offensichtlich ist (M) das kleinste Ideal in R, das die Menge M enthält:

$$(M) = \bigcap_{M \subseteq I,\ I \text{ Ideal in } R} I.$$

Beispiel 6.29. (1) Im Ring $\mathbb{Z}$ ist für jedes $n \in \mathbb{Z}$ die von n erzeugte Untergruppe ein Ideal

$$(n) = n\mathbb{Z} = \{na \ ; \ a \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

(2) In jedem Ring R sind $(0) = \{0\}$ und $(1) = R$ Ideale. Alle anderen Ideale von R heißen **echte Ideale** von R.
(3) Im Ring $\mathbb{Z}[X]$ ist

$$(2, X) = \{f = \sum_{i \geq 0} a_iX^i \ ; \ a_i \in \mathbb{Z} \text{ für alle } i \geq 0 \text{ und } 2 \mid a_0\}$$

ein Ideal.

Bemerkung 6.30. 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 6.31. *(1) Der Kern eines Ringhomomorphismus $f : R \to S$ ist ein Ideal.*
(2) Jedes Ideal ist der Kern eines geeigneten Ringhomomorphimus.
(3) 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 $I = \ker(p)$.

Beweis. (1) Der Kern von f ist auch der Kern von $f : (R, +) \to (S, +)$ als Gruppenhomomorphismus der additiven Gruppen, also ist $\ker(f) \subseteq R$ eine Untergruppe bezüglich Addition. Außerdem gilt für jedes $a \in R$ und $x \in \ker(f)$ auch $ax \in \ker(f)$, weil

$$f(ax) = f(a)f(x) = f(a)0 = 0.$$

Damit ist $\ker(f)$ ein Ideal.

Aussage (2) folgt aus (3), und das beweisen wir jetzt. 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. □

Definition 6.32. Der Ring R/I aus Satz 6.31 wird **Faktorring** von R nach I genannt. Die Quotientenabbildung $p : R \to R/I$ heißt **kanonische Projektion**.

Beispiel 6.33. 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 6.31.

6.5. Quotienten und Isomorphiesätze.

Satz 6.34 (Quotienten)**.** *Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist $p : R \to R/I$ eine Quotientenabbildung, d.h., es gilt die universelle Eigenschaft:*

(i) $I \subseteq \ker(p)$, und
(ii) für jeden Ringhomomorphismus $f : R \to S$ mit $I \subseteq \ker(f)$ gibt es ein eindeutiges $\varphi : R/I \to S$ mit $f = \varphi \circ p$.

Bemerkung 6.35. Wegen der universellen Eigenschaft ist der Quotient nach einem Ideal $I \subseteq R$ eindeutig bis auf eindeutigen Isomorphismus, sofern er existiert. Von der Existenz haben wir uns durch die Konstruktion des Faktorrings überzeugt.

Satz 6.36 (Homomorphiesatz)**.** *Sei $f : R \to S$ ein Ringhomomorphismus. Dann induziert f einen Isomorphismus*

$$\bar{f} : R/\ker(f) \to \mathrm{im}(f)$$
$$a + I \mapsto \bar{f}(a + I) = f(a)$$

Beweis. Der Beweis folgt analog zum Homomorphiesatz für Gruppen, Satz 4.20, aus der Quotienteneigenschaft von R/I.

Man kann auch sagen, daß $\bar{f}$ als Abbildung der Gruppen wegen Satz 4.20 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 Ringisomorphisimus ist. □

Beispiel 6.37. Die Struktur eines Faktorrings R/I beweist man am besten, indem man rät $S \simeq R/I$, 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 $(2, X)$.

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 6.38 (Erster Isomorphiesatz)**.** *Sei $U \subseteq R$ ein Unterring und $I \subseteq R$ ein Ideal.*
Dann ist $U \cap I$ ein Ideal in U und

$$\begin{aligned} U/(U \cap I) &\xrightarrow{\sim} (U + I)/I \\ u + (U \cap I) &\mapsto u + I \end{aligned}$$

ist ein Isomorphismus. □

Satz 6.39 (Zweiter Isomorphiesatz)**.** *Sei R ein Ring und seien $I \subseteq J \subseteq R$ Ideale.*
Dann ist J/I ein Ideal in R/I und die durch den Ringhomomorphismus $R/I \to R/J$, definiert durch $a + I \mapsto a + J$ für alle $a \in R$, induzierte Abbildung

$$(R/I)/(J/I) \xrightarrow{\sim} R/J$$

ist ein Isomorphismus. □

Übungsaufgaben zu §6

Übungsaufgabe 6.1. 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 6.2. 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 6.3. Sei R ein Ring. Berechnen Sie in $R[[X]]$ das Produkt $(1 - X) \cdot \sum_{i=0}^{\infty} X^i$.

Übungsaufgabe 6.4. 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

$$f : S \to \prod_{\alpha \in A} R_\alpha$$

mit $\mathrm{pr}_\alpha \circ f = f_\alpha$ für alle $\alpha \in A$ gilt.

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

$$\begin{aligned} i_\beta : R_\beta &\to \prod_{\alpha\in A} R_\alpha \\ x &\mapsto (0,\dots,0,\underset{\uparrow\beta}{x},0\dots,0) \end{aligned}$$

kein Ringhomomorphismus ist.

Übungsaufgabe 6.5. Zeigen Sie, daß es für jeden Ring R genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt.

Übungsaufgabe 6.6. 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 6.7. Welches sind die invertierbaren Elemente in $\mathrm{Abb}(X, R)$ und wie sieht die Gruppenstruktur auf $\mathrm{Abb}(X, R)^\times$ aus?

Übungsaufgabe 6.8. 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 6.9. 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 6.10. 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 Funktionene 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.

7. Hauptidealringe

7.1. **Integritätsringe und Hauptidealringe.** Den Körpern am nächsten kommen die Integritätsringe.

Lemma–Definition 7.1. *Ein **Integritätsring** ist ein Ring mit $1 \neq 0$, in dem die folgenden äquivalenten Bedingungen gelten.*

(a) Die Kürzungsregel gilt, d.h. für alle $a, x, y \in R$ und 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 7.2. (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 7.3 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.

Satz 7.3. *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 entsprechende Brüche: für $(a, b) \sim (c, d)$

$$\frac{a}{b} = \frac{ac}{bc} = \frac{ac}{ad} = \frac{c}{d}.$$

Die Menge der Äquivalenzklassen bezeichenen wir mit **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. Das 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

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

Die Abbildung

$$\begin{aligned} R &\to \mathrm{Quot}(R) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

ist ein Ringhomomorphismus. Dieser ist injektiv, und damit R isomorph zum Bild (Homomorphiesatz), einem Teilring im Körper $\mathrm{Quot}(R)$. □

Die nach den Körpern einfachsten Ringe sind die Hauptidealringe.

Definition 7.4. (1) Ein **Hauptideal** ist ein Ideal I in einem Ring R, das von einem Element a erzeugt werden kann:

$$I = (a) = \{ra \ ; \ r \in R\} = Ra.$$

(2) Ein **Hauptidealring** ist ein Integritätsring, in dem alle Ideale Hauptideale sind.

Beispiel 7.5. (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) 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.

Es gibt einen Dimensionsbegriff für kommutative Ringe mit dem Folgendes gilt:

- Körper sind genau die Integritätsringe von Dimension 0.
- Hauptidealringe sind Integritätsringe von Dimension 1, und zwar genau die ohne Singularitäten und ohne nicht-triviale Geradenbündel.
- Der Ring $\mathbb{Z}[X]$ hat beispielsweise die Dimension 2.

Proposition 7.6. *(1) Sei R ein Ring und $a \in R$. Dann gilt*

$$a \in R^\times \iff (a) = R.$$

(2) Sei R ein Integritätsring und $a, b \in R$. Dann gilt

$$(a) = (b)$$

genau dann, wenn es eine Einheit $\varepsilon \in R^\times$ gibt mit

$$a = \varepsilon b.$$

Beweis. (1) Für $a \in R^\times$ gilt $1 \in (a)$ und somit $R = (1) \subseteq (a) \subseteq R$.

Umgekehrt, wenn $(a) = R$, dann gilt $1 \in (a)$. Somit gibt es $b \in R$ mit $1 = ba$ und $a \in R^\times$.

(2) Sei $a = \varepsilon b$ mit ε Einheit. Dann ist wegen (1)

$$(a) = Ra = R\varepsilon b = (R\varepsilon)b = Rb = (b).$$

Sei umgekehrt $(a) = (b)$. 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. Dan muß aber wegen $b \in (a) = (0)$ auch $b = 0$ sein. Dann gilt $a = 1 \cdot b$ und 1 ist Einheit. Die Behauptung gilt also in jedem Fall. □

7.2. **Euklidische Ringe.** Wir formalisieren den Beweis, daß $\mathbb{Z}$ ein Hauptidealring ist, indem wir **Division mit Rest** abstrahieren.

Definition 7.7. 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 7.8. Die ganzen Zahlen $\mathbb{Z}$ sind ein euklidischer Ring mit der Euklidischen Gradfunktion $\delta(n) = |n|$ mit dem reellen Absolutbetrag $|\cdot|$.

Definition 7.9. Sei R ein Ring und $f \in R[X]$ ein Polynom. Wenn $f \neq 0$, dann 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.

Satz 7.10. *Sei K ein Körper.*

(1) Für alle $f, g \in K[X] \setminus \{0\}$ gilt

$$\deg(fg) = \deg(f) + \deg(g).$$

(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 $f = a_nX^n +$ Terme kleineren Grades und $g = b_mX^m +$ Terme kleiner Grades und $a_n, b_m \in K^\times$. Dann ist

$$fg = a_nb_mX^{n+m} + \text{ Terme kleineren Grades}$$

und somit $\deg(fg) = n + m$, weil $a_nb_m \neq 0$.

(2) Wenn $f \in K[X]$, 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 7.11. *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 7.10 ja $\deg(fg) = \deg(f) + \deg(g)$ gilt. Insbesonere 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 $a_n \neq 0 \neq b_m$. 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

$$\begin{aligned} q &= \tilde{q} + \frac{a_m}{a_n} X^{m-n} \\ r &= \tilde{r} \end{aligned}$$

und rechnen

$$f = \tilde{f} + \frac{a_m}{a_n} X^{m-n} d = \tilde{q}d + \tilde{r} + \frac{a_m}{a_n} X^{m-n} d = (\tilde{q} + \frac{a_m}{a_n} X^{m-n})d + \tilde{r} = qd + r.$$

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 7.12. *Ein euklidischer 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 7.13. *Der Polynomring $K[X]$ mit Koeffizienten aus einem Körper K ist ein Hauptidealring.*

Beweis. Dies folgt aus Theorem 7.12, da nach Satz 7.11 der Polynomring euklidisch ist. □

Wir beenden diesen Abschnitt mit zwei weiteren Beispielen.

Beispiel 7.14. 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 Normfunktion dient

$$\delta(a + bi) = a^2 + b^2.$$

Beispiel 7.15. Sei R ein euklidischer Ring mit euklidischer Gradfunktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$. Sei n_0 der kleinste Werte 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

$$|R^\times| + 1 \geq |R/(x)|. \tag{7.1}$$

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 (7.1) 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.

7.3. **Das Minimalpolynom.**

Bemerkung 7.16. Sei K ein Körper und $I \subseteq K[X]$ ein Ideal $I \neq (0)$. Dann gibt es ein eindeutiges normiertes Polynom $f \in K[X]$ mit

$$I = (f).$$

Zum einen ist I ein Hauptideal und damit von einem Polynom F erzeugt. Sei F vom Grad n und $F = a_n X^n + \ldots + a_0$. Mit Proposition 7.6 dürfen wir F durch das normierte Polynom

$$f = a_n^{-1} F = X^n + \frac{a_{n-1}}{a_n} X^{n-1} + \ldots + \frac{a_0}{a_n}$$

ersetzen. Dieses f ist eindeutig, denn wieder nach Proposition 7.6 kann man f nur um eine Einheit ε von $K[X]$ abändern. Nun ist $K[X]^\times = K^\times$ und somit der führende Koeffizient von εf gerade ε. Es gibt also nur für $\varepsilon = 1$ einen normierten Erzeuger von I.

Definition 7.17. Sei K ein Körper. Das **Minimalpolynom** einer Matrix $A \in \mathrm{M}_n(K)$ ist das eindeutige normierte Polynom

$$m_A(X) \in K[X]$$

welches den Kern der Auswertung $\mathrm{ev}_A : K[X] \to \mathrm{M}_n(K)$ erzeugt.

Hier ist zu überlegen, daß $\ker(\mathrm{ev}_A) \neq (0)$. Die Auswertung ev_A ist insbesondere eine K-lineare Abbildung. Da $\dim_K \mathrm{M}_n(K) = n^2$ endlich ist, aber $\dim_K K[X] = \infty$ unendlich, kann diese lineare Abbildung nicht injektiv sein.

Jedes Polynom $P(X) \in K[X]$ mit $P(A) = 0$ ist also von der Form $P(X) = Q(X) \cdot m_A(X)$ für ein Polynom $Q(X) \in K[X]$.

Bemerkung 7.18. Man vergleiche diese Definition des Minimalpolynoms mit derjenigen aus der Vorlesung Lineare Algebra 1. Dort wurde $m_A(X)$ als das normierte Polynom P kleinsten Grades definiert mit der Eigenschaft $P(A) = 0$. Dies erinnert an den Beweis, daß euklidische Ringe Hauptideale sind, genauer daran, wie man den Erzeuger des Ideals $\ker(\mathrm{ev}_A)$ im Beweis von Theorem 7.12 bestimmt.

Definition 7.19. Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Das **Minimalpolynom** eines Endomorphismus $f : V \to V$ ist das eindeutige normierte Polynom

$$m_f(X) \in K[X]$$

welches den Kern der Auswertung $\mathrm{ev}_f : K[X] \to \mathrm{End}_K(V)$ erzeugt.

Hier ist dieselbe Überlegung anzustellen wie oben. Wir überlegen uns lieber das folgende. Jedes Polynom $P(X) \in K[X]$ mit $P(f) = 0$ ist also von der Form $P(X) = Q(X) \cdot m_f(X)$ für ein Polynom $Q(X) \in K[X]$.

Proposition 7.20. *Sei $f \in \mathrm{End}_K(V)$ mit Matrix $A = \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(f)$ bezüglich der Basis $\mathscr{B}$. Dann gilt*

$$m_f(X) = m_A(X).$$

Insbesondere gilt für jede Matrix $S \in \mathrm{GL}_n(K)$

$$m_{SAS^{-1}}(X) = m_A(X).$$

Beweis. Der Koordinatenisomorphismus für Endomorphismen

$$\mathrm{M}_{\mathscr{B}}^{\mathscr{B}} : \mathrm{End}_K(V) \to \mathrm{M}_n(K)$$

ist sogar ein Ringisomorphismus. Es gilt $\mathrm{ev}_A = \mathrm{M}_{\mathscr{B}}^{\mathscr{B}} \circ \mathrm{ev}_f$. Dies folgt aus der universellen Eigenschaft für den Polynomring aus Satz 6.25, wonach wir nur zeigen müssen, daß beide Abbildungen auf den Koeffizienten K und der Variablen X übereinstimmen. Das ist aber klar.

Damit gilt für alle $P(X) \in K[X]$, daß $P(A) = 0 \iff P(f) = 0$. Somit stimmen die Kerne $\ker(\mathrm{ev}_f) = \ker(\mathrm{ev}_A)$ überein, und deshalb auch die normierten Erzeuger.

Die Matrix SAS^{-1} beschreibt auch den Endomorphismus f, nur bezüglich einer anderen Basis. Die Gleichung

$$m_{SAS^{-1}}(X) = m_f(X) = m_A(X).$$

folgt durch zweimaliges Anwenden des zuerst bewiesenen. □

7.4. **Primideale und maximale Ideale.** Wir beschreiben nun spezielle Klassen von Idealen.

Definition 7.21. Ein **maximales Ideal** ist ein Ideal $\mathfrak{m}$ eines Rings R mit $\mathfrak{m} \neq R$, das maximal bezüglich Inklusion unter allen von R verschiedenen Idealen von R ist: es gibt kein Ideal I mit

$$\mathfrak{m} \subseteq I \subseteq R$$

und $I \neq \mathfrak{m}$ und $I \neq R$.

Proposition 7.22. *Sei $f : R \to S$ ein surjektiver Ringhomomrphismus. Dann definiert*

$$I \mapsto f^{-1}(I)$$

eine Bijektion von der Menge der Ideale von S mit den Idealen von R, die $\ker(f)$ enthalten.

Beweis. Man überlegt sich leicht, daß $f^{-1}(I)$ ein Ideal ist, etwa als Kern der Komposition

$$R \xrightarrow{f} S \to S/I,$$

das $\ker(f)$ enthält. Die Inverse Abbildung ist $J \mapsto f(J)$. Nach Homomorphiesatz und zweitem Isomorphiesatz ist $f(J)$ gerade der Kern der Abbildung

$$S \simeq R/\ker(f) \to (R/\ker(f))/(J/\ker(f)).$$

Also ist $f(J)$ tatsächlich ein Ideal. Weil $\ker(f) \subseteq J$ ist, gilt

$$J = f^{-1}(f(J))$$

und weil f surjektiv ist, gilt

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

Die angegebenen Abbildungen sind also invers zueinander. □

Wir leiten ein Kriterium für maximale Ideale ab, das oft benutzt wird, um maximale Ideale als solche zu erkennen.

Satz 7.23. *Ein Ring ist genau dann ein Körper, wenn er keine echten Ideale hat und* $1 \neq 0$.

Beweis. Sei $I \subseteq K$ ein Ideal in einem Körper K mit $I \neq (0)$. Dann gibt es ein $0 \neq x \in I$ und damit ist jedes $y \in K$ schon wegen $y = yx^{-1} \cdot x \in I$, also $I = K$.

Sei umgekehrt R ein Ring, der keine echten Ideale hat. Dann ist für alle $0 \neq x \in R$ das Hauptideal $(x) = R$. Damit ist x eine Einheit und in R sind alle von 0 verschiedenen Elemente invertierbar. Damit ist R ein Körper, denn $0 \neq 1$. □

Korollar 7.24. *Sei I ein Ideal im Ring R. Der Faktorring R/I ist ein Körper genau dann, wenn I ein maximales Ideal in R ist.*

Beweis. Nach Satz 7.23 ist R/I ein Körper genau dann, wenn $0 \neq 1$ und es keine echten Ideale in R/I gibt, also wenn R/I genau die zwei verschiedenen Ideale $(0) \neq (1)$ hat. Wir betrachten nun die Quotientenabbildung

$$p : R \to R/I.$$

Nach Proposition 7.22 sind die Ideale von R/I mittels $J \mapsto p^{-1}(J)$ in Bijektion mit den Idealen von R, die I enhalten. Es enthält also R/I genau zwei Ideale, wenn

$$\{J \ ; \ J \text{ Ideal in } R \text{ mit } I \subseteq J \subseteq R\}$$

nur aus den verschiedenen Idealen $I = p^{-1}((0))$ und $R = p^{-1}((1))$ besteht, also wenn I ein maximales Ideal ist. □

Beispiel 7.25. (1) Sei K ein Körper. Das Ideal (X) in $K[X]$ ist der Kern des Auswertungshomomorphismus $f \mapsto f(0)$:

$$\mathrm{ev}_0 : K[X] \to K.$$

In der Tat, für $f = a_0 + a_1X + \ldots a_nX^n$ haben wir $f(0) = a_0$ und f liegt im Kern, wenn

$$f = X \cdot (a_1 + a_2X + \ldots + a_nX^{n-1}) \in (X).$$

Die Auswertung ist klar surjektiv, also nach dem Homomorphiesatz $K[X]/(X) \simeq K$ und (X) ist ein maximales Ideal.

(2) Sei K ein Körper und $\alpha \in K$. Polynomdivision von $f \in K[X]$ mit $X - \alpha$ führt zu $d, r \in K[X]$ mit r konstant, so daß

$$f = d(X - \alpha) + r.$$

Wegen $f(\alpha) = d(\alpha)(\alpha - \alpha) + r(\alpha) = r$ gilt $f(\alpha) = 0$ genau dann, wenn $r = 0$. Also ist $f \in \ker(\mathrm{ev}_\alpha)$ genau dann, wenn $f = d(X - \alpha)$, somit

$$\ker(\mathrm{ev}_\alpha) = (X - \alpha).$$

Die Auswertung ist surjektiv (wegen der konstanten Polynoma), also nach dem Homomorphiesatz $K[X]/(X - \alpha) \simeq K$ und $(X - \alpha)$ ist ein maximales Ideal.

(3) Das Ideal $(2, X) \subseteq \mathbb{Z}[X]$ ist maximales Ideal, denn der Faktorring $\mathbb{Z}[X]/(2, X)$ ist isomorph zum Körper $\mathbb{F}_2$.

Das folgende Resultat nutzt das Auswahlaxiom, bzw. das dazu logisch äquivalente Zorn'sche Lemma.

Theorem 7.26. *Jedes Ideal $I \neq R$ eines Rings R ist in einem maximalen Ideal $\mathfrak{m} \subseteq R$ enthalten.*

Beweis. Die Menge

$$\mathscr{X} = \{J \subsetneq R \,;\; I \subseteq J, \text{ und } J \text{ ist eine Ideal}\}$$

ist bezüglich der partiellen Ordnung $\subseteq$ induktiv geordnet. Für eine aufsteigende Kette in $\mathscr{X}$

$$I \subseteq J_1 \subseteq J_2 \subseteq \ldots \subseteq J_n \subseteq \ldots$$

von Idealen $\neq R$, ist

$$J_\infty = \bigcup_n J_n$$

eine obere Schranke in $\mathscr{X}$. Es ist auch ein Ideal, und immer noch $\neq R$. Andernfalls wäre $1 \notin J_\infty$, und damit $1 \in J_n$ für ein hinreichend großes n und dann $J_n = R$. Das Lemma von Zorn garantiert nun die Existenz eines maximalen Elements in $\mathscr{X}$. Dies ist ein maximales Ideal von R, das per Konstruktion I enthält. □

Primideale sind genau die Ideale die zu besonders angenehmen Faktorringen führen.

Definition 7.27. Ein **Primideal** ist ein Ideal $I \subsetneq R$ eines Rings R, so daß für alle $a, b \in R$ gilt:

$$ab \in I \Longrightarrow a \in I \text{ oder } b \in I.$$

Satz 7.28. *Ein Ideal $I \subseteq R$ ist ein Primideal genau dann, wenn R/I ein Integritätsring ist.*

Beweis. Zunächst ist $I \neq R$ äquivalent zu $0 \neq 1$ in R/I. Sodann ist R/I nullteilerfrei, wenn für alle $a, b \in R$ aus $ab + I = (a + I)(b + I) = 0 \in R/I$, d.h. $ab \in I$, schon $a + I = 0$ oder $b + I = 0$ in R/I, d.h. $a \in I$ oder $b \in I$, also genau dann, wenn I ein Primideal ist. □

Korollar 7.29. *Ein maximales Ideal ist ein Primideal.*

Beweis. Ist $\mathfrak{m}$ maximales Ideal in R, dann ist $R/\mathfrak{m}$ ein Körper und damit Integritätsring. Also ist $\mathfrak{m}$ ein Primideal. □

Beispiel 7.30. Maximale Ideale sind Primideale aber nicht umgekehrt:

(1) Das Ideal $(0) \subseteq \mathbb{Z}$ ist ein Primideal, denn $\mathbb{Z} = \mathbb{Z}/(0)$ ist ein Integritätsring, aber (0) ist nicht maximal, denn z.B. $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.

(2) Das Ideal $(X) \subseteq \mathbb{Z}[X]$ ist ein Primideal, denn $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$, induziert vom Auswertungshomomorphismus $X \mapsto 0$. Aber (X) ist kein maximales Ideal, denn $(X) \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$.

In beiden Fällen ist der Faktorring $\mathbb{Z}$ kein Körper, also das Ideal nicht maximal.

Übungsaufgaben zu §7

Übungsaufgabe 7.1. Sei R ein Integritätsring. Bestimmen sie die Einheitengruppe im Polynomring $R[X]$ und im Potenzreihenring $R[[X]]$.

Übungsaufgabe 7.2. Sei K ein Körper. Zeigen Sie, daß $K[[X]]$ ein Hauptidealring ist. Gibt es eine euklidische Gradfunktion auf $K[[X]]$?

Übungsaufgabe 7.3. Wir betrachten den Unterring $R \subseteq K[[X]]$ aus Aufgabe 6.6 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.

8. Arithmetik in Hauptidealringen

8.1. Teilbarkeit in Integritätsringen.

Definition 8.1. 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:

(a) Es gibt ein $y \in R$ mit $a = xy$.

(b) $a \in (x)$.

(c) $(a) \subseteq (x)$.

Ansonsten schreiben wir $x \nmid a$, wenn x kein Teiler von a ist.

Beispiel 8.2. Sei $A \in \mathrm{M}_n(K)$ und $P(X) \in K[X]$ mit $P(A) = 0$. Dann ist das Minimalpolynom $m_A(X)$ von A ein Teiler von $P(X)$. Analoges gilt für einen Endomorphismus $f \in \mathrm{End}_K(V)$ bezüglich des Minimalpolynoms von f.

Satz 8.3. *Das Minimalpolynom einer quadratischen Matrix A (bzw. eines Vektorraum-Endomorphismus f) teilt das charakteristische Polynom von A (bzw. von f):*

$$m_A(X) \mid P_A(X) \quad (\text{bzw. } m_f(X) \mid P_f(X)\ ).$$

Beweis. Die Aussage ist äquivalent zum Satz von Cayley–Hamilton. Wegen $P_A(A) = 0$ gilt

$$P_A(X) \in \ker(\mathrm{ev}_A) = (m_A(X)).$$

Analog (oder weil beide Polynome nur von einer darstellenden Basis abhängen) zeigt man die Aussage für Endomorphismen. □

Proposition 8.4 (Eigenschaften der Teilerrelation)**.** *Sei R ein Integritätsring und $a, b, c \in R$ beliebig. Dann gilt:*

(1) $1 \mid a$.
(2) $a \mid 0$.
(3) $a \mid 1 \iff a \in R^\times$.
(4) *Wenn $a \mid b$, dann gilt $ac \mid bc$.*
(5) $a \mid b$ *und* $b \mid c \Longrightarrow a \mid c$.
(6) *Seien $a_1, \dots a_n$ Elemente von R. Dann folgt aus $x \mid a_i$ für alle i, daß für alle $b_i \in R$, für $1 \le i \le n$ auch*

$$x \mid b_1a_1 + \dots b_na_n.$$

(7) $(a \mid b$ *und* $b \mid a) \iff (a) = (b) \iff \exists u \in R^\times : a = ub$. *Man sagt dann a und b seien* ***assoziiert*** *und schreibt $a \sim b$.*

Beweis. Aussagen (1)-(5) folgen unmittelbar aus der Definition der Teilbarkeit und bleiben zur Übung. Wir zeigen (6) und (7).

(6) Es gibt y_i mit $a_i = xy_i$ für alle $1 \le i \le r$. Dann gilt

$$x \mid x(b_1y_1 + \dots + b_nx_n) = b_1a_1 + \dots + b_na_n.$$

(7) Es teilt $a \mid b$ und $b \mid a$ genau dann, wenn $(b) \subseteq (a)$ und $(a) \subseteq (b)$, was äquivalent ist zu $(a) = (b)$. Dies ist nach Proposition 7.6 dasselbe wie $a = ub$ für eine Einheit $u \in R^\times$. □

8.2. **Der ggT und das kgV.** In Hauptidealringen kann man größte gemeinsame Teiler und kleinste gemeinsame Vielfache definieren.

Definition 8.5. Sei R ein Hauptidealring.

(1) Der **größte gemeinsame Teiler (ggT)** der Elemente $a_1, \dots, a_r \in R$ ist das bis auf Multiplikation mit einer Einheit bestimmtes Element $d \in R$ mit

$$(d) = (a_1, \dots, a_r).$$

(2) Das **kleinste gemeinsame Vielfache (kgV)** der Elemente $a_1, \dots, a_r \in R$ ist ein bis auf Multiplikation mit einer Einheit bestimmtes Element $v \in R$ mit

$$(v) = \bigcap_{i=1}^{r} (a_i).$$

Bemerkung 8.6. Der ggT und das kgV sind eigentlich als Ideale definiert. Der Übergang zu Elementen führt zu Unbestimmtheit bis auf eine Einheit, siehe Proposition 7.6.

Bemerkung 8.7. Der ggT ist ein gemeinsamer Teiler, und jeder andere gemeinsame Teiler teilt den ggT, somit ist dieser der größte solche. Wenn $t \in R$ ein Teiler von a_i für alle $1 \le i \le r$ ist, etwa $a_i = b_it$, dann gilt für alle $x_i \in R$

$$t \mid (x_1b_1 + \dots + x_rb_r)t = x_1a_1 + \dots + x_ra_r.$$

Dies gilt insbesondere für den ggT $d \in (a_1, \dots, a_r)$, somit

$$t \mid a_i \text{ für alle i } \Longrightarrow t \mid d.$$

Andererseits gilt

$$a_i \in (a_1, \ldots, a_r) = (d)$$

und damit $d \mid a_i$ für alle $1 \leq i \leq r$. Der ggT ist insbesondere ein gemeinsamer Teiler der a_i.

Analog überlegt man sich, daß das kgV das Kleinste unter den gemeinsame Vielfachen ist.

Satz 8.8 (Satz von Bézout)**.** *Sei R ein Hauptidealring und d der ggT der Elemente $a_1, \ldots, a_r$. 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 Definition des ggT klar. □

Definition 8.9. Sei R ein Hauptidealring. Elemente $a_1, \ldots, a_r \in R$ heißen **teilerfremd**, wenn ihr ggT eine Einheit ist, also

$$(1) = (a_1, \ldots, a_r).$$

Korollar 8.10. *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 $1 \leq i \leq r$. □

8.3. **Der euklidische Algorithmus in euklidischen Ringen.** Sei R ein Hauptidealring und d der ggT von $a, b \in R$. Es ist besonders interessant, den ggT von a, b als R-Linearkombination

$$d = \alpha a + \beta b$$

algorithmisch zu bestimmen. 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.

Sei δ eine euklidische Gradfunktion auf R. Wir setzen als Startwert $x_0 = a$ und $y_0 = b$ mit oBdA $\delta(x_0) \geq \delta(y_0)$ oder $y_0 = 0$. Angenommen, wir haben bereits x_i, y_i konstruiert mit

$$\delta(x_i) \geq \delta(y_i) \quad \text{oder} \quad y_i = 0. \tag{$\star$}$$

Falls $y_i = 0$, so halten wir den Algorithmus an und setzen

$$d = x_i.$$

Andernfalls bestimmen wir q_i, r_i mit

$$x_i = q_i y_i + r_i$$

und $r_i = 0$ oder $\delta(y_i) > \delta(r_i)$. Wir setzen

$$A_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$$

und

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} := A_i \begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} y_i \\ r_i \end{pmatrix}.$$

Damit ist gewährleistet, daß weiter ($\star$) gilt. Der Algorithmus terminiert (endet nach endlich vielen Schritten), denn $\delta(y_n)$ ist als Funktion von n wegen

$$\delta(y_i) > \delta(r_i) = \delta(y_{i+1})$$

für alle i ist streng monoton fallend, hat aber nur endlich viele Werte zur Verfügung: die ganzen Zahlen im Intervall $[0, \delta(y_0)]$. Für hinreichend großes n muß also $y_n = 0$ sein. Dann ist d der ggT von a, b, denn es gilt für alle $0 \leq i < n$

$$(x_i, y_i) = (q_i y_i + r_i, y_i) = (r_i, y_i) = (x_{i+1}, y_{i+1})$$

und so per Induktion

$$(a, b) = (x_0, y_0) = \ldots = (x_n, y_n) = (d, 0) = (d).$$

Die Koeffizienten in der R-Linearkombination, die den ggT darstellt, kann man nebenher wie folgt berechnen. Wir setzen für $1 \leq i \leq n$

$$B_i = \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix} := A_{i-1}A_{i-2}\dots A_0$$

und $B_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. In jedem Schritt berechnen wir auch

$$B_{i+1} = A_i B_i.$$

Dann gilt (per Induktion)

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = B_i \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

und als erste Zeile für $i = n$

$$d = \alpha_n x_0 + \beta_n y_0.$$

Bemerkung 8.11. Hat man den ggT von mehr als zwei Elementen in einem euklidischen Ring zu bestimmen, etwa $a_1, \dots, a_r \in R$, dann bestimmt man zunächst mit dem euklidischen Algorithmus

$$(d_1) = (a_1, a_2),$$

nutzt dann

$$(a_1, a_2, a_3, \dots, a_r) = (d_1, a_3, \dots, a_r)$$

und hat das Problem auf dasselbe mit einem Element weniger zurückgeführt. Dieses Vorgehen iteriert man, bis nur noch der ggT übrig bleibt.

8.4. **Primelemente und irreduzible Elemente.**

Definition 8.12. Ein Element $a \neq 0$ eines Rings R heißt **irreduzibel**, wenn a keine Einheit ist und aus $a = xy$ folgt, daß x oder y eine Einheit ist.

Beispiel 8.13. (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 $\deg(q) = \deg(f) - \deg(X - \lambda) > 0$ zeigt, daß $q \notin K[X]^\times$.

Definition 8.14. 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**.

Proposition 8.15. *Sei R ein Integritätsring. Dann ist jedes Primelement irreduzibel.*

Beweis. Sei a ein Primelement und $a = xy$ eine beliebige Zerlegung. Dann gilt $a \mid xy$ und oBdA $a \mid x$. Es gibt also $z \in R$ mit $az = x$. Dann ist $azy = xy = a = a \cdot 1$ und Kürzen mit a zeigt $zy = 1$. Damit ist y eine Einheit. Da dies für jede Zerlegung $a = xy$ gilt, ist a irreduzibel. □

Der folgende Satz und der Fall der Primelemente in $\mathbb{Z}$, nämlich der Primzahlen, rechtfertigt den Namen Primelement.

Satz 8.16. *Sei $0 \neq a \in R$ ein Element eines Hauptidealrings R und keine Einheit. Dann sind äquivalent:*

(i) a *ist Primelement.*
(ii) a *ist irreduzible.*
(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 8.15, und (iii) $\Longrightarrow$ (iv) ist trivial.

(ii) $\Longrightarrow$ (iii): 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 (a, x) ist 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 und c eine Einheit sein. Wenn $c \in R^\times$, dann gibt es einen Widerspruch durch

$$(b) = (ac) = (a) \subsetneq (a, x) = (b).$$

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 8.17. Hier ist ein direktes Argument für (ii) $\Longrightarrow$ (i) in Satz 8.16:
Sei a irreduzibel und $a \mid xy$. Betrachten wir die Menge

$$(a : x) := \{z \in R \,;\; zx \in (a)\} \subseteq R.$$

Dann ist $(a : x)$ ein Ideal in R, denn mit $z, z_1, z_2 \in (a : x)$ und $r \in R$ gilt

$$(z_1 + z_2)x = z_1x + z_2x \in (a),$$

$$(rz)x = r(zx) \in r(a) \subseteq (a),$$

daher gilt $z_1 + z_2, rz \in (a : x)$. Da R ein Hauptidealring ist, gibt es ein $b \in R$ mit

$$(b) = (a : x).$$

Es gilt $a \in (a : x)$. Damit gibt es $c \in R$ mit $a = bc$. Da a irreduzible ist, gibt es nun zwei Fälle.

Fall 1: $b \in R^\times$. Dann ist $(a : x) = (b) = R$ und wegen $1 \in (a : x)$ muß $x \in (a)$ gelten. Das bedeutet $a \mid x$.

Fall 2: $c \in R^\times$. Weil $a \mid xy$, also $xy \in (a)$, gilt $y \in (a : x) = (b) = (a)$. Das bedeutet $a \mid y$.

Proposition 8.18. *Sei R ein Integritätsring und $a \in R$. Dann ist a irreduzibel genau dann, wenn (a) maximal bezüglich Inklusion unter den echten Hauptidealen ist.*

Beweis. Sei a irreduzibel und $(a) \subseteq (x) \subsetneq R$. Dann ist $a \in (x)$, also gibt es y mit $a = xy$. Da a irreduzibel ist, muß x oder y Einheit sein. Da $(x) \neq R$ kann x keine Einheit sein. Somit ist y Einheit und

$$(a) = Ra = Ryx = (Ry)x = Rx = (x).$$

Daher ist (a) maximal unter den echten Hauptidealen.

Umgekehrt sei (a) maximal unter den echten Hauptidealen. Sei $a = xy$ eine beliebige Faktorisierung. Wir müssen zeigen, daß x oder y eine Einheit ist. Wegen

$$(a) = Ra = (Rx)y \subseteq Ry = (y)$$

folgt entweder $(y) = R$, und damit ist y Einheit und wir sind fertig, oder $(y) = (a)$. In diesem Fall gibt es auch ein $b \in R$ mit $y = ab$. Dann ist $a = xy = x(ab) = a(xb)$. Aus der Kürzungsregel foglt nun $1 = xb$ und x ist Einheit. Damit sind wir auch fertig. □

Bemerkung 8.19. (1) Konzeptionell kann man Primelement auch definieren als Elemente a, so daß (a) ein Primideal ist. Das folgt unmittelbar aus der Definition.

(2) Hier ist ein alternativer Beweis von Satz 8.16, der konzeptionell mit maximalen Idealen und Primidealen arbeitet.

Sei $a \in R$ ein irreduzibles Element im Hauptidealring R. Nach Proposition 8.18 ist (a) maximal unter den echten Hauptidealen. In einem Hauptidealring gibt es nur Hauptideale, so daß hier genauer (a) ein maximales echtes Ideal ist und äquivalent dazu $R/(a)$ ein Körper ist. Maximale Ideale sind Primideale, somit ist a ein Primelement.

Die Richtung (i) $\Longrightarrow$ (ii) wurde in Proposition 8.15 bereits allgemeiner gezeigt.

Korollar 8.20. *In einem Hauptidealring R ist jedes von (0) verschiedene Primideal ein maximales Ideal.*

Beweis. In einem Hauptidealring wird jedes Primideal $\mathfrak{p} \neq (0)$ von einem Primelement $\pi \in R$ erzeugt. Nach Satz 8.16 ist π auch irreduzibel und genauer $\mathfrak{p} = (\pi)$ ein maximales Ideal. □

Bemerkung 8.21. Im Allgemeinen ist die Umkehrung von Proposition 8.15 falsch. Für ein Beispiel betrachten wir den Unterring

$$R = \mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10}\ ;\ a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

und darin das Element $1 + \sqrt{10}$. Da $\sqrt{10}$ irrational ist, sind die Koeffizienten $a, b \in \mathbb{Z}$ für jedes $a + b\sqrt{10} \in R$ eindeutig.

Das Element $1 + \sqrt{10}$ ist nicht prim, denn

$$(1 + \sqrt{10})(\sqrt{10} - 1) = 9 = 3 \cdot 3,$$

aber

$$1 + \sqrt{10} \nmid 3,$$

weil aus $a, b \in \mathbb{Z}$ mit $(1 + \sqrt{10})(a + \sqrt{10}b) = 3$ durch Koeffizientenvergleich folgt

$$0 = a + b$$
$$3 = a + 10b$$

oder $b = -a = 1/3 \notin \mathbb{Z}$, Widerspruch.

Andererseits ist $1 + \sqrt{10}$ irreduzibel in R. Wir zeigen, daß es keine Faktorisierung

$$1 + \sqrt{10} = (a + b\sqrt{10})(u + v\sqrt{10}) \tag{8.1}$$

mit $a, b, u, v \in \mathbb{Z}$ gibt, in der kein Faktor eine Einheit ist. Die Faktorisierung bedeutet

$$1 = au + 10bv$$
$$1 = av + bu$$

woraus ebenso

$$1 - \sqrt{10} = (a - b\sqrt{10})(u - v\sqrt{10}) \tag{8.2}$$

folgt. Multiplizieren wir entsprechende Terme von (8.1) und (8.2), so erhalten wir

$$-9 = (a^2 - 10b^2)(u^2 - 10v^2). \tag{8.3}$$

Da weder $a + b\sqrt{10}$ noch $u + v\sqrt{10}$ Einheiten sind, dürfen die Faktoren in (8.3) nicht ± 1 sein. Daher muß einer der Faktoren 3 und der andere -3 sein, oBdA

$$a^2 - 10b^2 = 3.$$

Dies führt zum Widerspruch zur Liste der Quadrate modulo 10, denn $3 = a^2 - 10b^2 \equiv a^2$ modulo 10 kommt nicht in der Liste

x mod 10	0	± 1	± 2	± 3	± 4	5
x^2 mod 10	0	1	4	9	6	5

vor.

Korollar 8.22. *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 8.16 und der Definition einer Primzahl. □

Bemerkung 8.23. Wir brauchen Satz 8.16 im Beweis von Satz 8.22, weil wir mit der traditionellen Definition einer Primzahl arbeiten, anstatt von Primelementen in $\mathbb{Z}$ zu sprechen. Beides ist äquivalent, erfordert aber den Satz 8.16.

Notation 8.24. Für eine Primzahl p bezeichenen 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.

8.5. **Die Eindeutigkeit der Primzerlegung in Hauptidealringen.** Der Satz über die Eindeutigkeit der Primfaktorzerlegung ist schon sehr alt, aber keineswegs trivial. In Hauptidealringen gilt der Satz allgemein. Nicht aber in beliebigen Ringen als Satz über eindeutige Faktorisierung in irreduzible Elemente, wie das klassische Beispiel in

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \ ; \ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

mit den zwei echt verschiedenen Faktorisierungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

zeigt[12].

Satz 8.25. *Sei R ein Hauptidealring. Dann läßt sich jedes $0 \neq a \in R$, als Produkt einer Einheit und endlich vieler Primelemente schreiben.*

Beweis. Wir betrachten die Menge der Hauptideale, die von einem Gegenbeispiel erzeugt werden:

$$\mathscr{M} = \{(x) \ ; \ x \in R, x \neq 0 \text{ und } x \text{ hat nicht die Form } x = u \cdot \prod_{i=1}^{n} p_i \text{ mit } u \in R^\times, \ p_i \text{ prim in } R\},$$

und zeigen, daß sie leer ist. Die Menge $\mathscr{M}$ ist wohldefiniert, denn verschiedene Erzeuger von (x) unterscheiden sich nur um eine Einheit und diese kann in einer Produktzerlegung einem Faktor zugeschlagen werden. Die Bedingung, daß sich der Erzeuger x nicht als Produkt endlich vieler Primelemente von R schreiben läßt gilt also für einen Erzeuger genau dann, wenn es für jeden Erzeuger gilt.

Angenommen, es gibt kein bezüglich Inklusion in $\mathscr{M}$ 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 $i \geq 1$. Eine leichte Überlegung zeigt, daß

$$I = \bigcup_{i \geq 1} (x_i)$$

auch ein Ideal in R ist. Da R Hauptidealring ist, gibt es $x \in R$ mit $I = (x)$. Für hinreichend großes j muß schon $x \in (x_j)$ gelten, woraus für alle $j \leq i$

$$I = (x) \subseteq (x_j) \subsetneq (x_i) \subseteq I$$

ein Widerspruch folgt. Es gibt also maximale Gegenbeispiele.

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 nach Satz 8.16 sind irreduzible Elemente prim und a wäre ein Produkt (mit nur einem Faktor) von Primelementen. 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. Entsprechend ist $(a) \subsetneq (y)$ eine echte Inklusion. Da (a) maximal in $\mathscr{M}$ gewählt wurde, sind $(x), (y) \notin \mathscr{M}$. Es gibt daher eine Zerlegung

$$x = u \cdot p_1 \cdot \ldots \cdot p_n$$
$$y = v \cdot q_1 \cdot \ldots \cdot q_m$$

[12]Hier ist natürlich noch einiges zu zeigen, daß die Elemente 2, 3 und $1 \pm \sqrt{-5}$ irreduzibel sind.

für Primelemente $p_1, \ldots, p_n, q_1, \ldots, q_m$ 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 8.26. Im Polynomring $K[X]$ kann man Satz 8.25 leicht per Induktion über den Grad beweisen. Für $\deg(f) = 0$ handelt es sich um 0 oder eine Einheit. Für $\deg(f) > 0$ ist entweder f irreduzibel, dann ist nach Satz 8.16 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 7.10 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 multiplizieren zu einer Faktorzerlegung von f.

Bemerkung 8.27. Ist p ein Primelement und u eine Einheit. Dann ist auch $q = up$ ein Primelement, denn $(p) = (q)$ und damit für alle $x \in R$

$$p \mid x \iff q \mid x.$$

Theorem 8.28 (Eindeutige Primfaktorzerlegung in Hauptidealringen)**.** *Sei R ein Hauptidealring und $a \in R$, $a \neq 0$. Dann ist die Zerlegung*

$$a = u \cdot p_1 \cdot \ldots \cdot p_n$$

in Primelemente p_i für $1 \leq i \leq n$ und eine Einheit u 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. Wir zeigen die Behauptung 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 $n = 0$. 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[13] 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 8.16, 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. □

[13] 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.

Die Primfaktorzerlegung erlaubt es, den ggT und das kgV auszudrücken.

Korollar 8.29. *Seien $p_i \in R$ für $1 \leq i \leq n$ paarweise verschiedene Primelemente eines Hauptisdealrings R.*

(1) Sei mit $u \in R^\times$

$$a = u \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$$

und $b \mid a$. Dann gibt es $0 \leq f_n \leq e_n$ und $v \in R^\times$ mit

$$b = v \cdot p_1^{f_1} \cdot \ldots \cdot p_n^{f_n}.$$

(2) Sei $u_j \in R^\times$ und

$$a_j = u_j \cdot \prod_{i=1}^{n} p_i^{e_{ij}}$$

mit $e_{ij} \in \mathbb{N}_0$ für alle $1 \leq i \leq n$ und $1 \leq j \leq r$. Sei

$$m_i = \min_{1 \leq j \leq r} \{e_{ij}\}$$

und

$$M_i = \max_{1 \leq j \leq r} \{e_{ij}\}.$$

Dann ist der ggT d von $a_1, \ldots, a_r$ gegeben durch

$$d = \prod_{i=1}^{n} p_i^{m_i}$$

und das kgV D von $a_1, \ldots, a_r$ gegeben durch

$$D = \prod_{i=1}^{n} p_i^{M_i}.$$

Beweis. (1) Wir schreiben $a = bc$. Die Primfaktorzerlegung von b und c legt nun wegen der Eindeutigkeit die von a fest: man multipliziere beide Zerlegungen. Aussage (2) folgt sofort aus Aussage (1). □

8.6. **Das Minimalpolynom und Teilbarkeit.** Nach Satz 8.3 bestimmt man für das Minimalpolynom einer Matrix A am besten zuerst das charakteristische Polynom von A. Das geht algorithmisch als Determinante

$$P_A(X) = \det(X \cdot E - A).$$

Sodann zerlegt man $P_A(X)$ in irreduzible normierte Faktoren (das ist im Allgemeinen schwierig)

$$P_A(X) = \lambda \prod_{i=1}^{r} p_i(X)^{n_i} \tag{8.4}$$

(mit $p_i(X)$ paarweise verschieden). Aufgrund der eindeutigen Primfaktorzerlegung in $K[X]$, siehe Theorem 8.28, muß $m_A(X)$ ein Produkt der Form

$$m_A(X) = \prod_{i=1}^{r} p_i(X)^{e_i} \tag{8.5}$$

mit $e_i \leq n_i$ sein. Analog geht man für einen Endomorphismus $f : V \to V$ vor. Wir zeigen nun, daß jeder irreduzible Faktor von $P_f(X)$ (und damit $P_A(X)$) auch in $m_f(X)$ (und damit $m_A(X)$) auftritt.

Beispiel 8.30. (1) Das Minimalpolynom von $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ist X^2, denn $A^2 = 0$, somit ist $m_A(X)$ ein Teiler von X^2, aber $A \neq 0$, also $X \notin \ker(\mathrm{ev}_A)$.

(2) Sei $0 \neq a \in K$. Das Minimalpolynom von $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ ist $m_A(X) = (X-1)^2$, denn $A - 1 = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ und somit wie im ersten Beispiel $(A-1)^2 = 0$. Damit teilt $m_A(X)$ das Polynom $(X-1)^2$, aber $A - 1 \neq 0$, also $X - 1 \notin \ker(\mathrm{ev}_A)$.

(3) Sei $a \neq b \in K$. Das Minimalpolynom von $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ ist $(X-a)(X-b)$.

In jedem dieser Beispiele ist das Minimalpolynom $m_A(X) = P_A(X)$ gleich dem charakteristischen Polynom. Das gilt oft, aber nicht immer.

Beispiel 8.31. Sei $a \in K$. Das Minimalpolynom von $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ ist $X - a$.

Definition 8.32. Sei $q \in K[X]$ ein Polynom, $f : V \to V$ ein Endomorphismus eines K-Vektorraums V. Der verallgemeinerte Eigenraum von f zum Polynom q ist der K-Unterraum von V

$$V_q(f) = \{v \in V \ ; \ q(f)(v) = 0\} = \ker(q(f)).$$

Analog für quadratische Matrizen $A \in \mathrm{M}_n(K)$:

$$V_q(A) = \{v \in K^n \ ; \ q(A)v = 0\} = \ker(q(A)).$$

Beispiel 8.33. Sei $q(X) = X - \lambda$ linear. Dann ist

$$V_{X-\lambda}(f) = \{v \in V \ ; \ f(v) = \lambda v\}$$

der Eigenraum von f zum Eigenwert λ.

Satz 8.34. *Sei V ein endlich-dimensionaler K-Vektorraum und $f \in End_K(V)$. Sei $q \in K[X]$ ein irreduzibles Polynom. Dann sind äquivalent:*

(a) $V_q(f) \neq (0)$.
(b) *q teilt das Minimalpolynom:* $q \mid m_f(X)$,
(c) *q teilt das charakteristische Polynom:* $q \mid P_f(X)$,

Beweis. (a) $\Longrightarrow$ (b): Wir führen einen Widerspruchsbeweis. Sei $V_q(f) \neq (0)$ und trotzdem $q \nmid m_f(X)$. Der ggT $(q, m_f(X))$ ist entweder q oder 1, da q irreduzible ist, somit hier gleich 1. Nach dem Satz von Bezout, Satz 8.8, gibt es dann Polynome $a(X), b(X) \in K[X]$ mit

$$1 = a(X)q(X) + b(X)m_f(X).$$

Dies werten wir in $X = f$ in $\mathrm{End}_K(V)$ aus

$$\mathrm{id}_V = a(f)q(f) + b(f)m_f(f) = a(f)q(f),$$

und dann auf $0 \neq v \in V_q(f)$:

$$v = \mathrm{id}_V(v) = a(f)q(f)(v) = a(f)\big(q(f)(v)\big) = 0.$$

Dies ist der gesuchte Widerspruch.

(b) $\Longrightarrow$ (c): Dies folgt aus $m_f(X) \mid P_f(X)$ nach Satz 8.3.

(c) $\Longrightarrow$ (a): Das beweisen wir hier nur, falls $P_f(X)$ in Linearfaktoren zerfällt. Dann ist $q(X) = X - \lambda$ linear und λ Nullstelle des charakteristischen Polynoms. Damit ist der Eigenraum $V_\lambda(f) = V_q(f)$ nicht der Nullraum.

Und so geht (c) $\Longrightarrow$ (a) allgemein: Wir müssen zeigen, daß die lineare Abbildung $q(f) : V \to V$ nichttrivialen Kern hat. Dazu wählen wir eine Basis von V und schreiben f als Matrixmultiplikation mit einer Matrix $A \in \mathrm{M}_n(K)$. Dann ist $q(f)$ Matrixmultiplikation mit $q(A)$.

Es gibt einen Erweiterungskörper $K \subseteq L$, so daß $P_f(X)$ in Linearfaktoren zerfällt. Das nehmen wir hier einmal an, und verweisen auf die Vorlesung Algebra[14]. Wir fassen nun A auch als Matrix in $\mathrm{M}_n(L)$ auf und benennen dann A zur Unterscheidung mit A_L. Der springenden Punkt ist, daß die Dimensions des Kerns von der Erweiterung der Skalare von K nach L unabhängig ist:

$$\begin{aligned}\dim(\ker(q(A))) &= n - \mathrm{Rang}(q(A)) \\ &= n - \max\{r \ ; \text{ es gibt } r \times r \text{ Untermatrix von } q(A) \text{ mit det} \neq 0\} \\ &= n - \max\{r \ ; \text{ es gibt } r \times r \text{ Untermatrix von } q(A_L) \text{ mit det} \neq 0\} \\ &= n - \mathrm{Rang}(q(A_L)) = \dim(\ker(q(A_L))).\end{aligned}$$

Sei $\lambda \in L$ eine Nullstelle von $q(X)$. Dann gibt es ein Polynom $p(X) \in L[X]$ mit $q(X) = p(X)(X - \lambda)$ in $L[X]$. Außerdem ist λ ein Eigenwert von A_L. Sei $v \in L^n$ ein Eigenvektor zu λ, demnach

$$q(A_L)v = p(A_L)(A_L - \lambda)v = p(A_L)(A_Lv - \lambda v) = 0.$$

Dies zeigt $\ker(q(A_L)) \neq (0)$ und damit auch $V_q(f) = \ker(q(A)) \neq (0)$. □

Korollar 8.35. *Eine Nullstelle des charakteristischen Polynoms ist auch eine Nullstelle des Minimalpolynoms.*

Beweis. Sei f Endomorphismus und $\lambda \in K$ mit $P_f(\lambda) = 0$. Dann ist $X - \lambda$ ein Teiler von $P_f(X)$ und somit nach Satz 8.34 auch ein Teiler von $m_f(X)$. Damit folgt aber $m_f(\lambda) = 0$. □

8.7. **Der Chinesische Restsatz.**

Lemma 8.36. *Sei R ein Hauptidealring und a, b teilerfremde Elemente von R. Dann gilt für das kgV*

$$(ab) = (a) \cap (b).$$

Beweis. Da $(ab) \subseteq (a)$ und analog mit (b) gilt $(ab) \subseteq (a) \cap (b)$. Zu zeigen ist also die umgekehrte Inklusion.

Da a, b teilerfremd sind, gibt es nach Sazt 8.8 $\alpha, \beta \in R$ mit

$$1 = \alpha a + \beta b.$$

Sei $z \in (a) \cap (b)$, also gibt es $x, y \in R$ mit $z = ax = by$. Dann ist

$$z = (\alpha a + \beta b)z = \alpha az + \beta bz = \alpha aby + \beta bax = (\alpha y + \beta x)ab,$$

und dies liegt im Ideal (ab). □

Satz 8.37 (Chinesischer Restsatz)**.** *Sei R ein Hauptidealring und a, b teilerfremde Elemente von 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*

$$R/(ab) \simeq R/(a) \times R/(b).$$

Beweis. Die kanonischen Projektionen definieren einen Ringhomomorphismus

$$\begin{aligned}\mathrm{pr} : R &\to R/(a) \times R/(b) \\ r &\mapsto (r + (a), r + (b))\end{aligned}$$

[14]Halt: wir kennen L bereits. Denn $L = K[X]/(q(X))$ ist nach Satz 8.16 ein Körper, der K als Restklassen der konstanten Polynome enthält. Das Element

$$\lambda = X + (q(X)),$$

also das Bild von X in L unter der Quotientenabbildung $K[X] \to L = K[X]/(q(X))$ erfüllt

$$q(\lambda) = q(X) \equiv 0 \mod (q(X))$$

quasi erzwungenermaßen per Konstruktion!

mit Kern (nach Lemma 8.36)

$$\ker(\mathrm{pr}) = \ker(\mathrm{pr}_a) \cap \ker(\mathrm{pr}_b) = (a) \cap (b) = (ab).$$

Die Behauptung folgt aus dem Homomorphiesatz für Ringe, Satz 6.36, wenn pr surjektiv ist.

Da a, b teilerfremd sind, gibt es nach Satz 8.8 $\alpha, \beta \in R$ mit

$$1 = \alpha a + \beta b.$$

Damit gilt (mit leicht mißbräuchlicher Notation mit Vertretern statt Nebenklassen)

$$\mathrm{pr}(\alpha a) = (\alpha a, 1 - \beta b) \equiv (0, 1)$$
$$\mathrm{pr}(\beta b) = (1 - \alpha a, \beta b) \equiv (1, 0).$$

Zu $x, y \in R$ berechnen wir nun für $z = x\beta b + y\alpha a$

$$\mathrm{pr}(z) = \mathrm{pr}(x)\,\mathrm{pr}(\beta b) + \mathrm{pr}(y)\,\mathrm{pr}(\alpha a) \equiv (x, x)(1, 0) + (y, y)(0, 1) = (x, 0) + (0, y) = (x, y),$$

und pr ist offensichtlich surjektiv. □

Korollar 8.38. *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 $b = a_2 a_3 \ldots a_n$ sind teilerfremd. Andernfalls hätte nach Satz 8.25 der ggT (a_1, b) einen Primteiler p. Aus $p \mid a_2 a_3 \ldots a_n$ 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 8.37 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 verfiziert leicht, daß dieser Isomorphismus aus den kanonischen Projektionen zusammengesetzt ist und so die behauptete Form hat. □

Beispiel 8.39. (1) Ist speziell $R = K[X]$ und $f = \prod_{i=1}^{n} p_i^{e_i}$ die Zerlegung in (paarweise verschiedene) Primfaktoren p_i von f, so gilt kanonisch

$$K[X]/(f) \cong \prod_{i=1}^{n} K[X]/(p_i^{e_i}).$$

(2) Im Fall des Hauptidealrings $\mathbb{Z}$ bedeutet Korollar 8.38 folgendes. Seien $n_1, \ldots, n_r$ paarweise teilerfremde positive natürliche Zahlen und $N = \prod_{i=1}^{r} n_i$ das Produkt. Dann ist die natürliche Abbildung

$$\varphi : \mathbb{Z}/N\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$$
$$a + N\mathbb{Z} \mapsto (a + n_i\mathbb{Z})$$

ein Isomorphismus von Ringen. Diese Aussage ist auch für die Struktur der zugrundeliegenden abelschen Gruppen interessant, wird aber leichter mit Ringen als nur mit Gruppen bewiesen.

Anders ausgedrückt besagt der Chinesische Restsatz konkret, daß für beliebige ganze Zahlen $a_i \in \mathbb{Z}$ für $1 \leq i \leq r$ das System der Kongruenzen

$$x \equiv a_i \mod n_i \quad \text{für alle } 1 \leq i \leq r$$

eine Lösung $x \in \mathbb{Z}$ besitzt, die als Lösung x modulo N sogar eindeutig ist.

Übungsaufgaben zu §8

Übungsaufgabe 8.1. 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 8.2. Sei 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, daßfür ein i mit $1 \leq i \leq n$ schon $p \mid a_i$.

Übungsaufgabe 8.3. Sei K ein Körper. Bestimmen Sie die primen Elemente in $K[[X]]$ bis auf Einheiten.

Übungsaufgabe 8.4. 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 8.5. 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 8.6. Sei R ein Ring und $x, y, q, r \in R$ mit $x = qy + r$. Dann gilt

$$(qy + r, y) = (r, y).$$

9. Die Jordannormalform

Eine Normalform für einen Endomorphismus $\varphi : V \to V$ eines K-Vektorraums ist eine Existenzaussage für eine besonderes an den Endomorphismus angepaßte Basis $\mathscr{B}$ von V, bezüglich derer die Matrix des Endomorphismus eine aussagekräftige Form annimmt.

Für eine Matrix $A \in \mathrm{M}_n(K)$ besagt eine Normalform entsprechend die Existenz einer Matrix $S \in \mathrm{GL}_n(K)$, so daß SAS^{-1} eine aussagekräftige Form annimmt. Das ist dasselbe in grün: man studiert A mittels des Endomorphismus 'Matrixmultiplikation mit A' und S ist dann die Basiswechselmatrix von der Standardbasis in die besondere Basis.

9.1. **Invariante Unterräume.**

Definition 9.1. Ein **invarianter Unterraum** eines K-Vektorraums V bezüglich eines Endomorphismus $\varphi : V \to V$ ist ein Untervektorraum $W \subseteq V$ mit $\varphi(W) \subseteq W$. Genauer ist die Bezeichnung **φ-invarianter Unterraum**.

Bemerkung 9.2. Bezüglich einer Basis $\mathscr{B} = (b_1, \ldots, b_n)$ von V, so daß W die lineare Hülle von $b_1, \ldots, b_r$ ist, offenbart sich die φ-invarianz von W durch eine Blockmatrixform

$$\mathrm{M}^{\mathscr{B}}_{\mathscr{B}}(\varphi) = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

der Blockgröße $(r, n-r)$, wobei A die Matrix von $\varphi|_W$ bezüglich $(b_1, \ldots, b_r)$ ist.

Proposition 9.3. *Sei $\varphi : V \to V$ ein Endomorphsimus eines K-Vektorraums V. Sei $P \in K[X]$ ein Polynom.*

(1) *$P(\varphi)$ kommutiert mit φ.*
(2) *$\ker(P(\varphi))$ und $\mathrm{im}(P(\varphi))$ sind φ-invariante Unterräume von V.*

Beweis. (1) Dies folgt mit dem Auswertungshomomorphismus ev_φ aus
$$P(\varphi)\varphi = \mathrm{ev}_\varphi(P(X)X) = \mathrm{ev}_\varphi(XP(X)) = \varphi P(\varphi)$$
wegen der Kommutativität des Polynomrings.

(2) Sei $v \in \ker(P(\varphi))$, dann gilt $\varphi(v) \in \ker(P(\varphi))$, denn
$$P(\varphi)\big(\varphi(v)\big) = \varphi\big(P(\varphi)(v)\big) = \varphi(0) = 0.$$
Sei $v \in \mathrm{im}(P(\varphi))$, also für ein geeignetes $w \in V$ gilt $v = P(\varphi)(w)$. Dann ist
$$\varphi(v) = \varphi(P(\varphi)(w)) = P(\varphi)\big(\varphi(w)\big)$$
somit auch $\varphi(v) \in \mathrm{im}(P(\varphi))$. □

Definition 9.4. Eine **invariante $\bigoplus$-Zerlegung** eines K-Vektorraums V bezüglich eines Endomorphismus $\varphi : V \to V$ ist eine Zerlegung
$$V = W_1 \oplus W_2$$
(oder auch mit mehr Summanden) mit φ-invarianten Unterräumen W_i, $i = 1, 2$. Genauer ist die Bezeichnung **φ-invariante $\bigoplus$-Zerlegung**.

Bemerkung 9.5. Bezüglich einer Basis $\mathscr{B} = (b_1, \ldots, b_n)$ von V, so daß W_1 die lineare Hülle von $\mathscr{B}_1 = (b_1, \ldots, b_r)$ und W_2 die lineare Hülle von $\mathscr{B}_2 = (b_{r+1}, \ldots, b_n)$ ist, offenbart sich die φ-invarianz der Zerlegung $V = W_1 \oplus W_2$ durch eine Blockmatrixform
$$\mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi) = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$
der Blockgröße $(r, n-r)$, wobei A_i die Matrix von $\varphi|_{W_i}$ bezüglich $\mathscr{B}_i$, $i = 1, 2$ ist.

Proposition 9.6. *Sei $\varphi : V \to V$ ein Endomorphismus eines endlich-dimensionalen K-Vektorraums V.*

(1) Sei $W \subseteq V$ ein φ-invarianter Unterraum. Dann gilt mit $\varphi_W = \varphi|_W$
$$P_{\varphi_W}(X) \mid P_\varphi(X),$$
$$m_{\varphi_W}(X) \mid m_\varphi(X).$$

(2) Sei $V = W_1 \oplus W_2$ eine φ-invariante Zerlegung. Dann gilt mit $\varphi_i = \varphi|_{W_i}$
$$P_\varphi(X) = P_{\varphi_1}(X)P_{\varphi_2}(X),$$
$$m_\varphi(X) = \mathrm{kgV}(m_{\varphi_1}(X), m_{\varphi_2}(X))$$

Beweis. Die Aussage zum charakteristischen Polynom in (1) und (2) folgt aus den Regeln der Determinante zu Matrizen in oberer Dreiecksblockform.

(1) Für alle $w \in W$ gilt
$$0 = m_\varphi(\varphi)(w) = m_\varphi(\varphi|_W)(w),$$
und damit liegt $m_\varphi(X)$ im von $m_{\varphi|_W}(X)$ erzeugten Ideal.

(2) Die Summanden W_1 und W_2 sind invariante Unterräume. Daher teilt $m_{\varphi_i}(X)$ für $i = 1, 2$ das Minimalpolynom $m_\varphi(X)$. Damit gilt
$$\mathrm{kgV}(m_{\varphi_1}(X), m_{\varphi_2}(X)) \mid m_\varphi(X).$$
Zu zeigen ist nun, daß das kgV ausgewertet auf φ schon die Nullabbildung auf V ist. Wir schreiben
$$D(X) := \mathrm{kgV}(m_{\varphi_1}(X), m_{\varphi_2}(X)) = f_1(X)m_{\varphi_1}(X) = f_2(X)m_{\varphi_2}(X)$$
und rechnen für beliebiges $v = w_1 + w_2 \in V$ mit $w_i \in W_i$, $i = 1, 2$
$$\begin{aligned} D(\varphi)v &= D(\varphi)w_1 + D(\varphi)w_2 = D(\varphi_1)w_1 + D(\varphi_2)w_2 \\ &= f_1(\varphi_1)\big(m_{\varphi_1}(\varphi_1)w_1\big) + f_2(\varphi_2)\big(m_{\varphi_2}(\varphi_2)w_2\big) = f_1(\varphi_1)0 + f_2(\varphi_2)0 = 0 \end{aligned}$$
(wir lassen zur Übersichtlichkeit ein paar Klammern weg). □

Satz 9.7 (Kernzerlegung)**.** *Sei $\varphi : V \to V$ ein Endomorphismus eines endlich-dimensionalen K-Vektorraums V. Sei $0 \neq f \in K[X]$ ein Polynom und sei*

$$f = c \cdot \prod_{i=1}^{s} p_i(X)^{n_i}$$

die Faktorisierung in irreduzible Polynome und $c \in K^\times$, wobei die p_i paarweise nicht assoziiert (etwa normiert und paarweise verschieden) sind. Dann gibt es die folgende φ-invariante Zerlegung

$$\ker(f(\varphi)) = \ker(p_1(\varphi)^{n_1}) \oplus \ldots \oplus \ker(p_s(\varphi)^{n_s}).$$

Beweis. Wir setzen für $1 \leq i \leq s$

$$q_i(X) = \prod_{\substack{j=1 \\ j \neq i}}^{s} p_j(X)^{n_j}.$$

Dann sind die $q_1(X), \ldots, q_s(X)$ (nicht paarweise) teilerfremd nach Korollar 8.29. Es gibt also nach dem Satz von Bézout, Satz 8.8, Polynome $a_i(X) \in K[X]$ mit

$$1 = a_1(X)q_1(X) + \ldots + a_s(X)q_s(X).$$

Sei $w \in W = \ker(f(\varphi))$ beliebig. Wir setzen $W_i = \ker(p_i(X)^{n_i})$ für $1 \leq i \leq s$ und weiter

$$w_i = a_i(\varphi)q_i(\varphi)(w),$$

so daß $w_i \in W_i$ weil

$$p_i(\varphi)^{n_i}(w_i) = a_i(\varphi)q_i(\varphi)p_i(\varphi)^{n_i}(w) = c^{-1} \cdot a_i(\varphi)f(\varphi)(w) = 0.$$

Außerdem gilt

$$w = \big(a_1(\varphi)q_1(\varphi) + \ldots + a_s(\varphi)q_s(\varphi)\big)(w) = w_1 + \ldots + w_s.$$

Somit erzeugen die Unterräume W_i für $1 \leq i \leq s$ den Kern W.

Es bleibt zu zeigen, daß die Summe direkt ist. Wir arbeiten durch Widerspruch. Sei dazu $v_i \in W_i$ mit $v_1 + \ldots + v_s = 0$, und nicht alle $v_i = 0$. Sei oBdA $v_1 \neq 0$. Da $p_1(X)^{n_1}$ und $q_1(X)$ teilerfremd sind, gibt es nach dem Satz von Bézout, Satz 8.8, Polynome $a(X), b(X) \in K[X]$ mit

$$1 = a(X)p_1(X)^{n_1} + b(X)q_1(X).$$

Weil für alle $j > 1$ gilt $q_1(\varphi)(v_j) = 0$, folgt der Widerspruch

$$v_1 = (1 - a(\varphi)p_1(\varphi)^{n_1})(v_1) = b(\varphi)q_1(\varphi)\big(-v_2 - \ldots - v_s\big) = 0.$$

Die Zerlegung ist φ-invariant nach Proposition 9.3. □

Korollar 9.8. *Sei $\varphi : V \to V$ ein Endomorphismus eines endlich-dimensionalen K-Vektorraums V. Sei*

$$m_\varphi(X) = \prod_{i=1}^{s} p_i(X)^{n_i}$$

die Faktorisierung des Minimalpolynoms in irreduzible Polynome, wobei die $p_i(X)$ paarweise verschieden sind. Dann hat V die φ-invariante Zerlegung

$$V = V_1 \oplus \ldots \oplus V_s$$

mit $V_i = \ker(p_i(\varphi))^{n_i}$ für $1 \leq i \leq s$. Das Minimalpolynom von $\varphi_i = \varphi|_{V_i}$ ist $p_i(X)^{n_i}$

Beweis. Das ist nichts anderes als die Kernzerlegung, Satz 9.7, für das Minimalpolynom, denn

$$V = \ker(m_\varphi(\varphi)).$$

per Definition. □

9.2. **Begleitmatrix und Jordanblock.** Wir studieren drei Beispiele.

9.2.1. *Die Begleitmatrix.* Sei

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$$

ein normiertes Polynom vom Grad n. Den Faktorring

$$V = K[X]/(f),$$

fassen wir mittels Operation der Konstanten aus K als K-Vektorraum auf. Nach Division mit Rest hat jedes Element $p + (f) \in V$ einen Representanten $r = p - qf$ vom Grad $< n$ (oder $r = 0$). Dieser ist auch eindeutig, da sonst f ein Teiler der Differenz, also eines Polynoms vom Grad $< n$ sein müßte. Es ist übersichtlicher, nun den Notationsmißbrauch zu begehen und jedes Element $r + (f) \in V$ mit $\deg(r) < \deg(f) = n$ (oder $r = 0$) mit dem Polynom r anzusprechen.

Wir nutzten die Ringstruktur von $V = K[X]/(f)$ und betrachten den Endomorphismus

$$\varphi : V \to V,$$

der durch die Multiplikation mit X gegeben ist. Da X mit den Konstanten kommutiert, ist dies K-linear.

Die bevorzugte Basis von $K[X]/(f)$ ist die Basis der Monome $\mathscr{B} = (1, X, X^2, \ldots, X^{n-1})$. Es ergibt sich folgende Matrix, die **Begleitmatrix** zu f.

$$\Lambda(f) := \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi) = \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(X\cdot) = \begin{pmatrix} 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{M}_n(K).$$

Ist speziell $f(X) = X - \lambda$ für ein $\lambda \in K$, so ist $K[X]/(X - \lambda)$ von Dimension 1 und die Begleitmatrix ist

$$\Lambda(X - \lambda) = (\lambda) \in \mathrm{M}_1(K).$$

Es operiert X und damit φ durch Multiplikation mit λ.

Proposition 9.9. *Minimalpolynom und charakteristisches Polynom von φ stimmen überein:*

$$P_\varphi(X) = f(X) = m_\varphi(X).$$

Beweis. Es operiert $f(\varphi)$ durch Multiplikation mit $f(X)$, denn

$$\mathrm{ev}_\varphi : K[X] \to \mathrm{End}_K(V)$$

ist ein Ringhomomorphismus. Wegen $f(X) = 0$ im Ring $K[X]/(f)$ ist auch Multiplikation mit $f(X)$ die Nullabbildung, somit

$$f(\varphi) = 0.$$

Damit gilt $m_\varphi(X) \mid f(X)$. Andererseits gilt für jedes $g \in K[X]$ mit $\deg(g) < \deg(f)$, daß ausgewertet auf dem Vektor $1 \in V = K[X]/(f)$

$$g(\varphi)(1) = g(X) \cdot 1 = g(X) \neq 0.$$

Damit kann das Minimalpolynom nicht kleineren Grad als n haben, ergo

$$m_\varphi(X) = f(X).$$

Damit liegt aber auch das Charakteristische Polynom fest (man könnte auch eine Determinante ausrechnen, aber dazu sind wir zu bequem, wenn es auch anders geht), denn als normiertes Vilefaches von $m_\varphi(X)$ vom Grad n bleibt nur $m_\varphi(X)$ selbst. □

Seien $p_i \in K[X]$ für $1 \leq i \leq s$ paarweise verschiedene irreduzible normierte Polynome und

$$f(X) = \prod_{i=1}^{s} p_i^{n_i}(X)$$

die Faktorisierung von $f(X)$ in $K[X]$. Dann stimmt die Zerlegung des Chinesischen Restsatzes aus Beispiel 8.39

$$K[X]/(f) \cong \prod_{i=1}^{n} K[X]/(p_i^{n_i}).$$

mit der Kernzerlegung von V bezüglich des Polynoms $f(X)$ überein. Man muß nur mittels des Isomorphismus die Faktoren $K[X]/(p_i^{n_i})$ zu Unterräumen $V_i \subseteq V$ machen, um eine innere direkte Summe zu erhalten (wenn man unbedingt will).

Es folgt die Existenz einer Matrix $S \in \mathrm{GL}_n(K)$ mit $S\Lambda(f)S^{-1}$ in Blockdiagonalform

$$S\Lambda(f)S^{-1} = \begin{pmatrix} \Lambda(p_1^{n_1}) & & \\ & \ddots & \\ & & \Lambda(p_s^{n_s}) \end{pmatrix}$$

9.2.2. *Der allgemeine Jordanblock.* Wir studieren das Beispiel aus Abschnitt §9.2.1 im Spezialfall $f(X) = p(X)^n$ mit einem irreduziblen Polynom vom Grad $d = \deg(p)$

$$p(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X].$$

Als Basis $\mathscr{B}$ wählen wir diesmal die $nd = \deg(p^n)$-vielen Vektoren

$$X^i p(X)^j$$

mit $0 \leq i < d$, und $0 \leq j < n$. Dies ist eine Basis, denn es handelt sich um die richtige Anzahl von Vektoren und diese erzeugen V: per fortlaufender Division mit Rest läßt sich jedes Polynom $g \in K[X]$ schreiben als

$$g = r_0 + g_0p = r_0 + (r_1 + g_1p)p = r_0 + r_1p + (r_2 + g_2p)p^2 = \ldots = r_0 + r_1p + r_2p^2 + \ldots + r_mp^m$$

mit $\deg(r_i) < \deg(p) = d$ für alle $0 \leq i \leq m$.

Wir ordnen $\mathscr{B}$ wie folgt an (lexikographisch nach (j, i) für $X^i p(X)^j$):

$$(1, X, \ldots, X^{d-1}, p(X), Xp(X), \ldots, X^{d-1}p(X), p(X)^2, Xp(X)^2, \ldots, X^{d-1}p(X)^{n-1}).$$

In dieser Basis wird der Endomorphismus φ, gegeben durch Multiplikation mit X auf $V = K[X]/(p^n)$ beschrieben durch die Matrix, der **Jordanblock der Länge n zum irreduziblen Polynom p**,

$$J(p(X)^n) := \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi) = \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(X\cdot) = \begin{pmatrix} \boxed{\Lambda(p)} & & & & \\ 1 & \boxed{\Lambda(p)} & & & \\ & 1 & \ddots & & \\ & & 1 & \boxed{\Lambda(p)} & \\ & & & 1 & \boxed{\Lambda(p)} \end{pmatrix}$$

Alle fehlenden Einträge von $J(p(X)^n)$ sind wie üblich mit 0 aufzufüllen. Die entscheidende Rechnungen sind

$$X(X^i p(X)^j = X^{i+1} p(X)^j$$

solange $i < d-1$, das erklärt die Matrix innerhalb der Blöcke bis auf die letzte Spalte, und

$$X(X^{d-1}p(X)^j) = X^d p(X)^j = (p(X) - \sum_{i=0}^{d-1} a_i X^i) p(X)^j = p(X)^{j+1} - \sum_{i=0}^{d-1} a_i (X^i p(X)^j),$$

für die Spalten mit der extra 1 unter den Kästchen.

Proposition 9.10. *Das charakteristische Polynom von $J(p(X)^n)$ ist $p(X)^n$ und stimmt mit dem Minimalpolynom von $J(p(X)^n)$ überein.*

Beweis. Das folgt aus Proposition 9.9, denn ein Basiswechsel ändert weder Minimalpolynom noch charakteristisches Polynom. □

9.2.3. *Der Jordanblock zu einem Eigenwert.* Wir spezialisieren weiter zu $p(X) = X - \lambda$ für ein $\lambda \in K$. Die Basis aus Abschnitt §9.2.2 wird nun

$$\mathscr{B} = (b_1 = 1, \ldots, b_i = (X-\lambda)^i, \ldots, b_{n-1} = (X-\lambda)^{n-1}).$$

Dann gilt mit der praktischen Konvention $b_n = 0$ für alle $1 \leq i \leq n$

$$\varphi(b_i) = Xb_i = \lambda b_i + (X-\lambda)b_i = \lambda b_i + (X-\lambda)(X-\lambda)^i = \lambda b_i + b_{i+1}.$$

Das gilt auch für $i = n-1$, denn in $V = K[X]/(X-\lambda)^n$ ist ja $(X-\lambda)^n = 0$. Es ergibt sich folgende Matrix, der **Jordanblock der Länge n zum Eigenwert λ**:

$$J_n(\lambda) := J((X-\lambda)^n) = \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi) = \mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(X\cdot) = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & 1 & \ddots & \\ & & \ddots & \lambda \\ & & & 1 & \lambda \end{pmatrix}$$

Alle fehlenden Einträge von $J_n(\lambda)$ sind wie üblich mit 0 aufzufüllen.

Proposition 9.11. *Das charakteristische Polynom von $J_n(\lambda)$ ist $(X-\lambda)^n$ und stimmt mit dem Minimalpolynom überein.*

Beweis. Das folgt als Spezialfall von Proposition 9.10. Wir geben trotzdem nochmals einen diekten Beweis, weil die nötige Determinante einfach genug auszuwerten ist.

Sei X eine Variable. Die Matrix $X \cdot E - J_n(\lambda)$ mit der Einheitsmatrix $E \in \mathrm{M}_n(K)$ ist diagonal mit allen Diagonaleinträgen $X - \lambda$. Damit ist das charakteristische Polynom $(X-\lambda)^n$. Das Minimalpolynom teilt das charakteristische Polynom und hat daher die Form $(X-\lambda)^m$ für ein $m \leq n$. Die Matrix $J_n(\lambda) - \lambda E$ ist

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

also mit der Standardbasis $(e_1, \ldots, e_n)$ und der bequemen Vereinbarung $e_i = 0$, falls $i > n$, gilt

$$(J_n(\lambda) - \lambda E)e_i = e_{i+1}.$$

Insbesondere gilt

$$(J_n(\lambda) - \lambda E)^m e_1 = e_{m+1}.$$

Daher muß $m \geq n$ sein, also $n = m$, und das Minimalpolynom stimmt mit dem charakteristischen Polynom überein. □

9.3. **Die Jordannormalform im zerfallenden Fall.**

Theorem 9.12 (Jordannormalform)**.** *Sei K ein Körper.*

(1) *Sei $\varphi : V \to V$ ein Endomorphismus eines endlich dimensionalen K-Vektorraums. Dann gibt es eine Basis von V, bezüglich der die Matrix von φ aus Jordanblöcken besteht, die längs der Diagonale angeordnet sind.*

(2) *Eine quadratische Matrix $A \in \mathrm{M}_n(K)$ über K ist ähnlich zu einer Matrix aus Jordanblöcken, die längs der Diagonale angeordnet sind.*

Konkret behauptet (1) die Existenz einer Basis $\mathscr{B}$, bzw. (2) die Existenz einer invertierbaren Matrix $S \in \mathrm{GL}_n(K)$ mit

$$\mathrm{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi) \text{ bzw. } SAS^{-1} = \begin{pmatrix} \boxed{J(p_1(X)^{n_1})} & & \\ & \ddots & \\ & & \boxed{J(p_s(X)^{n_s})} \end{pmatrix} \qquad (\star)$$

*Alle Einträge außerhalb der Blockdiagonale sind 0. Die Blockdiagonalmatrix $(\star)$ aus Jordanblöcken nennt man die **Jordannormalform** (des Edomorphismus φ bzw. der Matrix A).*

(3) *In (1) und (2) hängen die Anzahl der Jordanblöcke der Form $J(p(X)^n))$ für jedes feste n und jedes irreduzible normierte Polynom $p(X) \in K[X]$ nicht von den auftretenden Wahlen ab. Das heißt: jede Basis $\mathscr{B}$, bzw. jede invertierbaren Matrix S, welche zu einer Jordannormalform führt, liefert bis auf Permutation der Jordanblöcke dieselbe Jordannormalform.*

(4) *Das charakteristische Polynom von $(\star)$ ist*

$$P_\varphi(X) \text{ bzw. } P_A(X) = \prod_{i=1}^{s} p_i(X)^{n_i}.$$

Das Minimalpolynom von $(\star)$ ist das Produkt

$$m_\varphi(X) \text{ bzw. } m_A(X) = \prod_{p(X)} p(X)^{m_p}.$$

wobei $p(X)$ alle normierten irreduziblen Polynome durchläuft und der Exponent

$$m_p = \max\{n_i \ ; \ p_i(X) = p(X), 1 \leq i \leq s\}$$

nur endlich oft von 0 verschieden ist, und daher das Produkt trotzdem ein endliches ist.

Bemerkung 9.13. (1) Unter den Jordanblöcken einer Jordannormalform dürfen mehrere Jordanblöcke zum gleichen gleichen irreduziblen Polynom auftreten.

(2) Wenn man die Basis, welche zur Jordannormalform führt, in umgekehrter Reihenfolge durchläuft, dann wandern die Einträge 1 aus den Jordanblöcken von der ersten Nebendiagonalen unter der Diagonale zur ersten Nebendiagonalen oberhalb der Diagonale. Diese Variante der Jordannormalform ist bis eben auf die Umordnung der Basiselemente äquivalent und wird auch oft in der Literatur verwendet.

(3) Oft bestimmen schon $P_\varphi(X)$ und $m_\varphi(X)$ die Jordannormalform.

(4) Wenn $P_\varphi(X)$ in paarweise verschiedene (normierte) Linearfaktoren zerfällt, dann gibt es zu jedem Eigenwert λ von φ genau ein Jordanblock, und dieser hat Länge 1. Damit wird die Jordannormalform eine Diagonalform. Der Endomorphsimus ist diagonalisierbar (wie wir aus Linearer Algebra 1 schon wissen).
(5) Genauer: ist $m_\varphi(X)$ ein Produkt paarweise verschiedener (normierte) Linearfaktoren, dann haben alle Jordanblöcke die Länge 1. Dann und nur dann ist φ diagonalisierbar.

Beispiel 9.14. Sei $\dim_K(V) = 3$ und $\varphi : V \to V$ mit $P_\varphi(X) = (X-a)^2(X-b)$ für $a \neq b \in K$. Dann ist $m_\varphi(X) = (X-a)^e(X-b)$ mit $e = 1$ oder $e = 2$. Falls $e = 1$, so ist φ diagonalisierbar mit Jordannormalform

$$\begin{pmatrix} a & & \\ & a & \\ & & b \end{pmatrix}$$

und, falls $e = 2$, so muß die Jordannormalform

$$\begin{pmatrix} a & & \\ 1 & a & \\ & & b \end{pmatrix}$$

sein.

Beweis von Theorem 9.12 mit zerfallendem charakteristischen Polynom. Aussage (2) in Theorem 9.12 ist die Matrix-Version von Aussage (1). Wir zeigen also nur (1).

Die Behauptung zu charakteristischem Polynom und Minimalpolynom in Aussage (4) folgen sofort aus Proposition 9.6 (2) und Proposition 9.10.

Schritt 1: Zerlegung nach irreduziblen Faktoren.
Die Kernzerlegung bezüglich des Minimalpolynoms aus Korollar 9.8 sowie die Blockmatrixform bezüglich einer invarianten Summenzerlegung wie in Bemerkung 9.5 erlauben es uns anzunehmen, daß oBdA

$$m_\varphi(X) = p(X)^d$$

mit $p(X) \in K[X]$ normiert und irreduzible ist.

Ab jetzt nehmen wir an, daß φ ein zerfallendes charakteristisches Polynom hat.

Schritt 2: Verschiebung zu Eigenwert 0.
Sei $\lambda \in K$ und $m_\varphi(X) = (X-\lambda)^d$. Wir ersetzen nun

$$\psi = \varphi - \lambda.$$

Dann gilt $m_\psi(X) = X^d$. Wegen

$$J_n(\lambda) = J_n(0) + \lambda E_n$$

mit der Einheitsmatrix $E_n \in \mathrm{M}_n(K)$ reicht es, das Theorem für ψ zu zeigen, um es für φ und damit allgemein im zerfallenden Fall fertig zu beweisen.

Schritt 3: Induktion nach der Dimension.
Jetzt argumentieren wir per Induktion nach $\dim_K(V) = n$. Für den Induktionsanfang[15] mit $\dim_K(V) = 0$ ist nichts zu tun. Wir setzten nun

$$W = \mathrm{im}(\psi) \subseteq V.$$

Dann ist W ein ψ-invarianter Unterraum nach Proposition 9.3. Da

$$\psi^{d-1}(W) = \psi^{d-1}(\psi(V)) = \psi^d(V) = 0$$

gilt für das Minimalpolynom der Einschränkung $\psi|_W$

$$m_{\psi|_W}(X) \mid X^{d-1}.$$

[15]Es ist gefährlich, den Induktionsanfang in einen solchen degenerierten Fall zu legen. Manchmal stimmen die Begriffe dann nicht mehr, oder nur mit der richtigen Interpretation. Dies ist hier aber nötig.

Damit gilt $W \neq V$, denn das Minimalpolynom hat sich geändert. Per Induktionsannahme gilt also die Jordannormalform für $\psi|_W : W \to W$.

Schritt 4: Beginn der Basiswahl.
Nach der konkreten Beschreibung aus Abschnitt §9.2.3 bedeutet dies, daß W eine Basis der Form

$$\mathscr{B}_W = \big(a_1, \psi(a_1), \ldots, \psi^{n_1-1}(a_1), a_2, \ldots, \psi^{n_{r-1}-1}(a_{r-1}), a_r, \psi(a_r), \ldots, \psi^{n_r-1}(a_r)\big)$$

mit $\psi^{n_i}(a_i) = 0$ für alle $1 \leq i \leq r$ hat. Dabei sorgt $a_i, \psi(a_i), \ldots, \psi^{n_i-1}(a_i)$ für einen Jordanblock der Form $J_{n_i}(0)$. Da $a_i \in W$ im Bild von ψ liegen, gibt es $b_i \in V$ mit $\psi(b_i) = a_i$ für alle $1 \leq i \leq r$.

Schritt 5: Ende der Basiswahl.
Da ψ bezüglich der Basis $\mathscr{B}_W$ so explizit ist, folgt leicht, daß die jeweils letzten Vektoren in den Jordanblöcken

$$\psi^{n_1}(b_1), \ldots, \psi^{n_r}(b_r)$$

eine Basis von

$$\ker(\psi|_W) = \ker(\psi) \cap W$$

bilden. Wir ergänzen dies durch

$$b_{r+1}, \ldots, b_s$$

zu einer Basis von $\ker(\psi)$. Diese Vektoren beschreiben jeder für sich einen Jordanblock der Form $J_1(0)$.

Schritt 6: Eine Basis.
Das foglende System ist eine passende Basis für die Jordannormalform von ψ:

$$\mathscr{B} = \big(b_1, \psi(b_1), \ldots, \psi^{n_1}(b_1), b_2, \ldots, \psi^{n_{r-1}}(b_{r-1}), b_r, \psi(b_r), \ldots, \psi^{n_r}(b_r), b_{r+1}, \ldots, b_s\big).$$

Wir müssen nur noch zeigen, daß dies tatsächlich eine Basis ist. Daß ψ in dieser Basis durch eine Blockform mit Jordanblöcken auf der Diagonalen beschrieben wird, sollte zu diesem Zeitpunkt offensichtlich sein, siehe Abschnitt §9.2.3.

Gegenüber der Basis $\mathscr{B}_W$ von W gibt es neue Vektoren $b_1, \ldots, b_r, b_{r+1}, \ldots, b_s$, so daß

$$|\mathscr{B}| = s + |\mathscr{B}_W| = s + \dim(W) = \dim(\ker(\psi)) + \dim(\operatorname{im}(\psi)) = \dim(V)$$

nach dem Dimensionssatz für Kern und Bild. Damit ist $\mathscr{B}$ Basis, wenn wir nachweisen, daß die Vektoren in $\mathscr{B}$ linear unabhängig sind.

Eine ökonomische Form eine Linearkombination der Vektoren aus $\mathscr{B}$ zu schreiben benutzt Polynome $f_i \in K[X]$ vom Grad $\deg(f_i) \leq n_i$ für alle $1 \leq i \leq r$ und $\lambda_{r+1}, \ldots, \lambda_s \in K$:

$$\sum_{i=1}^{r} f_i(\psi)(b_i) + \sum_{i=r+1}^{s} \lambda_i b_i. \tag{9.1}$$

Angenommen, diese Linearkombination sei 0. Dann wenden wir ψ darauf an, und finden

$$0 = \sum_{i=1}^{r} f_i(\psi)(a_i).$$

Weil $\mathscr{B}_W$ eine Basis von W ist, folgt $f_i(X) = \lambda_i X^{n_i}$ für gewisse $\lambda_i \in K$ und alle $1 \leq i \leq r$. Dann aber beschreibt (9.1) nur eine Linearkombination der Basis

$$\psi^{n_1}(b_1), \ldots, \psi^{n_r}(b_r), b_{r+1}, \ldots, b_s$$

von $\ker(\psi)$. Somit müssen alle $\lambda_i = 0$ sein und die Vektoren aus $\mathscr{B}$ sind in der Tat linear unabhängig. Dies beendet den Beweis der Existenz der Jordannormalform im Fall eines zerfallenden charakteristischen Polynoms.

Nun wenden wir uns der Eindeutigkeitsaussage (3) der Jordannormalform zu. Die Jordannormalform beschreibt eine φ-invarianten Zerlegung $V = \bigoplus_{i=1}^{s} W_i$ in Summanden W_i mit nur

einem Jordanblock (der Endomorphismus $\varphi|_{W_i}$ ist durch $J(p_i(X)^{n_i})$ dargestellt). Daher ist für jedes $P(X) \in K[X]$ der Kern $\ker(P(\varphi))$ blockweise zu bestimmen:

$$\ker(P(\varphi)) = \bigoplus_{i=1}^{s} \ker(P(\varphi|_{W_i})).$$

Ist $p(X) \in K[X]$ irreduzibel, dann tragen zu $\ker(p(\varphi)^m)$ nur die Jordanblöcke mit $p_i(X) = p(X)$ bei, und zwar mit dem rechten Teil des Jordanblocks der Größe $\min\{m, n_i\} \cdot \deg(p)$. Daraus folgt für alle irreduziblen Polynome $p(X) \in K[X]$ und $m \in \mathbb{N}_0$

$$\dim_K(\ker(p(\varphi)^m) = \sum_{\substack{1 \leq i \leq s \\ p_i(X) = p(X)}} \min\{m, n_i\} \cdot \deg(p).$$

Der Wert auf der linken Seite ist unabhängig von der gewählten Basis, welche die Jordannormalform anzeigt. Aus der rechten Seite kann man das Tupel der n_i durch doppeltes nehmen der Differenz bestimmen. Sei $a_n(p)$ die Anzahl der Jordanblöcke $J(p(X)^n)$. Dann ist

$$d_m(p) := \dim_K(\ker(p(\varphi)^m) - \dim_K(\ker(p(\varphi)^{m-1})) = \deg(p) \cdot \sum_{i \geq m} a_i(p)$$

und

$$a_m(p) = \frac{d_m(p) - d_{m+1}(p)}{\deg(p)}.$$

□

9.4. **Was im nicht-zerfallenden Fall passiert.** Falls ein Faktor $p(X)$ des charakteristischen Polynoms von Grad ≥ 2 ist, so argumentiert man wie gehabt, aber mit

$$W = \mathrm{im}(p(\psi)) \subseteq V.$$

Es gilt wieder $\dim(W) < \dim(V)$, denn das Minimalpolynom von $\psi|_W$ kommt mit einem um 1 verminderten Exponenten aus. Man wählt wieder eine Basis von W und liftet den jeweils ersten Vektor eines Jordanblocks a_i zu einem b_i mit $p(\psi)(b_i) = a_i$.

Sodann analysiert man wieder den Schnitt mit dem Kern. Jetzt kommt der Unterschied. Auf $\ker(p(\psi))$ operiert der Polynomring durch den Quotienten

$$K[X] \to K[X]/(p(X)) =: L$$

welcher eine Körpererweiterung von K ist, in der erzwungenermaßen das Polynom $p(X)$ eine Nullstelle hat, nämlich das Bild von X in L! Dieser Körper beschreibt neue Skalare, die auf dem K-Vektorraum $\ker(p(\psi))$ operieren und daraus in verträglicher Weise einen L-Vektorraum machen (die Skalare $K \subseteq L$ vermöge der Bilder konstanter Polynome operieren wie gehabt).

Wir suchen nun eine Basis von $\ker(p(\psi))$ als L-Vektorraum, wobei wir die jeweils letzten Vektoren der Form $p(\psi)^{n_i}(b_i)$ zunächst als L-linear unabhängig in $\ker(p(\psi))$ erkennen und dann zu einer Basis ergänzen. Die ergänzten Basisvektoren führen zu Jordanblöcken $J(p(X)) = \Lambda(p(X))$ der Länge 1.

Der Rest des Beweises geht wieder analog wie im Fall eines Linearfaktors $p(X)$.

Übungsaufgaben zu §9

Übungsaufgabe 9.1. Sei $\dim_K(V) = 3$ und $\varphi : V \to V$ ein Endomorphismus. Zeigen Sie, daß in jedem Fall die Jordannormalform bereits durch charakteristisches Polynom $P_\varphi(X)$ und Minimalpolynom $m_\varphi(X)$ von φ bis auf Permutation der Jordanblöcke festgelegt ist.

Übungsaufgabe 9.2. Finden Sie einen K-Vektorraum V und zwei Endomorphismen $\varphi, \psi \in End_K(V)$, so daß $m_\psi(X) = m_\varphi(X)$ und $P_\varphi(X) = P_\psi(X)$ gilt, aber φ und ψ verschiedene Jordannormalform haben. Welches ist die kleinste Dimension $\dim_K(V)$, in der solche Beispiele konstruiert werden können?

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