Einführung in die Algebra

Marc Technau

Marc Technau, Arbeitsgruppe Computeralgebra und Zahlentheorie, Universität Paderborn, Warburger Str. 100, 33098 Paderborn
Email address: technau@math.upb.de
URL: https://www.math.tugraz.at/~mtechnau

2025-01-27 @ 20:16.

Einleitung

Die Vorlesung orientiert sich nicht konkret an einem Buch. Bei der Ausarbeitung dieser Vorlesung waren jedoch die Lehrbücher [2, 6, 33, 37, 48] hilfreich. Ebenfalls hilfreich waren Unterlagen zu einer Vorlesung von Nils Rosehr an der Universität Würzburg, welche auf Unterlagen von Theobald Grundhöfer zu basieren scheinen [20]. Vorlesungsnotizen von Peter Müller (Universität Würzburg) waren ebenfalls hilfreich. Das Buch von Aluffi [2] sei als besonders inspirierend hervorgehoben. Eine hingegen sehr prägnante Darstellung findet man z.B. bei Wolfahrt [48].

Im Laufe des Semesters erhielt ich einige Verbesserungsvorschläge und Hinweise auf Tippfehler. Hierfür sei Felix Halbwedl, Martin Kalck, Adrian Steinmann, Jason Lin und Doris Vogel gedankt. Für die Mitteilung jeweils einer besonders langen Korrekturliste sei insbesondere auch Christoph Raunjak und Nazarii Shkarlat, sowie Gina Pohlenz gedankt.

Wozu Algebra?

Bevor wir uns nun den eigentlichen Themen der Vorlesung zuwenden, soll zunächst exemplarisch auf das Studium der *Algebra* eingestimmt werden.

> „*Algebra is the offer made by the devil to the mathematician. The devil says: 'I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvellous machine.'*“
>
> — Sir Michael Atiyah, OM, FRS, FRSE [3]

Historisch betrachtet erwuchs die Algebra aus der Bestrebung zum Lösen von Gleichungen durch kalkülartiges Anwenden von Rechenregeln. Heutzutage ist es schwierig, Algebra streng einzugrenzen, da diese und die in ihr verwendeten Methoden bereits fast alle anderen Bereiche der Mathematik durchwachsen haben. Wagt man sich trotzdem an die zum Scheitern verurteilte Aufgabe, den Themenkomplex der *Algebra* näher zu fassen, mag man vielleicht sagen, dass man mittlerweile — jedenfalls an der Hochschule — unter „Algebra“ das Lösen von Problemen *mit* (und *mittels*) Struktur versteht. Wir illustrieren dies anhand einiger Beispiele, bei denen wir davon ausgehen, dass Leserinnen und Leser mit der linearen Algebra bereits vertraut sind.

Ausnutzen von Struktur in Problemen

Beispiel (Lineare Gleichungssysteme)**.** Wir betrachten das bekannte Problem, ein lineares Gleichungssystem

$$\begin{cases} a_{11}X_1 + a_{12}X_2 + \ldots + a_{1m}X_m = 0, \\ \vdots \quad\quad \vdots \quad\quad \ddots \quad\quad \vdots \quad \vdots \\ a_{n1}X_1 + a_{n2}X_2 + \ldots + a_{nm}X_m = 0, \end{cases}$$

mit reellen Koeffizienten a_{ij} $(i = 1, \ldots, n,\ j = 1, \ldots, m)$ in m Variablen $X_1, X_2, \ldots, X_m$ zu lösen. Offensichtlich ist[1] $(x_1, x_2, \ldots, x_m) = (0, 0, \ldots, 0)$ trivialerweise eine Lösung und wir interessieren uns primär für „nicht-triviale Lösungen“. In der linearen Algebra sieht man in obigem Gleichungssystem mehr Struktur, als man vielleicht zunächst vermuten würde. In der Tat fasst man die linke Seite des Gleichungssystems als eine Abbildung auf: Einsetzen eines Vektors $\boldsymbol{x} = (x_1, x_2, \ldots, x_m) \in \mathbb{Q}^m$ für die Variablen $X_1, X_2, \ldots, X_m$ liefert links einen Vektor in $\mathbb{Q}^n$ und man fragt sich zur Lösung des Gleichungssystem, welche $\boldsymbol{x}$ unter dieser Abbildung auf den Nullvektor in $\mathbb{Q}^n$ abgebildet werden. Die so erhaltene *lineare(!)* Abbildung

$$f\colon \mathbb{Q}^m \to \mathbb{Q}^n, \quad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix},$$

ist, wie man in der linearen Algebra lernt, strengen Gesetzmäßigkeiten unterworfen. Ist beispielsweise $m > n$, also die Anzahl m der Variablen größer als die Anzahl n der Gleichungen in unserem Gleichungssystem, so folgt aus der bekannten Dimensionstheorie, dass f einen nichttrivialen Kern besitzt. Elemente des Kerns $\ker f = f^{-1}(0, \ldots, 0)$ sind aber genau die Lösungen unseres Gleichungssystems. Man kann also unter der Voraussetzung $m > n$ ohne irgendwelche weitere Kenntnis der Koeffizienten a_{ij} auf die nichttriviale Lösbarkeit des betrachteten Gleichungssystems schließen.

Beispiel (Nullstellenfreiheit der Exponentialfunktion)**.** Wir betrachten die Potenzreihe

$$\sum_{n=0}^{\infty} \frac{1}{n!} z^n.$$

In der Analysis lernt man, dass diese Potenzreihe für alle komplexen Zahlen z konvergiert und ihr Wert mit der (jedenfalls für reelle Argumente) bereits aus der Schule bekannten Exponentialfunktion übereinstimmt. Man erkennt sofort

$$\exp(0) = 1.$$

[1] Beim „Einsetzen“ in (groß geschriebene) Variablen benutzen wir des Öfteren Kleinbuchstaben.

Durch eine leichte Rechnung mit dem binomischen Lehrsatz und der Cauchyschen Formel für das Produkt zweier Potenzreihen bestätigt man die bekannte Formel

$$\exp(z+w) = \exp(z)\cdot\exp(w).$$

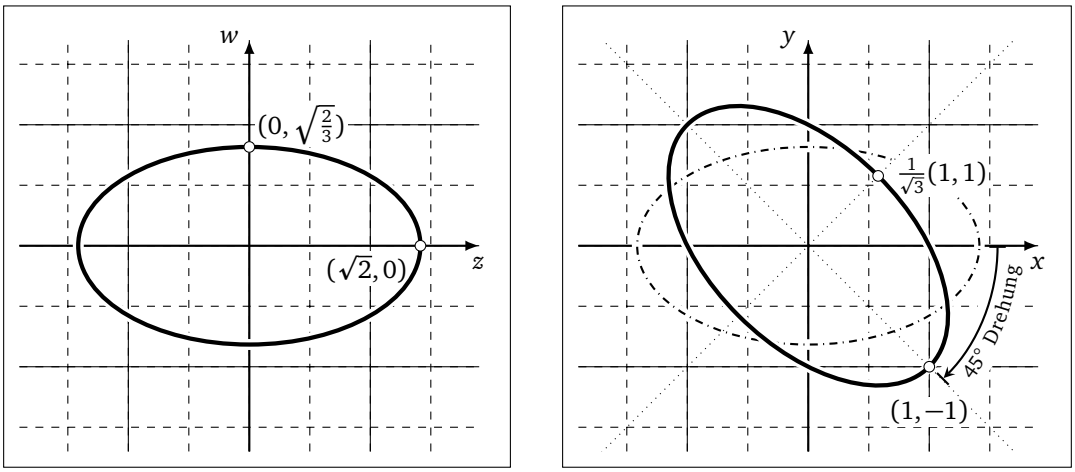
Wir überlegen uns nun, dass aus diesen beiden Formeln, — die offensichtlich additive Struktur der komplexen Zahlen zu multiplikativer Struktur übersetzen —, auf ganz kalkülartige Art und Weise die Nullstellenfreiheit der Exponentialfunktion folgt. Man beachte hierbei, dass die Nullstellenfreiheit der Exponentialfunktion nicht unmittelbar aus ihrer Potenzreihendarstellung ersichtlich scheint: bei der Berechnung einer unendlichen Reihe ist oft nicht klar, ob bei dem hierzu durchzuführenden Grenzprozess mit zunehmend mehr Summanden genug Auslöschung zur Erzeugung einer Nullstelle entsteht, oder eben nicht entsteht. Nun zum Beweis: für beliebiges $z \in \mathbb{C}$ ist

$$1 = \exp(0) = \exp(z-z) = \exp(z+(-z)) = \exp(z)\cdot\exp(-z).$$

Also folgt $\exp(z) \neq 0$, denn anderenfalls stünde auf der rechten Seite der obigen Gleichung ja $0\cdot\exp(-z) = 0$, was aber nicht gleich 1 ist.

Ausnutzen von Symmetrien

Die vorangegangenen beiden Beispiele illustrieren die Schlagkraft von Ausnutzung diverser vorhandener Struktur beim Lösen von Problemen. Die nächsten drei Beispiele illustrieren die Ausnutzung diverser *Symmetrien* (obgleich dies im ersten davon vielleicht nicht unmittelbar klar scheint).



(a) $\tilde{\mathscr{E}}$: Punkte (z,w) mit $\frac{1}{2}z^2 + \frac{3}{2}w^2 = 1$. **(b)** $\mathscr{E}$: Punkte (x,y) mit $x^2 + xy + y^2 = 1$.

Abbildung 1. Die Ellipsen $\tilde{\mathscr{E}}$ und $\mathscr{E}$.

Beispiel (Quadratische Formen)**.** Wir fragen uns, welches geometrische Objekt sich hinter der Menge

$$\mathscr{E} = \{\,(x,y) \in \mathbb{R}^2 : x^2 + xy + y^2 = 1\,\}$$

verbirgt? Wir bemerken hierzu, dass es sich bei

$$X^2+XY+Y^2=\begin{pmatrix}X\\Y\end{pmatrix}^{\mathrm{T}}\underbrace{\begin{pmatrix}1&1/2\\1/2&1\end{pmatrix}}_{=:A}\begin{pmatrix}X\\Y\end{pmatrix}=:q(X,Y)$$

um eine quadratische Form handelt. Wir betrachten nun das Paar $(\mathbb{R}^2,q)$ bestehend aus dem Vektorraum $\mathbb{R}^2$ und der obigen quadratischen Form $q\colon \mathbb{R}^2\to\mathbb{R}$. Das Anwenden eines linearen, orthogonalen Isomorphismus $f\colon\mathbb{R}^2\to\mathbb{R}^2$ übersetzt $(\mathbb{R}^2,q)$ zu dem Paar $(f^{-1}(\mathbb{R}^2),q\circ f)$; wir haben dann ein kommutatives Diagramm

$$\begin{array}{ccc} f^{-1}(\mathbb{R}^2) & \xrightarrow[\sim]{f} & \mathbb{R}^2\,. \\ & {\scriptstyle q\circ f}\searrow \quad \swarrow{\scriptstyle q} & \\ & \mathbb{R} & \end{array}$$

Ist $S\in\mathbb{R}^{2\times 2}$ die Darstellungsmatrix für f bezüglich der Standardbasis des $\mathbb{R}^2$, so ist $f(\boldsymbol{v})=S\boldsymbol{v}$ für alle $\boldsymbol{v}\in\mathbb{R}^2$ und wegen Orthogonalität gilt $S^{\mathrm{T}}=S^{-1}$. Insbesondere ist

$$(q\circ f)(\boldsymbol{v})=f(\boldsymbol{v})^{\mathrm{T}}Af(\boldsymbol{v})=(S\boldsymbol{v})^{\mathrm{T}}AS\boldsymbol{v}=\boldsymbol{v}^{\mathrm{T}}S^{\mathrm{T}}AS\boldsymbol{v}=\boldsymbol{v}^{\mathrm{T}}(S^{-1}AS)\boldsymbol{v}.$$

Wir wählen nun f (und damit S) so, dass $S^{-1}AS$ diagonal ist. Man erkennt, dass

$$S=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\-1&1\end{pmatrix}$$

dies leistet. Dann ist also

$$(q\circ f)(Z,W)=\begin{pmatrix}Z\\W\end{pmatrix}^{\mathrm{T}}S^{-1}AS\begin{pmatrix}Z\\W\end{pmatrix}=\begin{pmatrix}Z\\W\end{pmatrix}^{\mathrm{T}}\begin{pmatrix}1/2&\\&3/2\end{pmatrix}\begin{pmatrix}Z\\W\end{pmatrix}=\tfrac{1}{2}Z^2+\tfrac{3}{2}W^2.$$

Nun ist[2]

$$\mathscr{E}=\{\,\boldsymbol{v}\in\mathbb{R}^2:q(\boldsymbol{v})=1\,\}=f(\{\,\boldsymbol{u}\in\mathbb{R}^2:(q\circ f)(\boldsymbol{u})=1\,\})=f(\tilde{\mathscr{E}}),$$

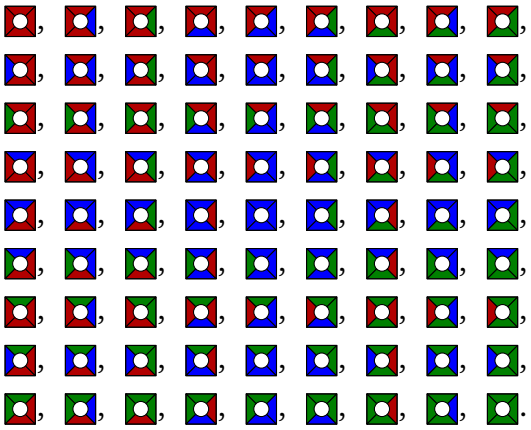
mit der Menge

$$\tilde{\mathscr{E}}=\{\,(z,w)\in\mathbb{R}^2:\tfrac{1}{2}z^2+\tfrac{3}{2}w^2=1\,\}.$$

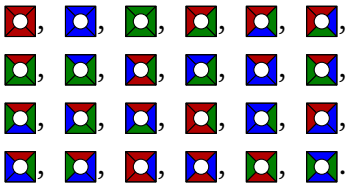
Bei der Menge $\tilde{\mathscr{E}}$ handelt es sich aber offenbar um eine Ellipse mit Mittelpunkt $(0,0)$, welche die Punkte $(\sqrt{2},0)$ und $(0,\sqrt{2}/\sqrt{3})$ enthält. Die Anwendung von f vermittelt eine Drehung von $\tilde{\mathscr{E}}$ um 45° im Uhrzeigersinn.[3] Wegen $\mathscr{E}=f(\tilde{\mathscr{E}})$ klärt das also die Form von $\mathscr{E}$; siehe Abbildung 1.

[2]Das obige Diagramm leitet vielleicht die hier durchgeführte Rechnung an; $\mathscr{E}$ ist das Urbild von $\{1\}$ unter q, lebt also im Diagramm „links unten“. An dieses Urbild kommen wir aber auch (man beachte die Bijektivität von f) heran, wenn wir zunächst das Urbild von $\{1\}$ bezüglich $q\circ f$ berechnen (links oben!) und dieses mit f wieder „nach unten“ holen.

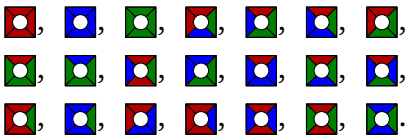
[3]Der Zusatz „im Uhrzeigersinn“ setzt voraus, dass das Koordinatensystem „in der üblichen Art“ gezeichnet wird: Die erste Koordinate wird horizontal von links nach rechts hin wachsend aufgetragen und die zweite Koordinate vertikal von unten nach oben hin wachsend. Vertauscht man beide Achsen, so gebiert sich f als Drehung *entgegen* des Uhrzeigersinns.



(a) Ohne Symmetriebetrachtung.
81 Möglichkeiten.



(b) Drehsymmetrie.
24 Möglichkeiten.



(c) Dreh- und Spiegelsymmetrie.
21 Möglichkeiten.

Abbildung 2. Alle möglichen Färbungen der Seiten eines Quadrats mit bis zu drei verschiedenen zuvor gewählten Farben. Das linke Bild zeigt alle Möglichkeiten, ohne jegliche Identifikation zwischen diesen. Bei den beiden rechten Bildern wurden Färbungen, die durch gewisse Symmetrieoperationen ineinander überführt werden können, zusammengefasst. Pro Klasse von äquivalenten Färbungen wurde hier jeweils nur eine (willkürlich gewählte) Färbung gezeichnet.

Beispiel (Färbungen und Symmetrien)**.** Wir fragen nun auf wie viele Arten man die Seiten eines Quadrates mit drei Farben färben kann. Ohne weitere Einschränkungen sind dies offenbar

$$\{\text{Anzahl der Farben}\}^{\{\text{Anzahl der Seiten}\}} = 3^4 = 81.$$

Falls man nun verschiedene Färbungen als identisch betrachtet, wenn diese durch eine Drehung ineinander überführt werden können, so erhält man offenbar weniger Färbungen. Beispielsweise entstehen aus der Färbung  durch Drehung die drei weiteren Färbungen  ,  und  . Man könnte daher naiv zu der *Vermutung* gelangen, dass die Färbungen unter Drehung in Viererpaare zerfallen und die Gesamtzahl solcher Paare somit durch 81/4 gegeben sei. Dass jene Zahl keine ganze Zahl ist, zeigt natürlich sofort, dass diese *Vermutung falsch* ist. In der Tat gibt es unter Drehsymmetrie auch andere Paarbildungen; Etwa die Färbung  geht durch Drehung nur in sich selbst über, und die Färbung  lässt sich nur zusätzlich zur zweiten Färbung drehen. Eine vorsichtige Betrachtung zeigt, dass es 24 unter Drehung verschiedene Färbungen der Seiten eines Quadrates mit drei Farben gibt.
Lässt man zusätzlich noch Spiegelungen zu, so erhält man abermals weniger Färbungen. Beispielsweise die beiden Färbungen und lassen sich nicht durch

Drehungen des Quadrates ineinander überführen, wohl aber durch eine Spiegelung. Eine weitere vorsichtige Zählung ergibt 21 verschiedene Färbungen. (Für eine Auflistung der Färbungen siehe Abbildung 2.)

Beispiel (Nullstellen von Polynomen)**.** Wir betrachten das Problem, zu gegebenen komplexen Zahlen b und c, die Gleichung

$$X^2 + bX + c = 0$$

zu lösen. Aus der Schule ist bekannt, dass jede Wahl eines Vorzeichens für „±“ in

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

eine Lösung stiftet und auch jede Lösung so erhalten wird. Macht man sich nun zur Aufgabe, Lösungen von

$$X^4 - 14X^2 + 4 = 0$$

zu bestimmen, so kommt man vielleicht auf die Lösung

$$\sqrt{2} + \sqrt{3 + \sqrt{5}}.$$

Mit Blick auf Rolle von Vorzeichen in der vorangegangenen Überlegung, mag man sich vielleicht fragen, ob es sich auch bei

$$\sqrt{2} + \sqrt{3 - \sqrt{5}}.$$

um eine Lösung handelt. Das ist nicht der Fall, hingegen ist aber

$$\sqrt{2} - \sqrt{3 - \sqrt{5}}$$

eine Lösung. Es liegt nahe, zu vermuten, dass Nullstellen von Polynomen auch gewissen „Symmetrien“ unterworfen sind. Nähere Untersuchungen hierzu sind Gegenstand der Vorlesung „Algebra“ [45]. Es sei hier nur erwähnt, dass die Symmetrien der Nullstellen von $X^4 - 14X^2 + 4$ viel mit den Symmetrien eines nicht quadratischen Rechtecks gemein haben (siehe Abbildung 3).

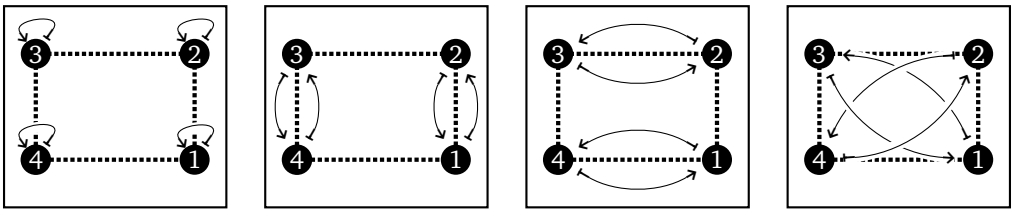


Abbildung 3. Symmetrien eines nicht quadratischen Rechtecks: Triviale Symmetrie, je eine Geradenspiegelung pro Mittelachse und eine Halbwinkeldrehung um den Mittelpunkt.

Inhaltsverzeichnis

Teil 1

Gruppentheorie

KAPITEL 1

Gruppen

Mit diesem Kapitel beginnen wir unseren Streifzug durch die fabelhaft starre Welt der Algebra. Wir führen den Gruppen-Begriff ein und stellen erste Untersuchungen zur Arithmetik in Gruppen. Viel des hier besprochenen Materials dürfte den Leserinnen und Lesern bereits aus der *linearen Algebra* bekannt sein. Der eigentliche Korpus der Theorie erschließt sich uns hingegen erst ab Kapitel 2, wenn wir strukturerhaltende Abbildungen zwischen Gruppen untersuchen.

1.1. Der Gruppen-Begriff

Es sei G eine Menge und $\circ\colon G \times G \to G$ eine Abbildung. Wir nennen $\circ$ auch ***(binäre, innere) Verknüpfung***. Anstatt der sonst üblichen Schreibweise $\circ(a, b)$ für die Auswertung von $\circ$ bei $(a, b) \in G$ benutzen wir im Folgenden die ***Infix-Schreibweise*** $a \circ b$. Wir nennen $\circ$ ***assoziativ***, falls für alle $a, b, c \in G$ die Gleichung[1]

$$(a \circ b) \circ c = a \circ (b \circ c)$$

erfüllt ist. Für eine assoziative Verknüpfung $\circ\colon G \times G \to G$ und $a_1, a_2, \ldots, a_n \in G$ mit $n \geq 2$ definieren wir

$$a_1 \circ a_2 \circ \ldots \circ a_n := (\ldots (a_1 \circ a_2) \circ \ldots) \circ a_n.$$

Man kann sich überlegen, dass man hierbei auch jede andere gültige Klammerung hätte verwenden können, zum Beispiel gilt für $a, b, c, d \in G$

$$((a \circ b) \circ c) \circ d = (a \circ b) \circ (c \circ d) = a \circ (b \circ (c \circ d)) = \ldots \quad \text{(etc.)}.$$

Eine ***Gruppe*** $(G, \circ)$ ist eine Menge G zusammen mit einer Verknüpfung $\circ\colon G \times G \to G$, welche den folgenden Axiomen genügt:

(1) Für alle $a, b, c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$;
(2) Es existiert ein $e \in G$ derart, dass für alle $a \in G$ die Gleichungen

$$a \circ e = a \quad \text{und} \quad e \circ a = a$$

gelten;

[1] In der sonst üblichen Schreibweise $\circ(a, b)$ hätte die angesprochene Gleichung die Gestalt $\circ(\circ(a, b), c) = \circ(a, \circ(b, c))$. — Sehr unübersichtlich!

(3) Für jedes $a \in G$ gibt es ein $b \in G$ mit

$$a \circ b = e \quad \text{und} \quad b \circ a = e,$$

wobei e Eigenschaft (2) erfülle.

Wir unterdrücken oft den Bezug auf die innere Verknüpfung $\circ$ und sprechen nur von „der Gruppe G“ anstatt $(G, \circ)$, benutzen aber auch gelegentlich letztere Notation, wenn eine explizite Benennung der Verknüpfung angemessen scheint.

Man kann die obigen Axiome auch abschwächen[2] und dennoch denselben Gruppen-Begriff erhalten: In (2) und (3) kann jeweils auf die erste der beiden Gleichungen (oder umgekehrt) verzichtet werden (aber nicht etwa gemischt bei einem nur die erste und beim anderen die zweite) — siehe Aufgabe 1.2.

Wir zeigen gleich (siehe Proposition 1.1), dass e aus (2) eindeutig bestimmt ist. Dieses Element nennt man auch ***neutrales Element (von G)***. Oft schreiben wir 1_G für e (oder 1, wenn der Bezug auf G klar erscheint) und sprechen dann vom ***Einselement (in G)***. Ein zu $a \in G$ gemäß (3) bestimmtes Element b ist ebenfalls eindeutig (siehe erneut Proposition 1.1) und wir notieren dieses als a^{-1} und nennen dieses das ***zu a inverse Element***.

Ist die Menge G endlich, so nennen wir die Gruppe G ***endlich*** und $\#G$ heißt ihre ***Ordnung***.

Erfüllt die Gruppe $(G, \circ)$ zusätzlich noch die folgende Eigenschaft, so nennen wir G ***abelsch***:

(4) Für alle $a, b \in G$ gilt $a \circ b = b \circ a$.

Statt $\circ$ benutzen wir auch häufig andere Symbole wie $\cdot$, $*$ etc. und sprechen von ***multiplikativ geschriebenen*** Gruppen. Bei solchen Gruppen unterdrücken wir auch oft die Verknüpfung und schreiben dann nur ab statt $a \circ b$. Für abelsche Gruppen benutzen wir außerdem häufig (allerdings nicht immer!) auch gerne „Strich-artige Symbole“ wie $+$ oder $\oplus$ und sprechen von ***additiv geschriebenen*** Gruppen. Dann schreiben wir auch 0_G oder nur 0 für 1_G und sprechen vom ***Nullelement (von G)***. Anstatt a^{-1} schreiben wir dann auch $-a$.

Proposition 1.1 (Rechenregeln in Gruppen)**.** *Es sei $(G, \circ)$ eine Gruppe. Ferner seien $a, b, x, y \in G$. Dann gelten die folgenden Aussagen:*

(1) Es gibt genau ein Element $e \in G$, welches dem Gruppenaxiom (2) genügt. (Dies rechtfertigt die Schreibweise 1_G.)

*(2) (**Kürzungsregel**) Aus $a \circ x = a \circ y$ oder $x \circ a = y \circ a$ folgt $x = y$.*

(3) Zu jedem $a \in G$ gibt es genau ein $b \in G$, welches dem Gruppenaxiom (3) genügt. (Dies rechtfertigt die Schreibweise a^{-1}.)

*(4) (**Hemd–Jacke-Regel**) Es gilt $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.*

*(5) (**Doppelte Inversion**) Es gilt $(a^{-1})^{-1} = a$.*

[2] Ein solches schwächeres Axiomensystem ist natürlich nützlich, um leichter prüfen zu können, ob es sich bei einem gegebenen Objekt um eine Gruppe handelt, ist aber für die Entwicklung der Theorie etwas umständlicher, da man zunächst weniger Rüstzeug an der Hand hat.

(6) *Man definiert* $a^0 := 1_G$ *und induktiv* $a^n = a^{n-1} \circ a$ *für* $n = 1, 2, \ldots$, *sowie* $a^{-n} = (a^{-1})^n$, *wobei* a^{-1} *hier das in* G *zu* a *inverse Element bezeichne. Dann gilt für alle* $n, m \in \mathbb{Z}$ *die Gleichung* $a^n \circ a^m = a^{n+m}$.
(Für eine additiv geschriebene Gruppe $(G, +)$ *benutzen wir statt der hier eingeführten Potenzschreibweise* $0 \cdot a := 0_G$, $n \cdot a := (n-1) \cdot a + a$ *und* $(-n) \cdot a = n \cdot (-a)$. *Dann gilt für alle* $n, m \in \mathbb{Z}$ *die Gleichung* $n \cdot a + m \cdot a = (n+m) \cdot a$.*)*

Beweis. (1) Sind e und e' zwei Elemente von G derart, dass $e \circ a = a = a \circ e$ und $e' \circ a = a = a \circ e'$ für alle a gilt, so erhalten wir unmittelbar $e = e \circ e' = e'$.

(2) Ist etwa $a \circ x = a \circ y$, so erhalten wir

$$\begin{aligned} x = 1_G \circ x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = a^{-1} \circ (a \circ y) \\ = (a^{-1} \circ a) \circ y = 1_G \circ y = y. \end{aligned}$$

Ganz analog schließt man auch aus $x \circ a = y \circ a$ auf $x = y$.

(3) Sind b und b' zwei Elemente mit $a \circ b = 1_G = a \circ b'$, so folgt $b = b'$ unmittelbar aus der eben bewiesenen Kürzungsregel (2).

(4) dank (3) genügt es einzusehen, dass $b^{-1} \circ a^{-1}$ invers zu $a \circ b$ ist. Ganz ausführlich aufgeschrieben sieht dies so aus:

$$\begin{aligned} (b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ (a \circ b)) = b^{-1} \circ ((a^{-1} \circ a) \circ b) \\ = b^{-1} \circ (1_G \circ b) = b^{-1} \circ b = 1_G. \end{aligned}$$

Die Gleichung $(a \circ b) \circ (b^{-1} \circ a^{-1}) = 1_G$ verifiziert man analog.

(5) folgt sofort aus $a \circ a^{-1} = 1_G = a^{-1} \circ a$ und der Eindeutigkeit inverser Elemente im Sinne von (3).

(6) ist nicht schwierig, aber aufwändig und sei daher der interessierten Leserin oder dem interessierten Leser zur freiwilligen Übung überlassen. (Man sollte im Wesentlichen eine Induktion in zwei Variablen führen. Für ähnliche Schlussweisen von diesem Typus betrachte man etwa, wie Landau [36, Satz 6] das Kommutativgesetz in $\mathbb{N}$ beweist.) □

1.2. Beispiele

Im Folgenden geben wir eine Serie von Beispielen. Die ersten paar davon werden uns im Rahmen der Vorlesung noch weiter beschäftigen, während die übrigen Beispiele nur kursorisch behandelt werden und einen Eindruck zur Relevanz der hier noch zu entwickelnden Theorie für andere mathematische Disziplinen geben sollen.

1.2.1. Einfache Beispiele. $(\mathbb{Z}, +)$ ist eine abelsche Gruppe, wobei „+“ hier die bekannte Addition von ganzen Zahlen bezeichne. Eine analoge Aussage gilt jeweils auch für $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$. Dies gilt auch für $(V, +)$ für jeden Vektorraum V zusammen mit der zugehörigen Vektoraddition. Bei $(\mathbb{N}, +)$ handelt es sich nicht um eine Gruppe, wie man leicht einsieht; es gibt nämlich kein Element von $\mathbb{N}$, welches die Rolle des neutralen Elements übernehmen könnte. Ebenfalls $(\mathbb{N}_0, +)$ bildet keine Gruppe. Hier lässt sich zwar 0 die Rolle des neutralen Elements zuordnen, allerdings

gibt es zu $1 \in \mathbb{N}_0$ kein $b \in \mathbb{N}_0$ mit $1 + b = 0$. Auch $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe (es gibt kein zu 2 (multiplikativ) inverses Element in $\mathbb{Z} \setminus \{0\}$). Dafür ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ aber schon eine Gruppe, ja sogar eine abelsche. (Man beachte aber, dass die Verknüpfung hier trotzdem nicht additiv geschrieben wird, um eine Verwechslung mit der auf $\mathbb{Q}$ definierten Addition zu vermeiden.)

1.2.2. Zyklische Gruppen. Sei $n \in \mathbb{N}$ und $C_n = \{0, 1, \ldots, n-1\}$. Wir definieren nun eine Verknüpfung auf C_n durch

$$\oplus\colon C_n \times C_n \to C_n, \quad (a, b) \mapsto \begin{cases} a + b & \text{falls } a + b < n, \\ a + b - n & \text{falls } a + b \geq n. \end{cases}$$

Dann lässt sich leicht nachrechnen, dass es sich bei $(C_n, \oplus)$ um eine abelsche Gruppe mit genau n Elementen handelt (siehe auch Abbildung 4; der Nachweis der Assoziativität ist etwas mühselig — siehe auch Seite 34, wo wir diese auf konzeptionellere Weise aus der Assoziativität der Addition auf $\mathbb{Z}$ folgern). Das neutrale Element ist hier 0. Dieses ist natürlich auch zu sich selbst invers ($0 + 0 = 0$). Das zu $a \in C_n$, $a \neq 0$, inverse Element ist $n - a$, wobei die hier benutzte Subtraktion als Subtraktion ganzer Zahlen zu verstehen ist. Die Gruppe $(C_n, \oplus)$ heißt auch die ***zyklische Gruppe der Ordnung n***. In § 1.4 studieren wir diese noch näher und definieren, wann eine Gruppe zyklisch heißt. Mit Korollar 2.8 klärt sich später noch der hiesige Gebrauch des bestimmten Artikels.

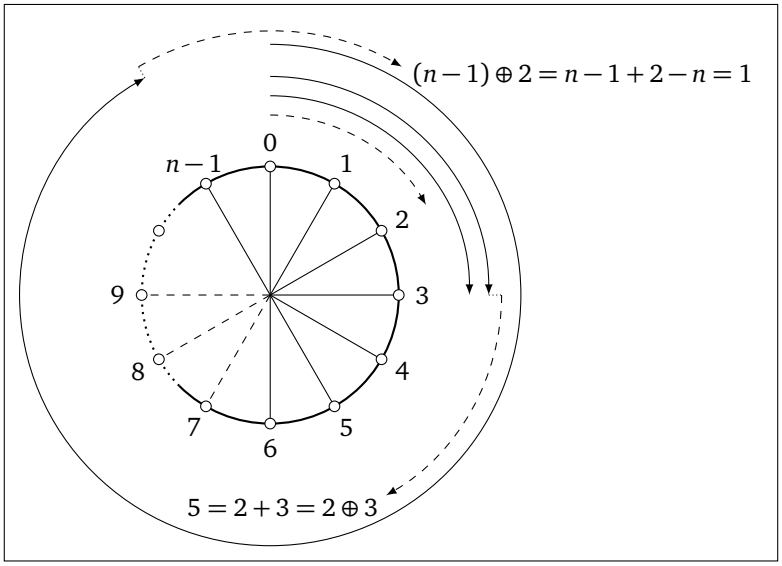


Abbildung 4. Zur Arithmetik in $(C_n, \oplus)$: $a \oplus b$ ist gegeben durch $a + b$, solange kein Übertrag entsteht (d.h. solange das Ergebnis kleiner als n ausfällt). In den übrigen Fällen wird noch n subtrahiert, um wieder ein Element von $C_n = \{0, 1, \ldots, n-1\}$ zu erhalten.

Beispiel. Wählt man $n = 12$ und denkt sich für 0 in C_{12} eine 12 geschrieben, so entspricht die Verknüpfung in C_{12} genau der Arithmetik, die man von den Stundenzeigern auf analogen Uhren kennt. Man veranschauliche sich diese Interpretation auch anhand von Abbildung 4.

1.2.3. Symmetrische Gruppen. Es sei M eine beliebige Menge und

$$\mathrm{Sym}(M) \coloneqq \{\text{bijektive Abbildungen } \sigma\colon M \to M\}.$$

Dann bildet $\mathrm{Sym}(M)$ zusammen mit der bekannten Verkettung von Abbildungen

$$\circ\colon \mathrm{Sym}(M) \times \mathrm{Sym}(M) \to \mathrm{Sym}(M), \quad (\sigma, \tau) \mapsto (m \mapsto \sigma(\tau(m)))$$

eine Gruppe, die ***symmetrische Gruppe von M***. Das neutrale Element ist hier die identische Abbildung $\mathrm{id}_M\colon M \to M$, $m \mapsto m$. Das zu $\sigma \in \mathrm{Sym}(M)$ inverse Element ist genau die Umkehrabbildung zu σ.
Für den Spezialfall $M = \{1, 2, \ldots, n\}$ benutzen wir auch die Bezeichnung $\mathfrak{S}_n \coloneqq \mathrm{Sym}(\{1, 2, \ldots, n\})$. In Kapitel 4 untersuchen wir die Gruppen $\mathfrak{S}_n$ noch näher.

Beispiel. Die Gruppe $\mathfrak{S}_2 = \mathrm{Sym}(\{1, 2\})$ enthält genau zwei Elemente, nämlich die beiden Bijektionen

$$\mathrm{id}_{\{1,2\}}\colon\ 1 \circlearrowright\ 2 \circlearrowright \qquad \text{und} \qquad \tau_{12}\colon\ 1 \rightleftarrows 2\,.$$

Man sieht sofort, dass es sich hierbei um eine abelsche Gruppe handelt.

Beispiel. Die Gruppe $\mathfrak{S}_3 = \mathrm{Sym}(\{1, 2, 3\})$ enthält genau sechs Elemente, nämlich die sechs Bijektionen

$$\mathrm{id}_{\{1,2,3\}}\colon\ 1 \circlearrowright\ 2 \circlearrowright\ 3 \circlearrowright, \qquad \tau_{12}\colon\ 1 \rightleftarrows 2\ \circlearrowright\ 3, \qquad \tau_{23}\colon\ 1 \circlearrowright\ 2 \rightleftarrows 3,$$

$$\sigma_{123}\colon\ 1 \to 2 \to 3 \to 1, \qquad \tau_{13}\colon\ 1 \rightleftarrows 2 \circlearrowright\ 3, \qquad \sigma_{132}\colon\ 1 \to 3 \to 2 \to 1.$$

Man berechnet etwa

$$\tau_{13} \circ \tau_{12} = \begin{array}{ccc} 1 & 2 & 3 \\ & \searrow\!\swarrow & \downarrow \\ 1 & 2 & 3 \\ & \swarrow\!\searrow & \\ 1 & 2 & 3 \end{array} = \sigma_{123} \neq \sigma_{132} = \begin{array}{ccc} 1 & 2 & 3 \\ & \downarrow\!\searrow & \\ 1 & 2 & 3 \\ & \searrow\!\downarrow & \\ 1 & 2 & 3 \end{array} = \tau_{12} \circ \tau_{13}.$$

Die Gruppe $\mathfrak{S}_3$ ist also *nicht* abelsch. Analog sieht man, dass $\mathfrak{S}_n$ für *kein* $n \geq 3$ abelsch ist.

1.2.4. Direkte Produkte von Gruppen. Sind $(G, \circ)$ und $(H, *)$ beliebige Gruppen, so lässt sich auch das mengentheoretische kartesische Produkt $G \times H = \{(g, h) : g \in G,\, h \in H\}$ mit einer Gruppenstruktur ausstatten:

$$(G \times H) \times (G \times H) \to G \times H, \quad ((g, h), (g', h')) \mapsto (g \circ g', h * h').$$

Das neutrale Element ist hier offenbar durch $1_{G\times H} = (1_G, 1_H)$ gegeben und das zu $(g, h) \in G \times H$ inverse Element ist $(g, h)^{-1} = (g^{-1}, h^{-1})$. Durch direkte Produkte

lassen sich aus bekannten Gruppen neue Gruppen konstruieren. Später werden wir so auch kompliziertere Gruppen in kleinere „Bausteine“ zerlegen (siehe beispielsweise Satz 5.3).

Beispiel. Die Gruppe $V = C_2 \times C_2$ heißt ***Kleinsche Vierergruppe***. Diese besteht aus genau vier Elementen. Wir schreiben in diesem Beispiel „$\tilde{\oplus}$“ für die Verknüpfung in V, behalten uns aber vor, diese später anders zu notieren. Die Verknüpfung von Elementen in V sieht wie folgt aus:

$$\begin{array}{c|ccc} \tilde{\oplus} & \dots & y & \dots \\ \hline \vdots & \ddots & \vdots & \\ x & \dots & x+y & \dots \\ \vdots & & \vdots & \ddots \end{array} : \qquad \begin{array}{c|cccc} \tilde{\oplus} & (0,0) & (0,1) & (1,0) & (1,1) \\ \hline (0,0) & (0,0) & (0,1) & (1,0) & (1,1) \\ (0,1) & (0,1) & (0,0) & (1,1) & (1,0) \\ (1,0) & (1,0) & (1,1) & (0,0) & (0,1) \\ (1,1) & (1,1) & (1,0) & (0,1) & (0,0) \end{array}.$$

Man beachte, dass jedes Element a von V ***selbstinvers*** ist: $a \tilde{\oplus} a = (0,0) = 0_V$. Die Gruppe C_4 aus § 1.2.2 erfüllt dies nicht: Darin sind zwar 0 und 2 beide selbstinvers, jedoch 1 und 3 nicht. (Zum Beispiel: $3 \oplus 3 = 2 \neq 0 = 0_{C_4}$.)

1.2.5. Gruppen in der linearen Algebra. Ist V ein beliebiger Vektorraum über einem Körper K, so bildet

$$\mathrm{GL}(V) = \{\text{bijektive lineare Abbildungen } f\colon V \to V\}$$

zusammen mit der Verkettung von Abbildungen eine Gruppe, die ***allgemeine lineare Gruppe*** (Engl. *general linear group*). Ferner schreiben wir

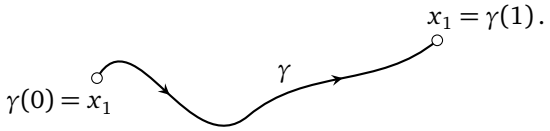
$$\mathrm{GL}_n K = \{\text{invertierbare } n\times n\text{-Matrizen über } K\}.$$

Diese Menge bildet zusammen mit der bekannten Matrixmultiplikation eine Gruppe. Man mag vermuten, dass es sich bei $\mathrm{GL}(K^n)$ und $\mathrm{GL}_n K$ *im Wesentlichen* um „dieselbe“ Gruppe handelt. Mengentheoretisch ist dies natürlich völlig falsch, da es sich bei den zugrundeliegenden Mengen um verschiedene Mengen handelt, allerdings werden wir später noch einen „Gleichheitsbegriff“ für Gruppen (Isomorphie von Gruppen) einführen, bezüglich dessen wir $\mathrm{GL}(K^n)$ und $\mathrm{GL}_n K$ identifizieren können. Den hierfür relevanten Homomorphie-Begriff untersuchen wir in Kapitel 2.
Aus der linearen Algebra kennt man auch noch weitere Matrizengruppen:

$$\mathrm{SL}_n K = \{A \in K^{n\times n} : \det(A) = 1_K\},$$
$$\mathrm{O}_n = \{A \in \mathbb{R}^{n\times n} : A^{\mathrm{T}} A = 1_{\mathrm{GL}_n \mathbb{R}}\},$$
$$\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n \mathbb{R}.$$

Die den Elementen A dieser Gruppe zugeordneten linearen Abbildungen $K^n \to K^n$, $x \mapsto Ax$, zeichnen sich dadurch aus, gewisse zusätzliche Strukturen zu erhalten. Für $\mathrm{SL}_n \mathbb{R}$ ist dies etwa das Erhalten von Volumen und Orientierung. Die den Elementen von O_n zugeordneten linearen Abbildungen erhalten Abstände bezüglich der Euklid-Norm und für SO_n wird noch zusätzlich die Orientierung erhalten.

1.2.6. Fundamentalgruppen topologischer Räume. Es sei $X \neq \emptyset$ ein topologischer Raum. Eine stetige Abbildung $\gamma\colon [0,1] \to X$ nennen wir einen ***Weg (in X)*** (siehe auch Abbildung 7 (a)). Der Raum X heißt ***wegzusammenhängend***, falls es für je zwei Punkte $x_0, x_1 \in X$ stets einen Weg $\gamma\colon [0,1] \to X$ gibt, der diese Punkte verbindet (d.h. es gelte $\gamma(0) = x_0$ und $\gamma(1) = x_1$):



Zwei Wege $\gamma_0, \gamma_1\colon [0,1] \to X$ mit denselben Endpunkten ($\gamma_0(0) = \gamma_1(0)$, $\gamma_0(1) = \gamma_1(1)$) heißen ***homotop (in X)***, falls sich diese stetig ineinander deformieren lassen, d.h. falls es eine stetige Abbildung $H\colon [0,1]^2 \to X$ mit den folgenden Eigenschaften gibt (vgl. Abbildung 5):

- $(t \mapsto H(t,0)) = \gamma_0$,
- $(t \mapsto H(t,1)) = \gamma_1$,
- für alle $s \in [0,1]$ gilt $H(0,s) = \gamma_0(0) = \gamma_1(0)$ und $H(1,s) = \gamma_0(1) = \gamma_1(1)$.

Eine solche Abbildung H heißt ***Homotopie*** zwischen γ_0 und γ_1. Man kann nachrechnen, dass durch den Homotopiebegriff eine Äquivalenzrelation auf der Menge der Wege in X gestiftet wird.

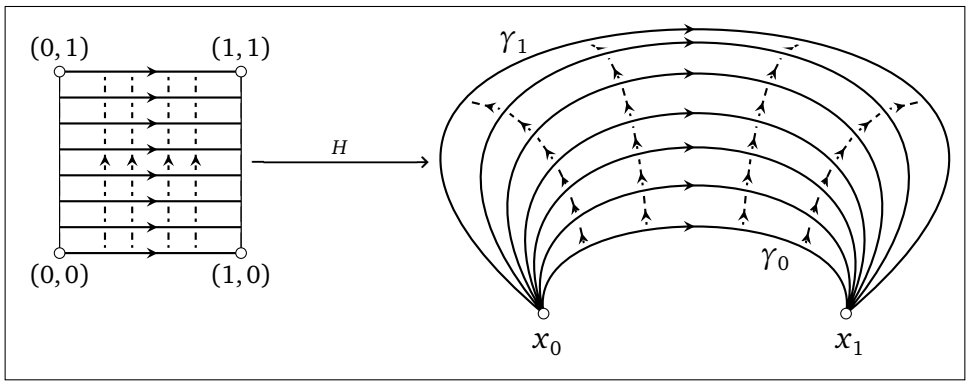


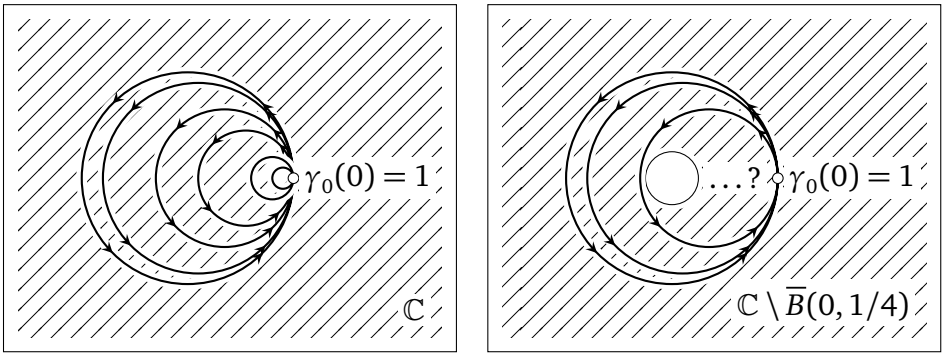
Abbildung 5. Zeichnung einer Homotopie.

Zu zwei Wegen γ_0 und γ_1 mit $\gamma_0(1) = \gamma_1(0)$ (Endpunkt von γ_0 = Startpunkt von γ_1) definiert man deren ***Zusammensetzung*** $\gamma_0 * \gamma_1\colon [0,1] \to X$ durch

$$(\gamma_0 * \gamma_1)(t) = \begin{cases} \gamma_0(2t) & \text{für } 0 \leq t \leq \frac{1}{2}, \\ \gamma_1(2t-1) & \text{für } \frac{1}{2} \leq t \leq 1. \end{cases}$$

Man beachte, dass die Zusammensetzung von drei Wegen nicht assoziativ ist (siehe Abbildung 7 (c)). Dieser Defekt behebt sich gleich durch den Übergang zu Homotopieklassen. Wir gehen nun davon aus, dass X wegzusammenhängend ist und ein

Punkt $x_* \in X$ fest gewählt ist. Das Paar (X, x_*) bezeichnet man auch als ***punktierten Raum*** und x_* als ***Basispunkt***.



(a) In $\mathbb{C}$ ist jeder geschlossene Weg homotop zu einem konstanten Weg.

(b) In $\mathbb{C} \setminus \overline{B}(0, 1/4)$ scheint dies nicht der Fall zu sein.

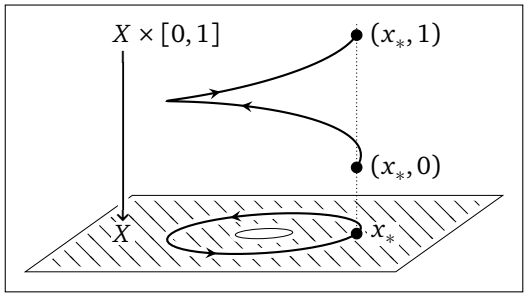
Abbildung 6. Heuristische Überlegung dazu, dass die Fundamentalgruppen $\pi_1(\mathbb{C}, 1)$ und $\pi_1(\mathbb{C} \setminus \overline{B}(0, 1/4), 1)$ echt verschieden zu sein scheinen. (Einen formalen Beweis hierfür liefern wir jedoch nicht.)

Ferner schränken wir unsere Betrachtung nun auf diejenigen Wege γ_0, γ_1 in X ein, deren Anfangs- und Endpunkt mit x_* übereinstimmt. Je zwei solche Wege kann man dann (in beliebiger Reihenfolge) zusammensetzen. Es bezeichne nun $[\gamma_0]$ die Menge aller Wege in X, welche zu γ_0 homotop sind, also die Äquivalenzklasse von γ_0 bezüglich der durch Homotopie gestifteten Äquivalenzrelation. Man kann nachrechnen, dass die Festlegung $[\gamma_0] * [\gamma_1] := [\gamma_0 * \gamma_1]$ unabhängig von der Wahl der Repräsentanten γ_0, γ_1 der auftretenden Äquivalenzklassen ist. Ferner kann man nachrechnen, dass

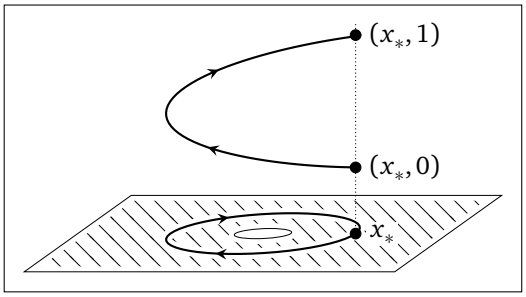
$$\pi_1(X, x_*) = \{ [\gamma] : \text{Wege } \gamma\colon [0,1] \to X \text{ mit } \gamma(0) = x_* = \gamma(1) \}$$

zusammen mit $*$ eine Gruppe bildet. Dabei handelt es sich bei der Klasse $[t \mapsto x_*]$ vom konstanten Weg $t \mapsto x_*$ um das neutrale Element in $\pi_1(X, x_*)$ und das zu $[\gamma] \in \pi_1(X, x_*)$ inverse Element ist $[\gamma^-]$, wo γ^- den Weg $t \mapsto \gamma(1-t)$, welcher γ „in umgekehrter Richtung“ durchläuft, bezeichne. Man beachte in diesem Zusammenhang insbesondere Abbildungen 7 (b), 7 (e) und 7 (f).

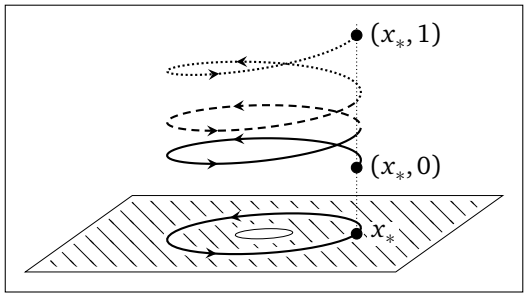
Man bezeichnet $(\pi_1(X, x_*), *)$ als ***Fundamentalgruppe von*** (X, x_*). Fundamentalgruppen wurden 1895 von Poincaré in seiner berühmten Arbeit *„Analysis situs“* eingeführt [41], mit welcher er das mathematische Gebiet der algebraischen Topologie begründete. Die Fundamentalgruppe eines topologischen Raums ist eine wichtige Invariante und kann etwa zur Unterscheidung mancher topologischer Räume gebraucht werden (siehe etwa Abbildung 6). Dies gründet sich insbesondere auf den Umstand, dass die Fundamentalgruppenkonstruktion nicht nur punktierten Räumen (X, x_*) eine Gruppe zuordnet, sondern auch auf Morphismen von punktierten Räumen



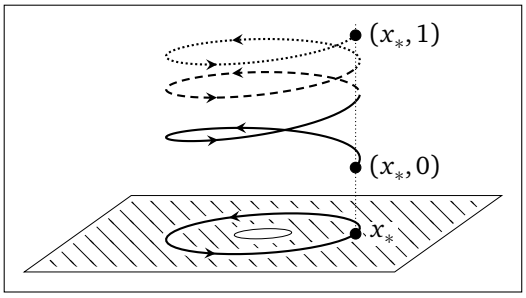
(a) Ein Kreisweg γ.



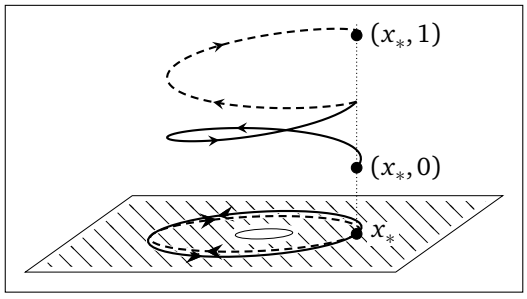
(b) Der zu γ inverse Weg γ^-.



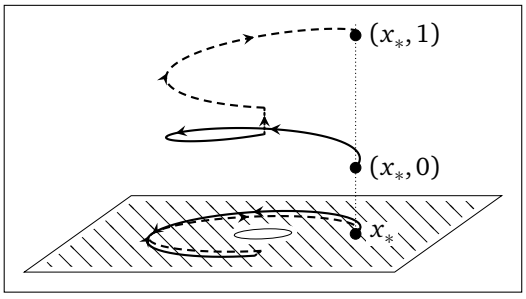
(c) Der Weg $(\gamma * \gamma) * \gamma$.



(d) Der Weg $\gamma * (\gamma * \gamma)$.



(e) Der Weg $\gamma * \gamma^-$. Die Spur dieses Weges ist hier mit Absicht leicht „verwackelt“, da man sonst nur einen Kreis sehen würde, bei dem Richtungspfeile in jeweils entgegengesetzter Richtung angebracht sind.



(f) Hier wird angedeutet, wie eine Homotopie H zwischen $\gamma * \gamma^-$ und dem konstanten Weg $t \mapsto x_*$ zu konstruieren ist:

$$H(t,s) = \begin{cases} \gamma(t) & \text{für } 2t \le 1-s, \\ \gamma^-(t) & \text{für } 2t \ge 1+s, \\ \gamma((1-s)/2) & \text{sonst.} \end{cases}$$

Abbildung 7. Zur Fundamentalgruppe $\pi(X, x_*)$. In den Bildern sieht man die Spuren $\tilde{\gamma}([0,1])$ verschiedener Wege $\tilde{\gamma}$, sowie deren Graphen $\{(\tilde{\gamma}(t), t) : t \in [0,1]\} \subseteq X \times [0,1]$.

geeignet antwortet. Dabei heißt $f : (X, x_*) \to (Y, y_*)$ ***Morphismus von punktierten Räumen***, falls $f : X \to Y$ eine stetige Abbildung ist und den Basispunkt x_* in den Basispunkt y_* überführt: $f(x_*) = y_*$. Nun ist für jeden Weg γ in X die Verkettung

$f \circ \gamma$ ein Weg in Y:

$$[0,1] \xrightarrow{\gamma} X \xrightarrow{f} Y\,.$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\quad \overset{f\circ\gamma}{\smile}$$

Man kann zeigen, dass durch $[\gamma] \mapsto [f \circ \gamma]$ eine wohl-definierte Abbildung zwischen $\pi_1(X, x_*)$ und $\pi_1(Y, y_*)$ gestiftet wird, die wir mit f_* bezeichnen wollen. Man kann zeigen, dass f_* eine strukturerhaltende Abbildung ist (ein Gruppenhomomorphismus; siehe Kapitel 2 für die Definition). Ferner gilt

$$(\mathrm{id}_X \colon (X, x_*) \to (X, x_*))_* = \mathrm{id}_{\pi_1(X,x_*)}$$

und für jeden weiteren Morphismus $g \colon (Y, y_*) \to (Z, z_*)$ zwischen punktierten Räumen gilt $(g \circ f)_* = g_* \circ f_*$:

$$\begin{array}{ccc} & (Y,y_*) & \\ {\scriptstyle f}\nearrow & & \searrow{\scriptstyle g} \\ (X,x_*) & \xrightarrow{g\circ f} & (Z,z_*)\,, \end{array} \qquad \begin{array}{ccc} & \pi_1(Y,y_*) & \\ {\scriptstyle f_*}\nearrow & & \searrow{\scriptstyle g_*} \\ \pi_1(X,x_*) & \xrightarrow{g_*\circ f_*} & \pi_1(Z,z_*)\,. \end{array}$$

Diese Eigenschaften ermöglichen es, gewisse Fragestellungen im Bereich der Topologie zu Problemen in der Gruppentheorie zu transportieren.

Wir *skizzieren*, wie sich etwa ein Beweis des ***Fundamentalsatzes der Algebra***, dass jedes nicht-konstante Polynom mit komplexen Koeffizienten in den komplexen Zahlen $\mathbb{C}$ eine Nullstelle besitzt, führen lässt. Für Details sei auf die Darstellung bei Hatcher [23, § 1.1] verwiesen. Man kann zeigen, dass die Fundamentalgruppe $\pi_1(\mathbb{S}^1, 1)$ der Sphäre $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$ gleich[3] $(\mathbb{Z}, +)$ ist. Ein hypothetisch existentes nullstellenfreies, komplexes Polynom f vom Grad $n \geq 1$ stiftet via

$$\gamma_r \colon [0,1] \to \mathbb{S}^1, \quad t \mapsto \frac{|f(r)|}{f(r)} \frac{f(r\exp(2\pi \mathrm{i}\, t))}{|f(r\exp(2\pi \mathrm{i}\, t))|},$$

ein Element $[\gamma_r] \in \pi_1(\mathbb{S}^1, 1)$. Für $r = 0$ ist γ_r die konstante Abbildung $t \mapsto 1$ und $[\gamma_0]$ das Nullelement von $\pi_1(\mathbb{S}^1, 1) = \mathbb{Z}$. Für große $r > 0$ kann man zeigen, dass γ_r und die Abbildung $\mathbb{S}^1 \to \mathbb{S}^1$, $z \mapsto z^n$, homotop sind und daraus lässt sich $[\gamma_r] = \pm n$ zeigen (hier sei daran erinnert, dass $\pi_1(\mathbb{S}^1, 1)$ „gleich“ $\mathbb{Z}$ ist). Allerdings sind γ_0 und γ_r homotop und damit folgt $0 = [\gamma_0] = [\gamma_r] = \pm n$, im Widerspruch zu $n \geq 1$.

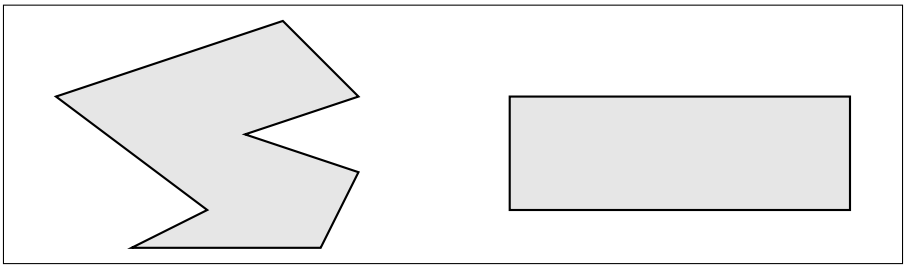
1.2.7. Weitere Gruppen in der Topologie. Die Topologie kennt auch noch viele weitere Theorien, in welcher Gruppen eine fundamentale[4] Rolle spielen (z.B. singuläre Homologie). Verwandt sind auch Kohomologietheorien, wie etwa die de Rham Kohomologie aus der Differentialgeometrie, welche sich der Aktion der Cartan-Ableitung auf Differentialformen variierenden Grades bedient. Hierbei entstehen allerdings

[3] Gemeint ist hier eigentlich „isomorph zu $(\mathbb{Z}, +)$ ist“, aber die hierfür nötige Sprache führen wir erst in Kapitel 2 ein.

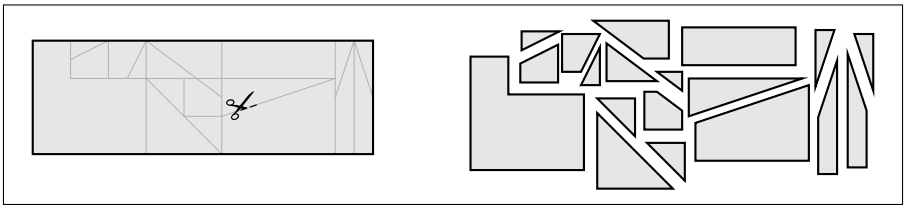
[4] Das offensichtliche Wortspiel ist an dieser Stelle durchaus beabsichtigt.

schon reichhaltigere Strukturen als Gruppen. (Details hierzu sind ggf. aus der *Analysis 3* bekannt; alternativ konsultiere man [31].)

1.2.8. Gruppen in der Geometrie. Wir betrachten zwei flächengleiche Polygone im $\mathbb{R}^2$, wie etwa in Abbildung 8 (a). Der ***Satz von Wallace–Bolyai–Gerwien*** besagt nun, dass man das eine Polygon geeignet durch geradlinige Schnitte in Teilpolygone zerschneiden lässt, sodass man das zweite Polygon aus den entstandenen Stücken durch Rotation und Verschiebung zusammensetzen kann; Siehe Abbildung 8 (b). (Für eine hübsche Animation hierzu, siehe [16].)



(a) Zwei flächengleiche Polygone.



(b) Illustration zum *Satz von Wallace–Bolyai–Gerwien*: Hier wird das obige Rechteck derart zerschnitten, dass sich aus den Teilstücken das zweite Polygon von oben zusammensetzen lässt.

Abbildung 8. Zum *Satz von Wallace–Bolyai–Gerwien*.

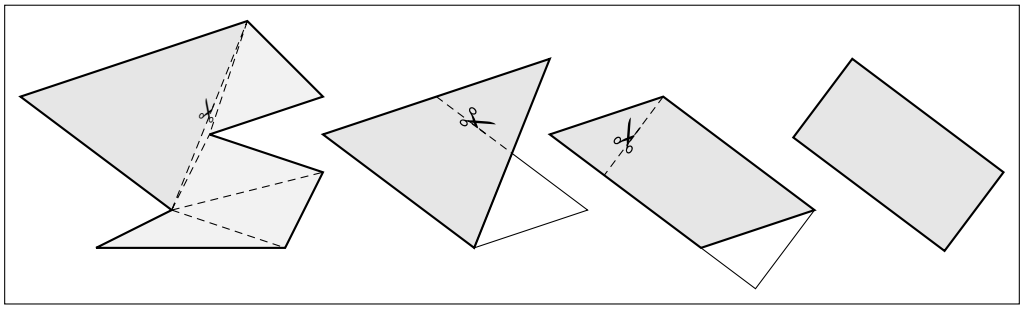


Abbildung 9. Eine mögliche Triangulierung des Polygons aus Abbildung 8 (a) (oben) und Transformation eines der auftretenden Dreiecke in ein Rechteck durch Zerschneiden.

Wir wollen uns nicht um einen streng formalen Beweis dieser Aussage bemühen und verweisen für Details auf [22, Ch. 5, § 24]. Dennoch skizzieren wir grob, wie man zu dieser Aussage gelangen kann. Wir betrachten eines der beiden Polygone und zerlegen dieses durch Schnitte in lauter Dreiecke, wie in Abbildung 9. (Dass es eine solche Zerlegung, eine sogenannte ***Triangulierung***, stets gibt, bedarf selbstverständlich eines Beweises. Wir verzichten allerdings darauf.)

Aus den Dreiecken lassen sich durch weitere Schnitte nun Parallelogramme und schließlich Rechtecke erzeugen. Dieser Prozess wird in Abbildung 9 dargestellt.

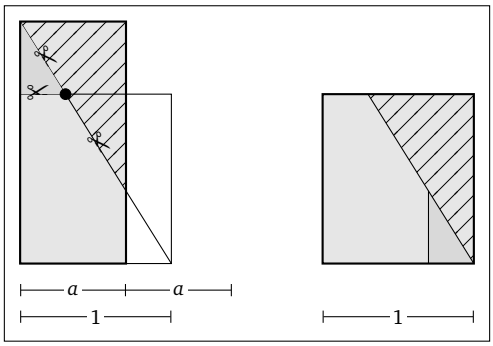


Abbildung 10. Transformation eines Rechtecks mit Seitenlänge $a \in [1/2, 1]$ zu einem flächengleichen Rechteck mit einer Seite der Länge 1 durch Zerschneidung.

Zum Beweis des Satzes von Wallace–Bolyai–Gerwien genügt es dann einzusehen, dass sich jedes Rechteck so zerschneiden lässt, dass man aus den Teilen ein flächengleiches Rechteck zusammensetzen kann, dessen eine Seite Länge 1 hat, siehe Abbildung 10. (Die in Abbildung 10 skizzierte Zerlegung funktioniert nur für $1/2 \leq a \leq 1$, da der schwarz markierte Punkt für andere Werte von a nicht mehr im Inneren des grauen Rechtecks liegt. Dieser Zuständ lässt sich allerdings, falls nötig, leicht durch zusätzliche Zerschneidungen herstellen. Hierzu gilt es nur zu beachten, dass man ein jedes Rechteck mit Seitenlängen $a, b > 0$ an einer Seite senkrecht halbieren kann und aus den Hälften ein Rechteck mit Seitenlängen $2a$, $b/2$ bzw. $a/2$, $2b$ zusammenfügen kann. Durch geeignete Iteration dieses Prozesses erhält man ein Reckteck mit einer Seitenlänge zwischen $1/2$ und 1.)

David Hilbert fragte im Jahr 1900, ob ein analoger Zerschneidungssatz, wie der von Wallace–Bolyai–Gerwien auch in drei Dimensionen bestand habe (siehe [25, S. 301f.])? Diese Frage wurde ein Jahr später von Max Dehn [15] verneinend beantwortet: Ein Würfel lässt sich nicht durch Zerschneidung entlang von Ebenen in (endlich viele) Stücke zerlegen, welche sich zu einem volumengleichen, regulären Tetraeder zusammensetzen lassen (Abbildung 11). Dehns Beweis, für den wir auf Hartshorne [22, Ch. 5, § 27] verweisen, ordnet jedem Polyeder P ein Element $\delta(P)$, der sogenannten ***Dehn-Invariante*** einer bestimmten abelschen Gruppe G zu. Für jene

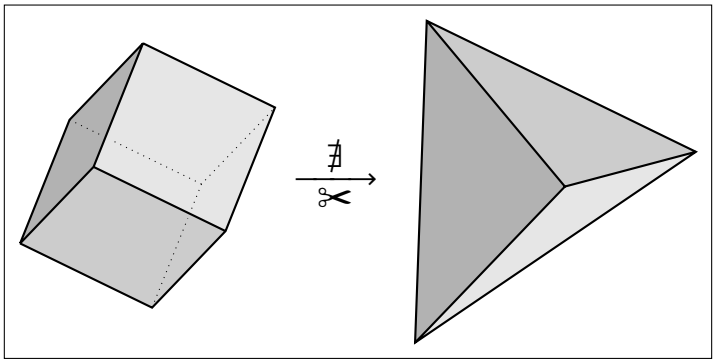


Abbildung 11. Ein Würfel und ein regulärer Tetraeder.

Zuordnung zeigt man dann, dass zwei durch Zerschneidung ineinander überführbare Polyeder dieselbe Dehn-Invariante besitzen. (In umgekehrter Richtung zeigte Sydler [44] im Jahr 1965, dass das gleiches Volumen und gleiche Dehn-Invariante sogar *hinreichend* für die Zerlegbarkeit von Polyedern ineinander sind. Das Volumen und die Dehn-Invariante *charakterisieren* somit den besprochenen Zerlegungsbegriff vollständig.) Anschließend folgt Dehns Satz durch die Beobachtung, dass Würfel und Tetraeder verschiedene Dehn-Invarianten besitzen.

Bei der oben erwähnten Gruppe G handelt es sich um das ***Tensorprodukt*** $G = \mathbb{R} \otimes_{\mathbb{Z}} (\mathbb{R}/\pi\mathbb{Z})$. Diese Gruppe lässt sich beschreiben als Menge der endlichen formalen Summen[5]

$$(a_1, \theta_1) + \ldots + (a_n, \theta_n)$$

mit $n \in \mathbb{N}_0$, $a_1, \ldots, a_n \in \mathbb{R}$, $\theta_1, \ldots, \theta_n \in \mathbb{R}/\pi\mathbb{Z}$,[6] wobei für diese formalen Summen zusätzlich die folgenden beiden Rechenregeln postulliert werden:

$$(a, \theta) + (a', \theta) = (a + a', \theta), \quad (a, \theta) + (a, \theta') = (a, \theta + \theta').$$

Die Addition zweier formaler Summen wird auf die offensichtlichen Art und Weise erklärt, wobei keine Rücksicht auf die Reihenfolge der Summanden genommen wird. (Wie man die Gruppe $\mathbb{R} \otimes_{\mathbb{Z}} (\mathbb{R}/\pi\mathbb{Z})$ formal konstruiert und wie man der Bezeichnung „formale Summen“ eine stichhaltige Bedeutung gibt, wollen wir hier nicht ausführen.)

Die *Dehn-Invariante* $\delta(P)$ *eines Polyeders* P bildet man nun wie folgt: Jede Kante K von P hat eine Länge a_K und entsteht durch das Aneinandertreffen zweier Seitenflächen des Polyeders. Zwischen diesen Seiten wird ein Winkel θ_K eingeschlossen. (Man messe den Winkel im Inneren des Polyeders.) Nun definiert $\delta(P)$ als die formale Summe

$$\delta(P) := \sum_K (a_K, \theta_K),$$

[5] $a \otimes \theta$ wäre hier die übliche Notation für (a, θ).

[6] Die Gruppe $\mathbb{R}/\pi\mathbb{Z}$ sollte man sich in Analogie zu § 1.2.2 als „$\mathbb{R}$ mit Reduktion um ganzzahlige Vielfache von π“ vorstellen. Für die genaue Konstruktion dieser Gruppe, siehe § 2.2.1. Wir schreiben im Folgenden auch $2(a, \theta)$ für $(a, \theta) + (a, \theta)$.

wobei K alle Kanten des Polyeders P durchläuft.

Beispiele. (1) Sei W ein Würfel mit Seitenlänge a. Dann gilt

$$\delta(W) = 12\,(a, \pi/2) = 6\,(a, \pi) = 0_{\mathbb{R}\otimes_{\mathbb{Z}}(\mathbb{R}/\pi\mathbb{Z})}.$$

(2) Sei T ein regulärer Tetraeder mit Seitenlänge a'. Dann gilt

$$\delta(T) = 6\,(a', \arccos(1/3)).$$

Man kann $\delta(T) \neq 0_{\mathbb{R}\otimes_{\mathbb{Z}}(\mathbb{R}/\pi\mathbb{Z})}$ zeigen. (Das ist allerdings nicht völlig trivial, da formale Summen ja gemäß gewisser Rechenregeln als gleich betrachtet werden.)

1.2.9. Gruppen in der komplexen Analysis. In der *komplexen Analysis* studiert man unter anderem die holomorphen Selbstabbildungen $f\colon \mathbb{D} \to \mathbb{D}$ von der Einheitskreisscheibe $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ auf sich. (Rechtfertigung dafür, dass die Einschränkung auf die Einheitskreisscheibe nicht so speziell ist, wie sie zunächst anmuten mag, liefert der Riemannsche Abbildungssatz.) Die ***Gruppe der Einheitskreisautomorphismen***

$$\{\text{biholomorphe Abbildungen } \phi\colon \mathbb{D} \to \mathbb{D}\}$$

lässt sich explizit bestimmen (Stichwort: *Lemma von Schwarz*). Die fragliche Gruppe besteht nämlich genau aus den Abbildungen $\mathbb{D} \to \mathbb{D}$ mit

$$z \mapsto \eta \frac{z - z_0}{1 - \overline{z_0} z},$$

wobei $z_0 \in \mathbb{D}$ und $\eta \in \partial\mathbb{D} = \mathbb{S}^1$ beliebig sind. Interessierte Leserinnen und Leser finden vielleicht Freude daran, den Nutzen der Einheitskreisautomorphismen beim Beweis des Riemannschen Abbildungenssatzes in [30, Kapitel 10] (oder [46, Kapitel 7]) zu studieren.

1.3. Untergruppen

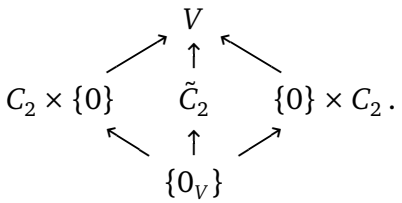
1.3.1. Definition und erste Eigenschaften. Es sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ heißt ***Untergruppe von G***, falls das Produkt $a \circ b$ von je zwei Elementen $a, b \in U$ wieder in U liegt und U zusammen mit der eingeschränkten[7] Verknüpfung $\circ|_{U\times U}\colon U \times U \to U$ eine Gruppe bildet. Wir schreiben dann $U \leq G$ und schreiben oft nur $\circ$ statt $\circ|_{U\times U}$.

Beispiele 1.2.

(1) Für jede Gruppe $(G, \circ)$ sind $\{1_G\}$ und G Untergruppen von G, die sogenannten ***trivialen Untergruppen***.
(2) $\mathbb{Z}$ ist eine Untergruppe von $(\mathbb{Q}, +)$ und $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ ist eine Untergruppe von $\mathbb{Z}$.

[7] Man beachte hier auch die subtile Einschränkung des Zielbereichs von $\circ$. Damit sich dieser hier auch auf U einschränken lässt, ist die zuvor genannte Bedingung „$a, b \in U \Rightarrow a \circ b \in U$“ unerlässlich.

(3) $\mathbb{Z} \setminus \{0\}$ ist keine Untergruppe von $(\mathbb{Q} \setminus \{0\}, \cdot)$.
(4) Für je zwei Gruppen $(G, \circ)$ und $(H, *)$ sind $G \times \{1_H\}$ und $\{1_G\} \times H$ Untergruppen von $G \times H$ (siehe auch § 1.2.4). Sind allgemeiner $U \leq G$ und $V \leq H$ Untergruppen, so ist $U \times V$ eine Untergruppe von $G \times H$. Allerdings sind im Allgemeinen nicht alle Untergruppen von $G \times H$ von dieser Form. Hierfür betrachte man die Kleinsche Vierergruppe $V = C_2 \times C_2$ aus § 1.2.4. Die Untergruppen von C_2 sind nur $\{0\} = \{0_{C_2}\}$ und C_2 selbst. Demnach hat V die Untergruppen $\{0_V\} = \{(0,0)\} = \{0\} \times \{0\}$, $\{0\} \times C_2$, $C_2 \times \{0\}$ und V selbst. Darüber hinaus hat V aber auch noch die „diagonal eingebettete" Kopie von C_2 als Untergruppe: $\tilde{C}_2 = \{(a,a) : a \in C_2\} \leq V$. Diese ist *nicht* von der Form $U \times V$ mit Untergruppen $U, V \leq C_2$. Das folgende Diagramm zeigt alle Untergruppen von V (Pfeile bedeuten Inklusionen):



Proposition 1.3 (Untergruppenkriterium)**.** *Es sei $(G, \circ)$ eine Gruppe und U eine Teilmenge von G. Dann ist U genau dann eine Untergruppe von G, falls die folgenden beiden Bedingungen erfüllt sind:*

(1) $1_G \in U$,
(2) für alle $a, b \in U$ ist $a \circ b^{-1} \in U$.

Beweis. Es sei zunächst U eine Untergruppe von G. *Wir überlegen uns zunächst, dass das neutrale Element 1_U von U mit dem neutralen Element 1_G von G übereinstimmt.* In der Tat ist ja

$$1_U \circ 1_U = 1_U \circ|_{U\times U} 1_U = 1_U = 1_U \circ 1_G.$$

Kürzen (in G) von 1_U mittels Proposition 1.1 (2) liefert $1_U = 1_G$. Analog ergibt sich auch, dass zu gegebenem $b \in U$ das in U zu b inverse Element mit dem in G zu b inversen Element b^{-1} übereinstimmt. (Man kürze b in $b \circ b^{-1\,(\text{in } G)} = 1_G = 1_U = b \circ b^{-1\,(\text{in } U)}$.) Also folgt zu $b \in U$ auch $b^{-1} \in U$ und dann auch für jedes weitere $a \in U$

$$a \circ b^{-1} = a \circ|_{U\times U} b^{-1} \in U.$$

Sei nun umgekehrt U eine Teilmenge von G, welche den beiden Eigenschaften aus der Proposition genügt. Dann liegt zu $b \in U$ auch $b^{-1} = 1_G \circ b^{-1}$ in U. Zu jedem weiteren $a \in U$ liegt dann allerdings auch $a \circ b = a \circ (b^{-1})^{-1}$ in U. Insbesondere schränkt sich $\circ\colon G \times G \to G$ zu einer Verknüpfung $\circ|_{U\times U}\colon U \times U \to U$ auf U ein. Diese eingeschränkte Verknüpfung ist, da $\circ$ ja assoziativ ist, ebenfalls assoziativ. Nun ist 1_G aber auch bezüglich dieser eingeschränkten Verknüpfung neutrales Element und zu jedem $b \in U$ liegt, wie schon gesehen, b^{-1} auch in U. Also ist U eine Untergruppe von G. □

Korollar 1.4. *Ist G eine Gruppe, I eine beliebige Indexmenge und $(U_i)_{i\in I}$ eine Familie von Untergruppen von G, so handelt es sich bei*

$$\bigcap_{i\in I} U_i = \{\, u \in G : u \in U_i \text{ für alle } i \in I \,\}$$

um eine Untergruppe von G.

Beweis. Es handelt sich um eine einfache Folgerung aus Proposition 1.3. □

Korollar 1.4 erlaubt die Betrachtung von möglichst kleinen Untergruppen, die vorgegebene Elemente enthalten. Es sei G eine Gruppe und $M \subseteq G$ eine beliebige Teilmenge von G. Dann gibt es genau eine *kleinste* Untergruppe (bezüglich der durch Teilmengeninklusion induzierten partiellen Ordnung auf G), welche M enthält, nämlich

$$\langle M\rangle := \bigcap_{\substack{U\leq G\\ M\subseteq U}} U.$$

Man nennt $\langle M\rangle$ die von M ***erzeugte*** Untergruppe (oder auch ***Erzeugnis von M***).

Beispiel. $\langle\emptyset\rangle = \{1_G\} = \langle\{1_G\}\rangle$, $\langle G\rangle = G$.

Ist $M = \{g\}$ einelementig, so schreibt man

$$\langle g\rangle := \langle\{g\}\rangle = \{\, g^n : n \in \mathbb{Z} \,\}. \tag{1.1}$$

(Für die letzte Gleichheit rechne man nach, dass es sich bei der rechten Seite davon um eine Untergruppe von G handelt, aber andererseits jede Untergruppe $U \leq G$ mit $g \in U$ natürlich auch $\{\, g^n : n \in \mathbb{Z} \,\}$ enthalten muss.) Die Ordnung von $\langle g\rangle$ (d.h. die Anzahl der Elemente von $\langle g\rangle$) nennt man auch ***Ordnung*** von g, sofern diese endlich ist und notiert $\operatorname{ord}(g) = \#\langle g\rangle$. Anderenfalls sagt man, g habe ***unendliche Ordnung*** und schreibt $\operatorname{ord}(g) = \infty$. In Verallgemeinerung von (1.1) kann man auch leicht

$$\langle M\rangle = \{\, g_1^{\epsilon_1}\cdots g_n^{\epsilon_2} : n \in \mathbb{N}_0,\, g_1,\ldots,g_n \in M,\, \epsilon_1,\ldots,\epsilon_n \in \{\pm 1\} \,\}$$

zeigen. Hierbei ist der subtile Spezialfall des leeren Produktes ($n = 0$) zu beachten; leere Produkte haben konventionsgemäß den Wert 1_G. Allgemein schreibt man $\langle u_1,\ldots,u_n\rangle := \langle\{u_1,\ldots,u_n\}\rangle$.

Beispiele.

(1) In $(\mathbb{R},+)$ hat man $\langle 1\rangle = \langle -1\rangle = \mathbb{Z} \subset \mathbb{R}$.

(2) Sei K ein Körper. $\mathrm{GL}_2(K)$ wird von sogenannten Elementarmatrizen erzeugt. Diese Aussage ist Grundlegend für den aus der *linearen Algebra* bekannten Gauß(–Jordan)-Algorithmus (siehe etwa [18, § 3.7.3]).

(3) In $\mathrm{GL}_2(\mathbb{R})$ ist

$$\left\langle \begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\right\rangle = \mathrm{SL}_2(\mathbb{Z}),$$

wobei die rechte Seite die Gruppe der 2×2-Matrizen mit ganzzahligen Einträgen und Determinante 1 bezeichnet. Die hier behauptete Gleichheit kann man elementar beweisen, allerdings ist diese keineswegs offensichtlich

und der Beweis benötigt etwas Arbeit. Wir verfolgen dies hier nicht (siehe etwa [14, $\mathrm{SL}_2(\mathbb{Z})$]).

1.3.2. Einschub: Teilbarkeit. Für unsere nächsten Untersuchungen (einschließlich § 1.4) benötigen wir etwas Vorwissen zu Teilbarkeit. Wir begnügen uns dabei mit recht wenig und greifen diesen Themenkomplex dafür dann in Kapitel 6 auf Seite 101 erneut auf und untersuchen ihn ab Kapitel 8 systematisch.

Lemma 1.5 (Division mit Rest)**.** *Für $m, t \in \mathbb{Z}$ mit $t > 0$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $m = qt + r$ und $0 \le r < t$.*

Beweis. Zur *Existenz*: wir setzen $q = \lfloor m/t \rfloor := \max\{ z \in \mathbb{Z} : z \le m/t \}$ und $r = m - qt$. Dann ist $0 \le m/t - q < 1$ und somit $0 \le r = t(m/t - q) < t$, wie gewünscht.

Nun zur *Eindeutigkeit*: es sei

$$qt + r = m = q't + r' \quad \text{mit} \quad 0 \le r, r' < t. \tag{1.2}$$

Subtraktion der beiden äußeren Seiten von (1.2) liefert

$$0 = (q - q')t + (r - r'), \quad \text{also} \quad |q - q'| = |r - r'|/|t| < 1.$$

Wegen $q - q' \in \mathbb{Z}$ folgt hieraus $q = q'$. Durch Einsetzen in (1.2) ergibt sich dann auch $r = r'$ und wir sind fertig. □

Eine ganze Zahl t heißt ***Teiler*** einer anderen Zahl m, falls es ein $q \in \mathbb{Z}$ mit $m = qt$ gibt. Wir schreiben hierfür auch $t \mid m$. Natürliche Zahlen $p > 1$, deren einzige positiven Teiler 1 und p selbst sind, nennt man ***Primzahlen***.

Beispiel.

n	1	2	3	$4 = 2 \cdot 2$	5	$6 = 2 \cdot 3$
Ist prim?	Nein	Ja	Ja	Nein	Ja	Nein

Der ***größte gemeinsame Teiler*** zweier Zahlen $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ ist die größte natürliche Zahl g mit $g \mid a$ und $g \mid b$. Wir schreiben $g = \mathrm{ggT}(a, b)$. Außerdem sei $\mathrm{ggT}(0, 0) := 0$. Offenbar gilt stets $0 \le \mathrm{ggT}(a, b) \le \max\{|a|, |b|\}$. Zahlen a und b mit $\mathrm{ggT}(a, b) = 1$ nennt man auch ***teilerfremd***.

Lemma 1.6 (Lemma von Bézout)**.** *Für $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ gibt es*[8] *$x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = ax + by$ und $\mathrm{ggT}(a, b)$ ist die kleinste natürliche Zahl, welche sich in dieser Form schreiben lässt. (Insbesondere gibt es für teilerfremde Zahlen a und b also $x, y \in \mathbb{Z}$ mit $1 = ax + by$.)*

Beweis. Wir betrachten

$$\mathfrak{g} = a\mathbb{Z} + b\mathbb{Z} := \{ ax + by : x, y \in \mathbb{Z} \}.$$

Wegen $|a| + |b| \in \mathfrak{g} \cap \mathbb{N}$ ist $\mathfrak{g} \cap \mathbb{N}$ nicht leer. Es gibt also eine *kleinste* natürliche Zahl g in $\mathfrak{g}$. Wir zeigen nun $g\mathbb{Z} = \mathfrak{g} = a\mathbb{Z} + b\mathbb{Z}$.

[8] Für den ausgeschlossenen Fall $(a, b) = (0, 0)$ ist die Gleichung $\mathrm{ggT}(a, b) = ax + by$ sogar *für alle* $x, y \in \mathbb{Z}$ erfüllt. Der fragliche Fall wird im Lemma nur ausgeschlossen, um die Gültigkeit des zweiten Teilsatzes gewährleisten zu können.

Da $\mathfrak{g}$ abgeschlossen unter Multiplikation mit Elementen von $\mathbb{Z}$ ist, gilt

$$g\mathbb{Z} := \{\, gq : q \in \mathbb{Z} \,\} \subseteq \mathfrak{g}.$$

Wir zeigen nun, dass hierbei auch die umgekehrte Inklusion „$\supseteq$“ gilt und also $g\mathbb{Z} = \mathfrak{g}$ ist. Hierzu sei $m \in \mathfrak{g}$ gegeben und wir bemühen Lemma 1.5, um $q, r \in \mathbb{Z}$ mit $0 \leq r < g$ und $m = qg + r$ zu finden. Da $\mathfrak{g}$ auch unter Addition von Elementen aus $\mathfrak{g}$ abgeschlossen ist, ist $r = m - qg$ ein Element von $\mathfrak{g}$. Aus der Minimalität von $g \in \mathfrak{g} \cap \mathbb{N}$ ergibt sich dann $r = 0$ und somit $m = qg \in g\mathbb{Z}$. Also folgt $g\mathbb{Z} = \mathfrak{g}$.

Wir zeigen nun noch $g = \mathrm{ggT}(a, b)$. Wegen $a, b \in \mathfrak{g} = g\mathbb{Z}$ ist g nämlich ein Teiler von a und b, also $g \leq \mathrm{ggT}(a, b)$. Umgekehrt ist aber auch $g = ax + by$ für geeignete $x, y \in \mathbb{Z}$ und aus $\mathrm{ggT}(a, b) \mid a, b$ folgt natürlich dann $\mathrm{ggT}(a, b) \mid g$. Insgesamt ist also $g = \mathrm{ggT}(a, b)$, wie behauptet. □

Beispiele.

- $\mathrm{ggT}(2, 3) = 1 = (-1) \cdot 2 + 1 \cdot 3$.
- $\mathrm{ggT}(86, 110) = 2 = (-23) \cdot 86 + 18 \cdot 110$.

1.3.3. Satz von Lagrange. Der nächste Satz liefert eine erste Einschränkung dafür, wie Untergruppen einer endlichen Gruppe zusammengesetzt sein können. Erste Anwendungen davon folgen gleich in § 1.4. In Kapitel 3 beschäftigen wir uns dann mit der Frage, in wie weit man den folgenden Satz umkehren kann.

Satz 1.7 (Satz von Lagrange)**.** *Es sei G eine endliche Gruppe und $U \leq G$ eine Untergruppe. Dann ist $\#U$ ein Teiler von $\#G$, d.h. es gibt eine ganze Zahl q mit $\#G = q \cdot \#U$.*

Beweis. Es bezeichne $gU = \{\, gu : u \in U \,\}$ die ***Linksnebenklasse*** (von U) bezüglich $g \in G$ und $G/U = \{\, gU : g \in G \,\}$ bezeichne die Menge aller dieser Klassen. Zu jedem fixierten $g \in G$ ist die Abbildung $\ell_g \colon G \to G$, $a \mapsto ga$, bijektiv (mit Umkehrabbildung $\ell_{g^{-1}}$) und bildet U auf gU ab. Also ist $\#U = \#(gU)$ und alle Linksnebenklassen besitzen dieselbe Anzahl an Elementen.

Falls sich zwei Linksnebenklassen aU, bU nichttrivial schneiden, etwa $c \in aU \cap bU$, so gibt es $u, v \in U$ mit $au = c = bv$. Multiplikation mit u^{-1} von rechts zeigt $a = b(vu^{-1}) \in bU$ und damit $aU \subseteq bU$. Aus Symmetriegründen erhält man auch die umgekehrte Inklusion, also $aU = bU$. Insbesondere sind je zwei *verschiedene* Linksnebenklassen disjunkt.

Da nun aber jedes Element $g \in G$ in einer Linksnebenklasse enthalten ist (nämlich in gU wegen $1_G \in U$), ist

$$\#G = \#\bigcup_{gU}{}^{\cdot}\, gU = \sum_{gU} \#(gU) = \sum_{gU} \#U = \#(G/U) \cdot \#U,$$

wobei der Index hier jeweils alle Elemente gU von G/U durchlaufe. □

Die Anzahl $\#(G/U)$ der Linksnebenklassen von U nennt man auch ***Index*** und notiert für diese $[G : U]$. Der Beweis vom Satz von Lagrange zeigt die wichtige Formel

$$\#G = [G : U] \#U. \tag{1.3}$$

In Aufgabe 2.2 wird eine Verallgemeinerung hiervon bewiesen.

Beispiel. Die Gruppe $G = C_3 \times C_5$ besitzt die Untergruppe $U = C_3 \times \{0\}$ und zerfällt in der wie folgt angedeuteten Art und Weise in 5 Nebenklassen gU ($g \in \{0\} \times C_5$):

$$G = \left\{ \begin{matrix} (0,0), \\ (1,0), \\ (2,0), \end{matrix} \middle| \begin{matrix} (0,1), \\ (1,1), \\ (2,1), \end{matrix} \middle| \begin{matrix} (0,2), \\ (1,2), \\ (2,2), \end{matrix} \middle| \begin{matrix} (0,3), \\ (1,3), \\ (2,3), \end{matrix} \middle| \begin{matrix} (0,4), \\ (1,4), \\ (2,4) \end{matrix} \right\}.$$

Man sieht, dass alle diese Nebenklassen gleich mächtig sind und die Formel (1.3) nimmt die Gestalt „$15 = 5 \cdot 3$“ an.

1.4. Zyklische Gruppen

Gruppen G, welche sich durch ein Element erzeugen lassen, $G = \langle g \rangle$ (für ein $g \in G$), nennt man ***zyklisch***.

Beispiel. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \langle 2, 3 \rangle = \langle 9, 10 \rangle \neq \langle 2 \rangle = 2\mathbb{Z}$ und $C_n = \langle 1 \rangle = \langle n-1 \rangle$.

Jedes Element in einer zyklischen Gruppe $G = \langle g \rangle$ ist von der Form g^n mit einem $n \in \mathbb{Z}$. Aus Proposition 1.1 (6) folgt, dass G abelsch ist:

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

Korollar 1.8. *Sei G eine Gruppe und $\#G$ sei eine Primzahl. Dann ist G zyklisch.*

Beweis. Das folgt sofort aus dem Satz von Lagrange (Satz 1.7), da jedes Element $a \in G \setminus \{1_G\}$ ja eine Untergruppe $\langle a \rangle \supsetneq \{1_G\}$ erzeugt, diese dann aber $\#G$ viele Elemente haben muss. □

Wir charakterisieren nun die Untergruppen endlicher zyklischer Gruppen in Abhängigkeit eines Erzeugers g.

Lemma 1.9. *Es sei G eine Gruppe und $g \in G$ ein Element von endlicher Ordnung $n = \operatorname{ord}(g) = \#\langle g \rangle < \infty$. Dann gilt für alle $k, l \in \mathbb{Z}$:*

(1) $g^n = 1_G$, $n = \min\{ r \in \mathbb{N} : g^r = 1_G \}$, $\langle g \rangle = \{1_G, g, g^2, \ldots, g^{n-1}\}$.
(2) $g^k = g^l \Longleftrightarrow n \mid k-l$.
(3) $g^k = 1_G \Longleftrightarrow n \mid k$.
(4) g^k *erzeugt* $\langle g \rangle \Longleftrightarrow k$ *und* n *sind teilerfremd.*

Beweis. (1) Weil $\langle g \rangle = \{ g^k : k \in \mathbb{Z} \}$ als Teilmenge der endlichen Menge G selbst endlich ist, existieren verschiedene $i, j \in \mathbb{Z}$ mit $g^i = g^j$. O.B.d.A. sei $i > j$. Dann folgt $g^{i-j} = 1_G$ und also $g^{i-j-1} = g^{-1}$. Insbesondere ist die Menge $\{ r \in \mathbb{N} : g^r = 1_G \}$ nicht leer und besitzt also ein Minimum m. Sei nun $k \in \mathbb{N}$ beliebig. Mittels Division mit Rest (Lemma 1.5) schreiben wir $k = qm + r$. Dann ist $g^k = g^{qm} g^r = (g^m)^q g^r = 1_G^q g^r = g^r$. Es folgt $\langle g \rangle = \{1_G, g, g^2, \ldots, g^{m-1}\}$ und unsere Überlegung mit i, j von oben zeigt, dass in der hier notierten Menge auch wirklich m Elemente enthalten sind (anderenfalls erhielte man einen Widerspruch zur minimalen Wahl von m). Wegen $n = \#\langle g \rangle$ folgt $m = n$ und (1) ist bewiesen.

(2) haben wir eigentlich implizit schon beim Beweis von (1) bewiesen. Trotzdem noch mal: O.B.d.A. sei $k > l$. Wegen $g^k = g^l \iff g^{k-l} = 1_G$ zeigt das obige Argument mit Division mit Rest schon $m \mid (k-l)$.

(3) folgt aus (2) mit $l = 0$.

(4) Wegen $\langle g^k \rangle \subseteq \langle g \rangle$ erzeugt g^k genau dann $\langle g \rangle$, wenn g in $\langle g^k \rangle$ enthalten ist. Es ist

$$g \in \langle g^k \rangle \iff \exists x \in \mathbb{Z}\colon g = (g^k)^x = g^{kx} \overset{(2)}{\iff} \exists x \in \mathbb{Z}\colon n \mid 1 - kx$$
$$\iff \exists x, y \in \mathbb{Z}\colon kx + ny = 1 \overset{\text{Lemma 1.6}}{\iff} \operatorname{ggT}(k,n) = 1. \qquad \square$$

Korollar 1.10 (Kleiner Satz von Fermat)**.** *Für jede endliche Gruppe G mit Ordnung n und jedes $g \in G$ gilt $g^n = 1$.*

Beweis. Nach dem Satz von Lagrange (Satz 1.7) ist $\operatorname{ord}(g)$ ein Teiler von $n = \#G$. Die Behauptung folgt somit aus Lemma 1.9 (3). $\square$

Das nächste Ergebnis ist eine Charakterisierung aller Untergruppen von der zyklischen Gruppe $(\mathbb{Z}, +)$.

Proposition 1.11 (Untergruppenverband von $(\mathbb{Z}, +)$)**.**

(1) Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Mengen $n\mathbb{Z} = \{ nz : z \in \mathbb{Z} \}$ mit $n \in \mathbb{N}_0$.

(2) Für $m, n \in \mathbb{Z}$ gilt: $m\mathbb{Z} \supseteq n\mathbb{Z} \iff m \mid n$. (*„**Teilen heißt Enthalten**.“*)

Beweis. Das ist Aufgabe T2.3. $\square$

Bemerkung. Das im Titel von Proposition 1.11 benutzte Wort „***Verband***“ weist auf eine gewisse algebraische Struktur hin. Wir bemessen diesen Strukturen hier allerdings keine gesonderte Betrachtung zu.

Die ***Eulersche φ-Funktion*** $\varphi\colon \mathbb{N} \to \mathbb{N}$ ist definiert durch

$$\varphi(n) = \#\{ k \in \{1, \dots, n\} : \operatorname{ggT}(k,n) = 1 \}.$$

Laut Lemma 1.9 (4) ist $\varphi(n)$ die Anzahl der Erzeuger jeder zyklischen Gruppe der Ordnung n. Dem Argument aus dem Beweis von Korollar 1.8 entnimmt man etwa $\varphi(p) = p - 1$ für jede Primzahl p. In Korollar 6.20 zeigen wir noch die schöne Formel

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right),$$

wobei der Index p alle (positiven) *Primzahlen* durchläuft, welche n teilen.

Beispiel. $120 = 2^3 \cdot 3 \cdot 5$ hat genau die Primteiler 2, 3 und 5. (Primfaktorzerlegung besprechen wir noch in Kapitel 8 genauer.) Demnach liefert die oben notierte Formel aus Korollar 6.20

$$\varphi(120) = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 120\frac{1}{2}\frac{2}{3}\frac{4}{5} = 2^2 \cdot 1 \cdot 2 \cdot 4 = 32.$$

Wir erinnern zunächst, für $n \in \mathbb{N}$, an die Konstruktion der abelschen Gruppe $(C_n, \oplus)$ aus § 1.2.2. Hier ist zu beachten, dass diese Gruppe zwar die ganze Zahl 1 enthält, aber ihr *neutrales Element* 0 ist.

Satz 1.12 (Untergruppenverband von $(C_n, \oplus)$)**.** *Es sei $n \in \mathbb{N}$ und $t \in \mathbb{N}$ ein Teiler von n. Dann gelten die folgenden Aussagen:*

(1) Es gibt genau eine Untergruppe der Ordnung t von $(C_n, \oplus)$, nämlich $\langle 0 \rangle$ für $t = 1$ und $\langle n/t \rangle$ für $t > 1$.

(2) In $(C_n, \oplus)$ gibt es genau $\varphi(t)$ Elemente der Ordnung t.

Beweis. Wir beweisen nur (1); (2) ist Aufgabe 3.1 (b). Der Fall $t = 1$ ist klar, da jede Untergruppe von C_n das neutrale Element 0 enthalten muss und es sich umgekehrt bei $\{0\}$ auch um eine Untergruppe von C_n handelt. Sei U daher nun eine Untergruppe von C_n mit Ordnung $t > 1$. Wir setzen $m = \min(U \setminus \{0\})$ und zeigen zunächst, dass U von m erzeugt wird. Für jedes $u \in U$ gibt es $q, r \in \mathbb{Z}$ mit $qm + r = u < n$ und $0 \leq r < m$. Es folgt $q \in \mathbb{N}_0$ und bei $qm = m + \ldots + m < n$ (q mal) und $m \oplus \ldots \oplus m$ (q mal) handelt es sich um dieselbe Zahl. Also folgt $u = qm + r = qm \oplus r$ und somit $r = (-qm) \oplus u \in U$, wobei $-qm$ hier das zu $qm \in C_n$ inverse Element, also $n - qm$ bezeichnet. Aus $r < m$ und der Minimalität von m folgt $r = 0$. Also gilt $U = \langle m \rangle$, wie behauptet.

Nun schreiben wir $n = q'm + r'$ mit $0 \leq r < m$. Erneut folgt $r' \in U$ und also $r' = 0$ wegen der minimalen Wahl von m. Also ist m ein Teiler von n. Der Definition von $\oplus$ entnimmt man nun, dass m erst nach n/m-maliger Verknüpfung mit sich das neutrale Element liefert; aus Lemma 1.9 (1) erhalten wir also $\#U = n/m$. Unsere Ausführungen liefern nun Folgendes: jede Untergruppe U von $(C_n, \oplus)$ mit t Elementen wird von $m = n/t$ erzeugt (d.h. insbesondere gibt es höchstens eine solche Untergruppe) und das Element $m = n/t$ in C_n erzeugt auch eine m-elementige Untergruppe, was die Existenzfrage klärt. Also gilt (1). □

Wir illustrieren den letzten Schritt des eben geführten Beweises anhand eines Beispiels:

Beispiel. Wir betrachten die Untergruppe U von $(C_{12}, \oplus)$, welche von $9 \in C_{12}$ erzeugt wird. Es gilt $9 \oplus 9 = (18 - 12) = 6$, $(9 \oplus 9) \oplus 9 = 6 \oplus 9 = (15 - 12) = 3$, $((9 \oplus 9) \oplus 9) \oplus 9 = 3 \oplus 9 = (12 - 12) = 0$. Also erhalten wir $U = \langle 9 \rangle = \{0, 3, 6, 9\}$. Das Element $3 = \min(U \setminus \{0\})$ stellt sich nun aber ebenfalls als Erzeuger von U heraus ($3 \oplus 3 = 6$, $(3 \oplus 3) \oplus 3 = 9$, $((3 \oplus 3) \oplus 3) \oplus 3 = 0$). Man beachte, dass $\#U = 4$ ein Teiler von 12 ist und, dass es sich bei $(\#C_{12})/\#U = 12/4 = 3$ um den *kleinsten* Erzeuger von U handelt.

Beispiel 1.13 (Untergruppenverband von $(C_{12}, \oplus)$)**.** Wir betrachten $(C_{12}, \oplus)$, $U_1 := \{0\} \leq C_{12}$ und die zugehörigen Untergruppen $U_t = \langle 12/t \rangle$ für alle positiven Teiler $1 < t < 12$ von 12. Das Diagramm in Abbildung 13 zeigt den vollständigen Untergruppenverband von C_{12}. Ein Pfeil von $U_t \xrightarrow{x} U_s$ bedeutet hier $U_t \leq U_s$ und

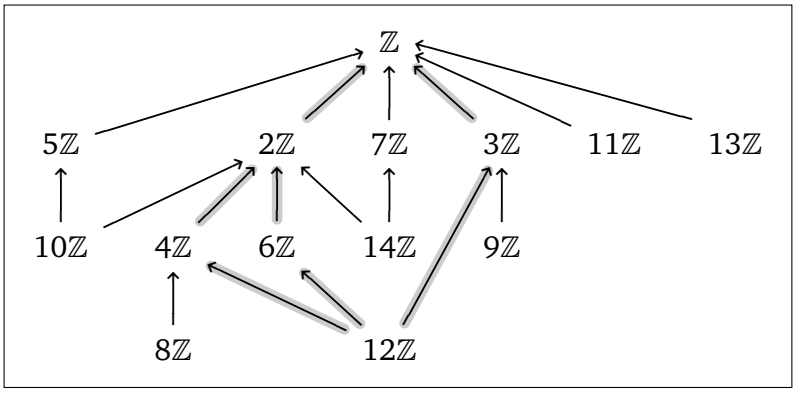


Abbildung 12. Ein Ausschnitt des Untergruppenverbandes von $(\mathbb{Z}, +)$; siehe Proposition 1.11. Man vergleiche den hervorgehobenen Teil mit dem in Beispiel 1.13 erhaltenen Verband.

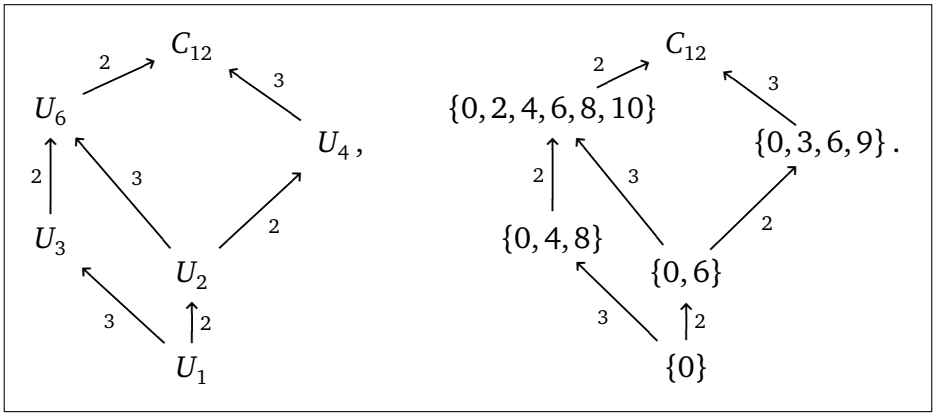


Abbildung 13. Der Untergruppenverband von $(C_{12}, \oplus)$; siehe Beispiel 1.13.

$[U_s : U_t] = x$ und führt kein Weg (den Pfeilen in gemäß Richtung folgend) von U_t zu U_s, so ist $U_t \nsubseteq U_s$.

Man vergleiche diesen Untergruppenverband auch mit Abbildung 12. Dass dort ein sehr ähnliches Bild auftritt, ist kein Zufall und wird sich noch im Rahmen unserer Untersuchungen zu Faktorgruppen klären.

Wir nutzen die Gelegenheit, um uns hier auch noch mal den Begriff der Linksnebenklasse zu veranschaulichen. Es ist $[U_6 : U_2] = \#U_6/\#U_2 = 6/2 = 3$. Es gibt also in U_6 genau drei Linksnebenklassen bezüglich U_2. Diese sind (additive Schreibweise beachten!)

$$0 + U_2 = \{0, 6\} = 6 + U_2, \qquad 2 + U_2 = \{2, 8\} = 8 + U_2,$$
$$4 + U_2 = \{4, 10\} = 10 + U_2.$$

Man sieht auch sofort

$$U_6 = \{0,6\} \cup \{2,8\} \cup \{4,10\} = (0+U_2) \cup (2+U_2) \cup (4+U_2).$$

Wir zeigen später, sobald Faktorgruppen zur Verfügung stehen, dass durch Proposition 1.11 und Satz 1.12 tatsächlich *alle* zyklischen Gruppen charakterisiert werden (siehe Korollar 2.8).

Korollar 1.14. *Für alle $n \in \mathbb{N}$ gilt* $n = \sum_{t|n} \varphi(t)$.

Beweis. Wir beachten $\#C_n = n$ und gruppieren die Elemente von C_n nach ihrer Ordnung (bei welcher es sich gemäß Satz 1.7 stets um einen Teiler t von n handelt). Wir haben also

$$n = \#C_n = \sum_{t|n} \#\{\, g \in C_n : \operatorname{ord}(g) = t \,\}.$$

Gemäß Satz 1.12 handelt es sich bei dem Summanden auf der rechten Seite genau um $\varphi(t)$. Damit ergibt sich die Behauptung des Korollars. □

Beispiel. $\sum_{t|15} \varphi(t) = \varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 1 + 2 + 4 + 8 = 15.$

KAPITEL 2

Homomorphismen, Faktorgruppen, Operationen

Um in den Dschungel der Gruppen etwas Ordnung bringen zu können, ist es wichtig, Gruppen miteinander vergleichen zu können und in Beziehung zueinander setzen zu können. Hierzu nötige Begriffe und Hilfsmittel entwickeln wir in diesem Kapitel.

2.1. Gruppenhomomorphismen

Ein ***Gruppenhomomorphismus*** f zwischen zwei Gruppen $(G,\circ)$ und $(G',*)$ ist eine Abbildung $f\colon G\to G'$, welche die Gruppenstruktur auf G respektiert. Konkret fordern wir hierfür, dass

$$f(a\circ b)=f(a)*f(b) \tag{2.1}$$

für alle $a,b\in G$ gilt. Nun gehört zu der Gruppenstruktur natürlich noch eine Aussage über ein neutrales Element und inverse Elemente. Konzeptionell wäre es adäquat, den Erhalt dieser Strukturen ebenfalls in der Definition eines Gruppenhomomorphismus zu fordern. Tatsächlich folgt dies aber schon aus (2.1), wie das folgende Lemma zeigt:

Lemma 2.1. *Für jeden Gruppenhomomorphismus $f\colon G\to G'$ gilt $f(1_G)=1_{G'}$ und für alle $a\in G$ ist $f(a)^{-1}=f(a^{-1})$.*

Beweis. Wir bezeichnen die Verknüpfung für G mit $\circ$ und die für G' mit $*$. Es ist

$$1_{G'}*f(1_G)=f(1_G)=f(1_G\circ 1_G)=f(1_G)*f(1_G).$$

Kürzen von $f(1_G)$ zeigt $1_{G'}=f(1_G)$, wie gewünscht. Für $a\in G$ erhält man

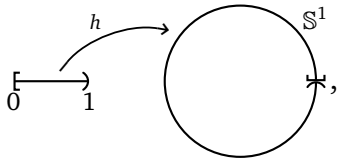
$$1_{G'}=f(a\circ a^{-1})=f(a)*f(a^{-1}).$$

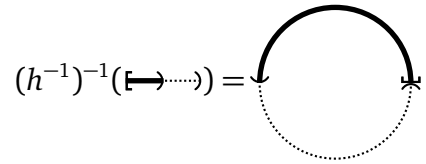
Multiplikation mit $f(a)^{-1}$ zeigt $f(a)^{-1}=f(a^{-1})$. □

Wir bezeichnen einen Gruppenhomomorphismus $f\colon G\to G'$ als

$$\textit{(Gruppen-)}\begin{Bmatrix}\textbf{\textit{Mono-}}\\ \textbf{\textit{Epi-}}\\ \textbf{\textit{Iso-}}\\ \textbf{\textit{Endo-}}\\ \textbf{\textit{Auto-}}\end{Bmatrix}\textbf{\textit{Morphismus}}\text{ falls }\begin{Bmatrix}f\text{ injektiv}\\ f\text{ surjektiv}\\ f\text{ bijektiv}\\ (G,\circ)=(G',*)\\ f\text{ bijektiv und }(G,\circ)=(G',*)\end{Bmatrix}\text{ ist.}$$

Bemerkung. Eine konzeptionell bessere Art, Gruppenisomorphismen zu definieren, wäre als Gruppenhomomorphismen $f\colon G \to G'$, zu denen es einen passenden Gruppenhomomorphismus $g\colon G' \to G$ mit $f \circ g = \mathrm{id}_{G'}$ und $g \circ f = \mathrm{id}_G$ gibt. Proposition 2.3 (siehe unten) zeigt jedoch, dass beide Begriffe äquivalent sind. Man entsinne sich allerdings an die Topologie. Dort zeigt etwa das Beispiel $h\colon [0,1) \to \mathbb{S}^1$, $t \mapsto \exp(2\pi \mathrm{i}\, t)$, dass eine bijektive stetige Abbildung nicht notwendigerweise eine *stetige* Umkehrabbildung zu haben braucht:





(nicht offen!).

Für den Begriff eines „Isomorphismus topologischer Räume“, eines sogenannten ***Homöomorphismus***, muss man *zusätzlich* zur Stetigkeit und Bijektivität auch die *Stetigkeit der Umkehrabbildung* fordern. Dies lässt sich auch äquivalent dazu ausdrücken, dass eine stetige Abbildung $f\colon X \to Y$ zwischen topologischen Räumen genau dann ein Homöomorphismus ist, wenn es eine stetige Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$ und $g \circ f = \mathrm{id}_X$ gibt.

Wir schreiben

$$\begin{aligned} \mathrm{Hom}(G, G') &:= \{\text{Gruppenhomomorphismen von } G \text{ nach } G'\},\\ \mathrm{End}(G) &:= \{\text{Gruppenendomorphismen von } G\},\\ \mathrm{Aut}(G) &:= \{\text{Gruppenautomorphismen von } G\}. \end{aligned}$$

Existiert ein Isomorphismus zwischen G und G', so nennen wir G und G' ***isomorph*** und schreiben $G \cong G'$. Für einen Gruppenhomomorphismus $f : G \to G'$ nennen wir

$$\ker f := f^{-1}(\{1_{G'}\}) = \{\, a \in G : f(a) = 1_{G'} \,\}$$

den ***Kern von f*** und

$$\mathrm{im}\, f = f(G) := \{\, a' \in G' : \exists a \in G \text{ mit } f(a) = a' \,\}$$

das ***Bild von f***.

Beispiele 2.2. Wir betrachten hier $\mathbb{R}$ als abelsche Gruppe mit der bekannten Addition ganzer Zahlen als Verknüpfung.

(1) $\mathbb{R} \to \mathbb{R}$, $z \mapsto 0$, ist ein Gruppenhomomorphismus.
(2) $\mathbb{R} \to \mathbb{R}$, $z \mapsto 1$, ist kein Gruppenhomomorphismus.
(3) $\mathrm{id}_{\mathbb{R}}\colon \mathbb{R} \to \mathbb{R}$ ist ein Gruppenisomorphismus.
(4) Es sei K ein Körper. Die Abbildung

$$\mathrm{GL}_n K \longrightarrow \mathrm{GL}(K^n), \quad A \longmapsto \begin{cases} K^n \to K^n, \\ \boldsymbol{v} \mapsto A\boldsymbol{v}, \end{cases}$$

ist ein Gruppenisomorphismus, wie man leicht nachrechnen kann. Ihre Umkehrabbildung ordnet jedem $f \in \mathrm{GL}(K^n)$ die zugehörige Darstellungsmatrix

$$\begin{pmatrix} | & \dots & | \\ f(e_1) & \dots & f(e_n) \\ | & \dots & | \end{pmatrix} \in K^{n\times n}$$

bezüglich der Standardbasis $e_1, \dots, e_n$ auf K^n zu. Insbesondere sind $\mathrm{GL}_n(K)$ und $\mathrm{GL}(K^n)$ isomorph. (Eine deratige Aussage wurde auch schon in § 1.2.5 vermutet bzw. angekündigt.)

(5) Es sei M eine beliebige endliche Menge mit genau n Elementen. Dann gibt es eine Bijektion $f\colon \{1,\dots,n\} \to M$. Bei der Abbildung

$$\Psi\colon \mathrm{Sym}(M) \longrightarrow \mathfrak{S}_n, \quad \sigma \longmapsto f^{-1} \circ \sigma \circ f,$$

handelt es sich um einen Gruppenisomorphismus und darum ist $\mathrm{Sym}(M) \cong \mathfrak{S}_n$. Wir illustrieren den Zusammenhang von σ und $\Psi(\sigma)$ anhand des folgenden kommutativen Diagramms:

$$\begin{array}{ccc} M & \xrightarrow{\quad\sigma\quad} & M \\ {\scriptstyle f}\uparrow\wr & & \wr\uparrow{\scriptstyle f} \\ \{1,\dots,n\} & \xrightarrow{\Psi(\sigma)} & \{1,\dots,n\}\,. \end{array}$$

(6) $\iota_1\colon \mathbb{R} \to \mathbb{R}\times\mathbb{R}$, $x \mapsto (x,0)$, ist ein Gruppenmonomorphismus; Es gilt $\ker \iota_1 = \{0\}$ und $\mathrm{im}(\iota_1) = \mathbb{R}\times\{0\}$.

(7) $\pi_1\colon \mathbb{R}\times\mathbb{R} \to \mathbb{R}$, $(x,y) \mapsto x$, ist ein Gruppenepimorphismus; Es gilt $\ker \pi_1 = \{0\}\times\mathbb{R}$ und $\mathrm{im}(\pi_1) = \mathbb{R}$.

(8) Man hat ein kommutatives Diagramm

$$\mathbb{R} \xrightarrow{\iota_1\colon x\mapsto(x,0)} \mathbb{R}\times\mathbb{R} \xrightarrow{\pi_1\colon (x,y)\mapsto x} \mathbb{R}\,.$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \searrow \quad \nearrow_{\mathrm{id}_{\mathbb{R}}}$$

(9) Sei $f\colon X \to Y$ eine stetige Abbildung zwischen topologischen Räumen. Sei $x_* \in X$ beliebig. Dann erhält man durch

$$f_*\colon \pi(X,x_*) \longrightarrow \pi(Y,f(x_*)), \quad [\gamma] \longmapsto [f\circ\gamma],$$

einen Gruppenhomomorphismus zwischen den den Räumen zugeordneten Fundamentalgruppen $\pi(X,x_*)$ und $\pi(Y,f(x_*))$ (siehe § 1.2.6).

Allgemein nennt man bei einem kommutativen Diagramm (mit Abbildungen $\iota\colon A\to B$ und $\pi\colon B\to A$)

$$A \xrightarrow{\iota} B \xrightarrow{\pi} A$$
$$\qquad\qquad \searrow \quad \nearrow_{\mathrm{id}_A}$$

die Abbildung ι einen ***Schnitt*** von π und π eine ***Retraktion*** von ι. Handelt es sich bei A und B um Gruppen und bei $\pi\colon B \to A$ um einen Gruppenhomomorphismus, so sagt man, es gebe einen Schnitt zu π, falls es einen Gruppenhomomorphismus $\iota\colon A \to B$ gibt, der im obigen Sinne ein Schnitt zu π (als Abbildungen aufgefasst) ist.[1] Analog definiert man Retraktionen von Gruppenhomomorphismen.

Proposition 2.3. *Es seien $(G,\bullet)$, $(G',*)$ und $(G'',\star)$ Gruppen. Ferner seien $f\colon G \to G'$ und $g\colon G' \to G''$ Gruppenhomomorphismen.*

(1) Auch $g \circ f\colon G \to G''$ ist ein Gruppenhomomorphismus.

$$G \xrightarrow{f} G' \xrightarrow{g} G'', \qquad G \xrightarrow{g\circ f} G''.$$

(2) Ist f ein Gruppenisomorphismus, so ist auch die Umkehrabbildung $f^{-1}\colon G' \to G$ ein Gruppenhomomorphismus (und sogar ein Gruppenisomorphismus).

*(3) $\mathrm{Aut}(G)$ bildet mit der Verkettung von Abbildungen eine Gruppe, die **Automorphismengruppe von G**.*

(4) Zu $U \leq G$ und $U' \leq G'$ sind auch $f(U) \leq G'$ und $f^{-1}(U') \leq G$. Insbesondere ist $\ker f$ eine Untergruppe von G und $\operatorname{im} f$ ist eine Untergruppe von G'.

(5) f ist genau dann ein Gruppenmonomorphismus, wenn f trivialen Kern hat, d.h. wenn $\ker f = \{1_G\}$ gilt.

Beweis. (1) folgt sofort aus

$$\begin{aligned}(g\circ f)(a\bullet b) &= g(f(a\bullet b)) = g(f(a)*f(b))\\ &= g(f(a))\star g(f(b)) = (g\circ f)(a)\star(g\circ f)(b).\end{aligned}$$

(2) Sind $a', b' \in G'$ beliebig und ist f ein Gruppenisomorphismus, so gibt es $a, b \in G$ mit $f(a) = a'$ und $f(b) = b'$. Dann ist aber auch $f(a\bullet b) = f(a)*f(b) = a'*b'$. Anwenden von f^{-1} liefert $f^{-1}(a')\bullet f^{-1}(b') = a\bullet b = f^{-1}(a'*b')$. Also ist f^{-1} ein Gruppenhomomorphismus. Überdies ist mit f natürlich auch f^{-1} bijektiv und somit f^{-1} sogar ein Gruppenisomorphismus.

(3) Man kann sich hier darauf berufen, dass $\mathrm{Sym}(G) \supseteq \mathrm{Aut}(G)$ bereits aus § 1.2.3 als Gruppe mit der üblichen Verkettung von Abbildungen erkannt wurde. Es genügt daher, zu sehen, dass es sich bei $\mathrm{Aut}(G)$ um eine *Untergruppe* von $\mathrm{Sym}(G)$ handelt. Das ergibt sich aber mit den bereits bewiesenen Teilaussagen (1) und (2) sehr leicht.

Die Verifikation von (4) sei der geneigten Leserin oder dem geneigten Leser zur freiwilligen Übung überlassen.

(5) Ist f injektiv, so enthält $\ker f = f^{-1}(\{1_{G'}\})$ natürlich höchstens ein Element, aber wegen $f(1_G) = 1_{G'}$ dann sogar genau ein Element, nämlich 1_G. Ist umgekehrt $\ker f = \{1_G\}$, so ist f injektiv, denn aus $a, b \in G$ mit $f(a) = f(b)$ folgt $1_{G'} =$

[1] Man beachte, dass π als Abbildung aufgefasst also einen Schnitt haben könnte, aber als Gruppenhomomorphismus eventuell nicht; wichtig ist hierbei eben noch die Frage, ob es ein $\iota\colon A \circ B$ mit $\pi\circ\iota = \mathrm{id}_A$ gibt *und*(!) ι auch ein Gruppenhomomorphismus ist.

$f(a)^{-1} * f(b) = f(a^{-1}) * f(b) = f(a^{-1} \bullet b)$, also $a^{-1} \bullet b \in \ker f = \{1_G\}$, d.h. $a^{-1} \bullet b = 1_G$ und somit $b = a$. □

Bemerkung. Wir benutzen oft diverse Verträglichkeitseigenschaften von Gruppenhomomorphismen und diversen bereits besprochenen Konzepten der Gruppentheorie. Wir geben zwei Beispiele:

(1) Ist $f\colon G \to H$ ein Gruppenhomomorphismen und hat $g \in G$ endliche Ordnung n, so hat $f(g) \in H$ ebenfalls endliche Ordnung und diese teilt n. (Beweis: $f(g)^n = f(g^n) = f(1_G) = 1_H$, also $\operatorname{ord}(f(g)) < \infty$ und $\operatorname{ord}(f(g)) \mid n$ gemäß Lemma 1.9.)

(2) Sind $f\colon G \to H$ und $f'\colon G' \to H'$ zwei Gruppenhomomorphismen, so ist durch $f \times f'\colon G \times G' \to H \times H'$, $(g, g') \mapsto (f(g), f'(g'))$, ein Gruppenhomomorphismus gegeben. Sind f und f' sogar Gruppenisomorphismen, so gilt dies auch für $f \times f'$. Insbesondere gilt: ist $G \cong H$ und $G' \cong H'$, so ist $G \times G' \cong H \times H'$. Die hier getroffenen Aussagen verallgemeinern sich unmittelbar auf direkte Produkte mit beliebig vielen Faktoren.

2.2. Faktorgruppen

2.2.1. Konstruktion von Faktorgruppen. *Welche Untergruppen $N \leq G$ sind Kerne von Gruppenhomomorphismen?* — Diese Frage beantworten wir in diesen Abschnitt.

Es sei zunächst die Existenz eines Gruppenhomomorphismus $f\colon G \to H$ mit $N = \ker f$ angenommen. Für alle $g \in G$ und alle $n \in N$ gilt dann

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)1_H f(g)^{-1} = f(g)f(g)^{-1} = 1_H, \tag{2.2}$$

also $gng^{-1} \in \ker f = N$.

Beispiele. (1) Für Gruppen N' und H ist $G = N' \times H$ natürlich wieder eine Gruppe. Außerdem ist $N := N' \times \{1_H\} \cong N'$ der Kern von der kanonischen Projektion $\pi_2\colon G \to H$, $(n', h) \mapsto h$. Diese ist natürlich ein Homomorphismus. Die Gleichung $gng^{-1} \in N$ nach (2.2), welche wir natürlich schon aus der eben gemachten Feststellung erhalten, lässt sich auch direkt in G nachrechnen: Für $g = (\tilde{n}, h)$ und $n = (n', 1_H)$ ist nämlich

$$\begin{aligned} gng^{-1} &= (\tilde{n}, h)(n', 1_H)(\tilde{n}, h)^{-1} = (\tilde{n}, h)(n', 1_H)(\tilde{n}^{-1}, h^{-1}) \\ &= (\tilde{n}n'\tilde{n}^{-1}, h1_H h^{-1}) = (\tilde{n}n'\tilde{n}^{-1}, 1_H) \in N. \end{aligned}$$

(2) Wir betrachten die symmetrische Gruppe $\mathfrak{S}_3$ und die Elemente

τ_{12}:  τ_{23}:  σ_{123}: 

Das Element τ_{12} hat Ordnung 2 in $\mathfrak{S}_3$ und erzeugt daher die 2-elementige Untergruppe $N = \langle \tau_{12} \rangle = \{\mathrm{id}_{\{1,2,3\}}, \tau_{12}\}$ von $\mathfrak{S}_3$. (Siehe auch Abbildung 15

auf Seite 65.) Wegen

$$\sigma_{123} \circ \tau_{12} \circ \sigma_{123}^{-1} = \begin{array}{ccc} 1 & 2 & 3 \\ & \searrow\swarrow & \\ 1 & 2 & 3 \\ & \searrow\swarrow & \\ 1 & 2 & 3 \\ & \searrow\swarrow & \\ 1 & 2 & 3 \end{array} = \tau_{23} \notin N$$

verletzt jene Untergruppe N die Eigenschaft „$gng^{-1} \in N$“, die wir unter Gleichung (2.2) erhalten hatten. Insbesondere handelt es sich bei $N = \langle \tau_{12} \rangle$ *nicht* um den Kern von *irgendeinem* Gruppenhomomorphismus $\mathfrak{S}_3 \to H$ (in irgendeine Gruppe H).
Ganz anders verhält es sich bei $N' = \langle \sigma_{123} \rangle$. Es handelt sich hierbei um eine Untergruppe von $\mathfrak{S}_3$ mit drei Elementen und man kann nachrechnen, dass diese wirklich die unter (2.2) gefolgerte Eigenschaft besitzt. Diese Untergruppe ist auch ein Kern eines Gruppenhomomorphismus, zum Beispiel von der kanonischen Projektion $\mathfrak{S}_3 \to \mathfrak{S}_3/N'$, $\sigma \mapsto \sigma N'$, (siehe weiter unten in diesem Abschnitt), oder vom Signum-Homomorphismus sgn: $\mathfrak{S}_3 \to \{\pm 1\}$, den wir in § 4.2 konstruieren (siehe Lemma 4.4).

Für Teilmengen A, B, C einer Gruppe G definieren wir das ***Komplexprodukt***

$$AB := \{ ab : a \in A,\ b \in B \}.$$

Wegen der Assoziativität der Verknüpfung in G ist auch das Komplexprodukt assoziativ; Wir haben

$$\begin{aligned} (AB)C &= \{ (ab)c : a \in A,\ b \in B,\ c \in C \} \\ &= \{ a(bc) : a \in A,\ b \in B,\ c \in C \} \\ &= A(BC) \end{aligned}$$

und dürfen darum (wie auch schon bei Gruppen) auch auf die Klammerung der Faktoren verzichten. Überdies definieren wir für $a, b \in G$

$$aB := \{a\}B \quad \text{und} \quad Ab := A\{b\}.$$

(Diese Schreibweise kennen wir schon von Links- bzw. Rechtsnebenklassen aus dem Beweis vom Satz von Lagrange, Satz 1.7.)

Ist N eine Untergruppe von G und $A \subseteq N$ eine beliebige nicht-leere Teilmenge von N, so gilt die folgende ***Adsorptionsregel***:

$$AN = N = NA.$$

(Dabei ist $AN \subseteq N$ klar, da Produkte an mit $a \in A \subseteq N$ und $b \in N$ ebenfalls in N liegen. Umgekehrt ist aber auch jedes $n \in N$ in AN enthalten; ist nämlich $a \in A$ beliebig, so ist $a^{-1} \in N$ und also auch $a^{-1}n \in N$ und somit $n = a(a^{-1}n) \in AN$.) Speziell für $A = N$ erhalten wir $NN = N$.

Lemma 2.4. *Es sei G eine Gruppe und N eine Untergruppe. Dann sind äquivalent:*

(1) $\forall g \in G\, \forall n \in N\colon gng^{-1} \in N$;

(2) $\forall g \in G\colon gNg^{-1} \subseteq N$;

(3) $\forall g \in G\colon gNg^{-1} = N$;

(4) $\forall g \in G\colon gN = Ng$.

Überdies ist $gN = hN$ für $g, h \in G$ genau dann wenn $g = hn$ für ein $n \in N$ gilt.

Beweis. „(1) $\Leftrightarrow$ (2)“, „(2) $\Leftarrow$ (3)“ und „(3) $\Leftrightarrow$ (4)“ sind klar. Für „(2) $\Rightarrow$ (3)“ sei die Gültigkeit von (2) angenommen und $g \in G$ beliebig. Wir wollen einsehen, dass jedes $n \in N$ auch Element von gNg^{-1} ist. Wegen (2) ist $g^{-1}n(g^{-1})^{-1}$ in N enthalten. Wegen $gNg^{-1} \ni g(g^{-1}n(g^{-1})^{-1})g^{-1} = n$ folgt $n \in gNg^{-1}$ und also (3).

Für den Zusatz beachte man, dass wegen $1_G \in N$ auch $g \in gN$ ist. Insbesondere folgt aus $gN = hN$ also $g = hn$ für ein $n \in N$. Gilt umgekehrt $g = hn$ für ein $n \in N$, so ist wegen $n^{-1} \in N$ natürlich $gN = hnN = hN$. □

Eine Untergruppe N von G, welche eine der äquivalenten Bedingungen aus Lemma 2.4 erfüllt, nennt man auch ***Normalteiler von G*** und schreibt hierfür $N \trianglelefteq G$.

Bemerkung. In einer abelschen Gruppe sind alle Untergruppen automatisch Normalteiler. Im Allgemeinen ist allerdings nicht jede Untergruppe einer nicht-abelschen Gruppe ein Normalteiler. Das kleinste Beispiel hierfür ist $\mathfrak{S}_3$ mit Untergruppe $U = \langle \tau_{12} \rangle$, mit der Permutation τ_{12} von oben. Wählt man etwa σ_{123} (ebenfalls wie oben), so sieht man leicht $\sigma_{123}U \neq U\sigma_{123}$. Alternativ betrachte man etwa die Untergruppe

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} : u \in \mathbb{R} \right\}$$

von $\mathrm{GL}_2(\mathbb{R})$. (Die hier auftretenden Matrizen beschreiben Scherungen.) Nun betrachte man die Matrix

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

welche eine Drehung um 90° beschreibt. Man rechnet leicht nach, dass

$$RU = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & u \end{pmatrix} : u \in \mathbb{R} \right\} \quad \text{und} \quad UR = \left\{ \begin{pmatrix} u & -1 \\ 1 & 0 \end{pmatrix} : u \in \mathbb{R} \right\}$$

gilt. Scharfes Hinsehen zeigt, dass diese beiden Mengen nicht übereinstimmen.

Für eine Untergruppe U von G und $g \in G$ nennt man das Komplexprodukt gU bekanntlich auch Linksnebenklasse von a bezüglich U. Die Menge aller Linksnebenklassen bezüglich U bezeichnet man auch mit $G/U = \{ gU : g \in G \}$. Analog definiert man die Menge[2] $U \setminus G = \{ Ug : g \in G \}$ aller Rechtsnebenklassen. (Es sei hier an den Satz von Lagrange, Satz 1.7, erinnert, bei dessen Beweis diese Nebenklassen bereits eine wichtige Rolle spielten.)

[2]Achtung: diese sollte man nicht mit der mengentheoretischen Exklusion $U \setminus G = \{ u \in U : u \notin G \} = \emptyset$ verwechseln.

Ist N ein Normalteiler, so kann man auf G/N eine Gruppenstruktur definieren! In der Tat bildet G/N zusammen mit der Verknüpfung

$$*\colon (G/N)\times(G/N)\to G/N,\quad (aN,bN)\mapsto (ab)N$$

eine Gruppe, die ***Faktorgruppe von G nach N***. Diese Verknüpfung ist wegen

$$aNbN = a(Nb)N = a(bN)N = (ab)(NN) = (ab)N$$

tatsächlich wohl-definiert,[3] wobei wir für die letzte Gleichung die Adsorptionsregel $NN = N$ benutzt haben. Die Assoziativität folgt leicht aus der Assoziativität des Komplexproduktes (was wiederum nur eine Konsequenz aus der Assoziativität der Verknüpfung auf G ist), als neutrales Element fungiert die Linksnebenklasse $1_G N = N$ und die zu aN inverse Klasse ist $a^{-1}N$. Bei

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

handelt es sich um einen Gruppenhomomorphismus, die sogenannte ***kanonische Projektion (auf G/N)***. Der Zusatz in Lemma 2.4 zeigt $\ker\pi = N$.

Beispiel. Sei $n\in\mathbb{N}$. Wir betrachten die Untergruppe $n\mathbb{Z}$ von $\mathbb{Z}$ (siehe Proposition 1.11). Wir überlegen uns nun, dass die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ Ordnung n hat. Hierfür sei $m\in\mathbb{Z}$. Division mit Rest (Lemma 1.5) liefert eine Darstellung $m = qn + r$ mit $q, r\in\mathbb{Z}$ und $0\le r < n$. Wegen $qn\in n\mathbb{Z}$ liefert der Zusatz in Lemma 2.4 die Gleichheit $m + n\mathbb{Z} = r + \mathbb{Z}$. Daraus folgt

$$\mathbb{Z}/n\mathbb{Z} = \{\, m + n\mathbb{Z} : m\in\mathbb{Z}\,\} = \{\, r + n\mathbb{Z} : 0\le r < n\,\}.$$

Der Parameter r auf der rechten Seite durchläuft die n Werte $0, 1, \ldots, n-1$. Tatsächlich sind die daraus resultierenden Nebenklassen $r + n\mathbb{Z}$ auch alle verschieden. Um dies einzusehen, sei $0\le r\le r' < n$ mit $r + n\mathbb{Z} = r' + n\mathbb{Z}$ gegeben. Wir wollen $r = r'$ einsehen. Wegen $r\in r + n\mathbb{Z} = r' + n\mathbb{Z}$ gibt es ein $q\in\mathbb{Z}$ mit $r = r' + qn$. Durch Umstellen erhalten wir also $r - r' = qn$. Vergleicht man nun Beträge, so erhält man $q = 0$ und also $r = r'$. Somit ist $\#(\mathbb{Z}/n\mathbb{Z}) = \#\{\, r + n\mathbb{Z} : 0\le r < n\,\} = n$, wie eingangs behauptet.
Durch den oben skizzierten Vorgang, welcher einer Nebenklasse $m + n\mathbb{Z}\in\mathbb{Z}/n\mathbb{Z}$ den Rest r, welchen m bei Division durch n lässt, zuordnet, stiftet eine Abbildung $f\colon \mathbb{Z}/n\mathbb{Z}\to\{0, 1, \ldots, n-1\}$ von welcher wir eben eingesehen haben, dass diese bijektiv ist. Fassen wir nun $\{0, 1, \ldots, n-1\}$ als die Gruppe $(C_n, \oplus)$ aus § 1.2.2 auf, so erkennen wir leicht, dass es sich bei f um einen Gruppenisomorphismus handelt: Lassen m und m' bei Division durch n den Rest r respektive r', so gilt

$$\begin{aligned} f((m + n\mathbb{Z}) + (m' + n\mathbb{Z})) &= f((r + n\mathbb{Z}) + (r' + n\mathbb{Z})) \\ &= f((r + r') + n\mathbb{Z}) \end{aligned}$$

[3] Der springende Punkt ist, dass eine Nebenklasse aN zwar notationsgemäß mit einem zugehörigen Element $a\in G$ „im Gepäck“ zu kommen scheint, doch ist dieses a nur *bis auf Multiplikation von rechts mit einem Element von N* eindeutig bestimmt. Ob hier $(ab)N = (a'b')N$ für alle $a, a', b, b'\in G$ mit $aN = a'N$ und $bN = b'N$ gilt, wird zu einer Aussage, die man erst beweisen muss.

$$
\begin{aligned}
&= \begin{cases} r + r' & \text{falls } r + r' < n \\ r + r' - n & \text{falls } r + r' \geq n \end{cases} \\
&= r \oplus r' \\
&= f(r + n\mathbb{Z}) \oplus f(r' + n\mathbb{Z}) \\
&= f(m + n\mathbb{Z}) \oplus f(m' + n\mathbb{Z}).
\end{aligned}
$$

Man beachte, dass es für diese Rechnung nicht nötig ist, zu wissen, dass es sich bei $(C_n, \oplus)$ um eine Gruppe handelt. Das kann man beispielsweise benutzen, um nachzurechnen, dass $\oplus$ das Assoziativgesetz erfüllt. (Man entsinne sich daran, dass wir diese jene Verifikation in § 1.2.2 nicht durchgeführt haben.) Hierfür brauchen wir nur, dass $+$ auf $\mathbb{Z}/n\mathbb{Z}$ das Assoziativgesetz erfüllt; Eine Eigenschaft die wir direkt aus der Assoziativität des Komplexproduktes (bzw. im konkreten Fall: der Assoziativität der Addition auf $\mathbb{Z}$) erhalten haben. Für $a, b, c \in C_n$ gilt

$$
\begin{aligned}
[a \oplus b] \oplus c &= [f(a + n\mathbb{Z}) \oplus f(b + n\mathbb{Z})] \oplus f(c + n\mathbb{Z}) \\
&= f((a + n\mathbb{Z}) + (b + n\mathbb{Z})) \oplus f(c + n\mathbb{Z}) \\
&= f([(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z})) \\
&= f((a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})]) \\
&= f(a + n\mathbb{Z}) \oplus f((b + n\mathbb{Z}) + (c + n\mathbb{Z})) \\
&= f(a + n\mathbb{Z}) \oplus [f(b + n\mathbb{Z}) + f(c + n\mathbb{Z})].
\end{aligned}
$$

Beispiel. Wir setzen das Beispiel von eben fort und spezialisieren $n = 2$. Wir betrachten also

$$\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z},\ 1 + 2\mathbb{Z}\} = \{\text{gerade Zahlen, ungerade Zahlen}\}.$$

Die zugehörige Verknüpfungstabelle sieht so aus:

$+$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$0+2\mathbb{Z}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$0+2\mathbb{Z}$.

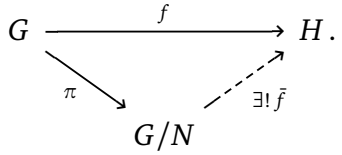
Korollar 2.5. *Sei G eine Gruppe. Dann sind die Normalteiler von G genau die Kerne von Gruppenhomomorphismen mit Definitionsbereich G:*

$$\{\textit{Normalteiler } N \textit{ von } G\} = \{\ker f : H \textit{ Gruppe}, f \in \mathrm{Hom}(G, H)\}.$$

Beweis. Dass Kerne von Gruppenhomomorphismen Normalteiler sind, hatten wir bereits eingangs nachgerechnet (siehe (2.2)). Umgekehrt ist aber auch jeder Normalteiler N von G der Kern eines Gruppenhomomorphismus, nämlich beispielsweise von der kanonischen Projektion $\pi\colon G \to G/N$, $g \mapsto gN$, auf die Faktorgruppe G/N. □

Satz 2.6. *Es sei N ein Normalteiler einer Gruppe G und $f\colon G \to H$ ein Gruppenhomomorphismus in eine Gruppe H. Ferner sei $N \subseteq \ker f$. Dann gibt es genau einen*

Gruppenhomomorphismus $\bar{f}\colon G/N \to H$, der das folgende Diagramm kommutativ macht:

(2.3)


Die Zuordnung $f \mapsto \bar{f}$ stiftet also eine 1:1-Korrespondenz (Bijektion)

$$\{ f \in \mathrm{Hom}(G,H) : N \leq \ker f \} \xrightarrow{1:1} \mathrm{Hom}(G/N,H).$$

Ist $N = \ker f$, so ist $\bar{f}$ injektiv.

Beweis. Zur *Existenz* von $\bar{f}$: Wir *definieren* $\bar{f}(gN) := f(g)$. Dies ist wohl-definiert, denn ist $g_1N = g_2N$, so gibt es laut Lemma 2.4 ein $n \in N$ mit $g_1 = g_2n$ und wir erhalten

$$f(g_1) = f(g_1)1_H = f(g_1)f(n) = f(g_1n) = f(g_2).$$

Man rechnet außerdem sofort nach, dass es sich bei dem so definierten $\bar{f}$ um einen Gruppenhomomorphismus handelt:

$$\bar{f}(aN\,bN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN).$$

Wegen $(\bar{f} \circ \pi)(g) = \bar{f}(\pi(g)) = \bar{f}(gN) = f(g)$ kommutiert (2.3).

Wir zeigen nun die *Eindeutigkeit* von $\bar{f}$: Jedes Element in G/N ist von der Form gN mit einem $g \in G$. Die Kommutativität von (2.3) impliziert, dass $\bar{f}(gN)$ gleich $f(g)$ sein muss. Also ist $\bar{f}$ eindeutig bestimmt.

Die Aussage über die gestiftete 1:1-Korrespondenz ist eine direkte Konsequenz aus der Aussage mit dem Diagramm: Die Injektivität der Abbildung $f \mapsto \bar{f}$ folgt aus der eben bewiesenen Eindeutigkeitsaussage. Für die Surjektivität braucht man nur zu gegebenem $\tilde{f} \in \mathrm{Hom}(G/N,H)$ den Homomorphismus $f := \tilde{f} \circ \pi$ betrachten. Für diesen gilt (wieder dank der Eindeutigkeitsaussage) $\bar{f} = \tilde{f}$.

Sei nun $N = \ker f$. Wegen $\ker \tilde{f} = \{ gN \in G/N : \tilde{f}(gN) = 1_H \} = \{ \pi(g) : g \in G, f(g) = 1_H \} = \pi(\ker f)$ und $\ker \pi = N$ folgt daraus $\ker \tilde{f} = \{1_{G/N}\}$. Aus Proposition 2.3 (5) ergibt sich die Injektivität von $\bar{f}$. □

2.2.2. Erster Isomorphiesatz und Korrespondenzsatz. Satz 2.6 hat bemerkenswerte Konsequenzen. Wir erwähnen zunächst die Folgende:

Korollar 2.7 (Erster Isomorphiesatz)**.** *Es sei $f\colon G \to H$ ein Gruppenhomomorphismus zwischen Gruppen G und H. Dann ist $G/\ker f \cong f(G)$.*

Beweis. Die f zugeordnete Abbildung $\bar{f}\colon G/\ker f \to H$ aus Satz 2.6 ist injektiv und bildet natürlich surjektiv auf ihr Bild ab; dieses stimmt mit dem Bild von f überein, weshalb die eingeschränkte Abbildung $\bar{f}\colon G/\ker f \to f(G)$ ein Gruppenisomorphismus ist. □

Beispiele.

(1) Für jeden Körper K ist die Determinantenabbildung det: $\mathrm{GL}_n K \to K^\times$ (mit $K^\times = K \setminus \{0_K\}$) ein Gruppenepimorphismus mit Kern $\mathrm{SL}_n K$. Insbesondere ist

$$(\mathrm{GL}_n K)/\mathrm{SL}_n K \cong K^\times. \tag{2.4}$$

(2) Die Exponentialabbildung $\mathbb{R} \to \mathbb{C}^\times$, $t \mapsto \exp(2\pi \mathrm{i}\, t)$, ist ein Gruppenhomomorphismus mit Kern $\mathbb{Z}$ und Bild $\mathbb{S}^1 = \{ z \in \mathbb{C} : |z| = 1 \}$. Insbesondere ist $(\mathbb{R}/\mathbb{Z}, +) \cong (\mathbb{S}^1, \cdot)$.

(3) Man kann den ersten Isomorphiesatz benutzen, um die zyklischen Gruppen zu klassifizieren, siehe unten (Korollar 2.8).

Beispiel. Zur Ergänzung wollen wir die Isomorphie in (2.4) auch rein rechnerisch einsehen. Dazu überlegen wir uns, dass jede Nebenklasse $A\,\mathrm{SL}_n K$ mit $A \in \mathrm{GL}_n K$ genau eine Matrix der Form

$$\mathrm{diag}(\lambda, 1, \ldots, 1) = \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} =: D_\lambda$$

mit einem $\lambda \in K^\times$ enthält. Da alle Elemente der Nebenklasse $A\,\mathrm{SL}_n K$ dieselbe Determinante besitzen, folgt $\lambda = \det A$ und dies klärt auch schon, dass jedenfalls nicht zwei verschiedene solche Matrizen in $A\,\mathrm{SL}_n K$ enthalten sind. Je zwei Matrizen vom obigen Typ multiplizieren sich wie folgt: $D_\lambda D_\mu = D_{\lambda\mu}$. Durch scharfes Hinsehen erkennt man hierin die Isomorphie (2.4). Diese lässt sich durch

$$K^\times \longrightarrow (\mathrm{GL}_n K)/\mathrm{SL}_n K, \quad \lambda \longmapsto D_\lambda\, \mathrm{SL}_n K,$$

vermitteln. Nun zu unserer Behauptung über die Existenz einer Diagonalmatrix vom obigen Typus in $A\,\mathrm{SL}_n K$: Man erinnere sich an elementare Spaltenumformungen aus der linearen Algebra. Diese können durch Rechtsmultiplikation mit gewissen Elementarmatrizen bewerkstelligt werden. Sei E_{ij} die $n \times n$-Matrix, welche nur aus Nulleinträgen besteht, bis auf eine Eins im Eintrag der zur i-ten Spalte und j-ten Zeile gehört. Ferner sei $\mathbf{1}_n$ die $n \times n$-Einheitsmatrix. Sei $i \neq j$. Rechtsmultiplikation mit der $(\mathrm{SL}_n K)$-Matrix $\mathbf{1}_n + \mu E_{ij}$ zu einer Matrix A liefert die Matrix A mit j-ter Spalte ersetzt durch die Summe der j-ten Spalte und dem μ-fachen der i-ten Spalte; zum Beispiel:

$$\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} \cdot (\mathbf{1}_3 + 4E_{13}) = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 11 \\ 2 & 5 & 16 \\ 3 & 6 & 21 \end{pmatrix}.$$

Ganz ähnlich bewirkt Rechtsmultiplikation mit der $\mathrm{SL}_n K$-Matrix

$$V_{ij} = \mathbf{1}_n + E_{ij} - E_{ji} - E_{ii} - E_{jj} = (\mathbf{1}_n + E_{ij}) \cdot (\mathbf{1}_n - E_{ji}) \cdot (\mathbf{1}_n + E_{ij}) \quad (i \neq j)$$

eine Vertauschung der i-ten Spalte mit dem Negativen der j-ten Spalte; zum Beispiel:

$$\begin{pmatrix}1&4&7\\2&5&8\\3&6&9\end{pmatrix}\cdot V_{13}=\begin{pmatrix}1&4&7\\2&5&8\\3&6&9\end{pmatrix}\cdot\begin{pmatrix}0&0&1\\0&1&0\\-1&0&0\end{pmatrix}=\begin{pmatrix}-7&4&1\\-8&5&2\\-9&6&3\end{pmatrix}.$$

Im Rahmen der *linearen Algebra* zeigt man, dass diese Spaltenumformungen ausreichen, um jede invertierbare Matrix auf Diagonalgestalt zu transformieren. (Das ist eine leicht eingeschränkte Form des Gauß-Algorithmus.) Durch Rechtsmultiplikation mit den $\mathrm{SL}_n K$-Matrizen $\mathbf{1}_n-(1-\mu)E_{11}-(1-\mu^{-1})E_{jj}$ ($j>1$, $\mu\in K^\times$) kann man diese Diagonaleinträge alle auf den ersten Eintrag „schieben“. Wir illustrieren den hier beschriebenen Prozess anhand eines Beispiels:

$$\begin{aligned}\begin{pmatrix}1&1&-1\\0&4&0\\3&2&0\end{pmatrix}\mathrm{SL}_3\mathbb{R}&=\begin{pmatrix}1&1&1\\0&4&0\\0&2&3\end{pmatrix}\mathrm{SL}_3\mathbb{R}=\begin{pmatrix}1&0&1\\0&4&0\\0&2&3\end{pmatrix}\mathrm{SL}_3\mathbb{R}=\begin{pmatrix}1&0&0\\0&4&0\\0&2&3\end{pmatrix}\mathrm{SL}_3\mathbb{R}\\&=\begin{pmatrix}1&0&0\\0&4&0\\0&0&3\end{pmatrix}\mathrm{SL}_3\mathbb{R}=\begin{pmatrix}4&0&0\\0&1&0\\0&0&3\end{pmatrix}\mathrm{SL}_3\mathbb{R}=\begin{pmatrix}12&0&0\\0&1&0\\0&0&1\end{pmatrix}\mathrm{SL}_3\mathbb{R}.\end{aligned}$$

Korollar 2.8 (Klassifikation zyklischer Gruppen)**.** *Es sei G eine Gruppe und $g\in G$ beliebig. Dann ist entweder $\langle g\rangle\cong\mathbb{Z}$ oder $\langle g\rangle\cong\mathbb{Z}/n\mathbb{Z}$ für ein (und nur ein) $n\in\mathbb{N}$.*

Beweis. Proposition 1.1 (6) zeigt, dass es sich bei $f\colon\mathbb{Z}\to G$, $n\mapsto g^n$ um einen Gruppenhomomorphismus handelt. Korollar 2.7 liefert $\mathbb{Z}/\ker f\cong f(G)=\langle g\rangle$. Da $\ker f$ eine Untergruppe von $(\mathbb{Z},+)$ ist, zeigt Proposition 1.11 $\ker f=n\mathbb{Z}$ für ein $n\in\mathbb{N}_0$. (Speziell im Fall $n=0$ haben wir $\ker f=\{0\}$ und also $\langle g\rangle\cong\mathbb{Z}/\ker f=\mathbb{Z}/\{0\}\cong\mathbb{Z}$.) Durch Betrachtung der jeweiligen Gruppenordnung sieht man $\mathbb{Z}/n\mathbb{Z}\ncong\mathbb{Z}/m\mathbb{Z}$ für alle $n,m\in\mathbb{N}_0$ mit $n\neq m$. Hieraus ergibt sich unmittelbar der Zusatz mit „*entweder* oder“ bzw. „nur ein“. □

Der nächste Satz klärt die Frage nach der Beschaffenheit des Untergruppenverbandes von Faktorgruppen:

Satz 2.9 (Korrespondenzsatz)**.** *Es sei G eine Gruppe, $N\trianglelefteq G$ ein Normalteiler von G und $\pi\colon G\to G/N$, $g\mapsto gN$, bezeichne die kanonische Projektion. Dann handelt es sich bei der Abbildung*

$${}^{\mathrm{a}}\pi\colon\begin{cases}\{\text{Untergruppen } U\leq G/N\}\to\{\text{Untergruppen } V\leq G \text{ mit } V\supseteq N\},\\ U\mapsto\pi^{-1}(U),\end{cases}$$

um eine inklusionserhaltende[4] *Bijektion, welche sich zu einer Bijektion*

$$\{\text{Normalteiler } U\trianglelefteq G/N\}\xrightarrow{1:1}\{\text{Normalteiler } V\trianglelefteq G \text{ mit } V\supseteq N\}$$

einschränkt.

[4] „*Inklusionserhaltend*“ heißt hier: $U\leq U'\leq G/N$ impliziert ${}^{\mathrm{a}}\pi(U)\subseteq{}^{\mathrm{a}}\pi(U')$.

Beweis. Das ist Aufgabe 4.2. □

Bemerkung. Satz 2.9 klärt die bereits bei Beispiel 1.13 und Abbildung 12 bemerkte Ähnlichkeit von Untergruppenverbänden von $C_{12} \cong \mathbb{Z}/12\mathbb{Z}$ (siehe Korollar 2.8) und $\mathbb{Z}$. Man überlege sich hierzu als freiwillige Übung, wie Satz 1.12 mittels Satz 2.9 aus Proposition 1.11 gefolgert werden kann.

2.2.3. Weitere Isomorphiesätze. Wir besprechen nun einige weitere Isomorphiesätze, die manchmal nützlich sind. Diese werden entsprechend durchnummeriert (zweiter und dritter Isomorphiesatz). Einen Konsens darüber, welcher dieser Sätze nun der zweite und welcher der dritte ist, scheint es in der Literatur nicht zu geben. Wir nutzen die Gelegenheit, um auf dem Weg zu den angekündigten Isomorphiesätzen noch einige weitere Werkzeuge bereitzustellen.

Sei $(G_i)_i$ eine (endliche oder unendliche) Folge von Gruppen zusammen mit einer Folge von Gruppenhomomorphismen $f_i\colon G_i \to G_{i-1}$. Wir visualisieren dies in der Form des Diagramms[5]

$$\ldots \longrightarrow G_{i+1} \xrightarrow{f_{i+1}} G_i \xrightarrow{f_i} G_{i-1} \longrightarrow \ldots$$

und nennen dieses Diagramm eine ***Sequenz***.[6] Diese Sequenz heißt ***exakt an der Stelle i*** (oder ***exakt bei G_i***, sofern hierdurch die Position unverwechselbar beschrieben wird), falls $\operatorname{im} f_{i+1} = \ker f_i$ gilt. Die Sequenz heißt ***exakt***, falls sie dies an jeder[7] Stelle ist.

Wir schreiben im Folgenden in Diagrammen auch 0 für die einelementige Gruppe.[8] Man beachte, dass für jede Gruppe G die Mengen $\operatorname{Hom}(0,G)$ und $\operatorname{Hom}(G,0)$ einelementig sind. Eine Sequenz der Form

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

nennt man auch ***kurz***. Ist diese exakt, so spricht man von einer ***kurzen exakten Sequenz***.

Lemma 2.10. *Seien G', G und G'' jeweils Gruppen. Dann gilt:*

(1) Die Sequenz $0 \longrightarrow G' \xrightarrow{f} G$ ist genau dann exakt, wenn f injektiv ist.

(2) Die Sequenz $G \xrightarrow{g} G'' \longrightarrow 0$ ist genau dann exakt, wenn g surjektiv ist.

(3) Die kurze Sequenz $0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$ ist genau dann exakt, wenn f injektiv, g surjektiv und $\operatorname{im} f = \ker g$ ist.

[5] Man kann sich die Position der Indizes so merken: Der in f_i *unten* stehende Index *erniedrigt* den Index von G_i; Man bildet also von G_i nach G_{i-1} ab.

[6] Der Begriff ***Folge*** ist auch in Gebrauch.

[7] An etwaigen Randstellen, also solchen i, für die entweder f_{i+1} oder f_i nicht definiert sind, wird Exaktheit als trivialerweise vorliegend betrachtet.

[8] Man sieht selbstverständlich sofort, dass „die“ einelementige Gruppe bis auf eindeutige Isomorphie eindeutig bestimmt ist und es somit gerechtfertigt ist, hier den bestimmten Artikel zu gebrauchen.

(4) *In der Situation der vorherigen Aussage ist* $G'' \cong G/f(G')$.
(5) *Jeder Gruppenhomomorphismus* $g\colon G \to G''$ *liefert eine kurze exakte Sequenz*
$$0 \longrightarrow \ker g \xhookrightarrow{\text{Inkl.}} G \xrightarrow{g} f(G) \longrightarrow 0\,.$$
(6) *Für jedes* $N \trianglelefteq G$ *ist die kurze Sequenz* $0 \longrightarrow N \xhookrightarrow{\text{Inkl.}} G \xrightarrow{\pi} G/N \longrightarrow 0$ *exakt.*

Beweis. Die fraglichen Aussagen sind unmittelbare Folgerungen aus der Definition von Exaktheit, sowie Korollar 2.7. □

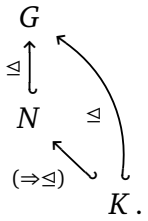
Satz 2.11 (Zweiter Isomorphiesatz)**.** *Es sei* G *eine Gruppe,* $U \leq G$ *und* $N \trianglelefteq G$*. Dann ist auch* $UN \leq G$ *und* $U \cap N \trianglelefteq U$ *sowie* $UN/N \cong U/(U \cap N)$*.*

Beweis. Das ist Aufgabe T4.2; für die behauptete Isomorphie betrachte man das kommutative Diagramm

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & U\cap N & \longrightarrow & U & \longrightarrow & U/(U\cap N) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \vdots\ \exists? & & \\
0 & \longrightarrow & N & \longrightarrow & UN & \longrightarrow & UN/N & \longrightarrow & 0
\end{array}$$

mit exakten Zeilen und Spalten, wobei die eingezeichneten Pfeile die offensichtlichen Gruppenhomomorphismen bezeichnen mögen. □

Satz 2.12 (Dritter Isomorphiesatz)**.** *Ist* G *eine Gruppe mit zwei Normalteilern* N *und* K*, wobei* $K \subseteq N$ *gelten möge:*



Dann ist $(G/K)/(N/K) \cong G/N$.

Beweis. Vorweg bemerken wir, dass $K \leq N$ als Normalteiler von G selbstverständlich auch ein Normalteiler von N ist, da ja $gK = Kg$ für alle $g \in G$ und somit insbesondere für alle $g \in N$ gilt. Bei dem im Satz notierten N/K handelt es sich also tatsächlich um eine Gruppe, ja sogar um eine Untergruppe von G/K. Mehr noch: N/K ist normal in G/K. (Das könnten wir direkt nachrechnen, aber es folgt auch aus der Exaktheit der Zeile (‡) im nachfolgenden Diagramm.) Wir betrachten das kommutative Diagramm

(zunächst ohne die gestrichelten Pfeile)

$$\begin{array}{cccccccccc}
 & & & & 0 & & 0 & & & \\
 & & & & \downarrow & & \downarrow & & & \\
 & & 0 & \longrightarrow & K & = & K & \longrightarrow & 0 & \\
 & & & & \downarrow{\scriptstyle \text{Inkl.}} & & \downarrow{\scriptstyle \text{Inkl.}} & & \downarrow & \\
(\dagger): & & 0 & \longrightarrow & N & \overset{\text{Inkl.}}{\hookrightarrow} & G & \longrightarrow & G/N & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \wr\downarrow{\scriptstyle \mathrm{id}_{G/N}} & & \\
(\ddagger): & & 0 & \longrightarrow & N/K & \dashrightarrow & G/K & \dashrightarrow & G/N & \longrightarrow & 0\,, \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & & 0 & &
\end{array}$$

wobei die unbeschrifteten Pfeile jeweils die kanonischen Homomorphismen bezeichnen mögen. Unter Anwendung von Satz 2.6 ergänzt sich dieses Diagramm um die gestrichelten Pfeile zu einem kommutativen Diagramm mit exakten Spalten und *a-priori* exakter Zeile (†). Eine Diagrammjagd liefert auch die Exaktheit der Zeile (‡). Eine solche Diagrammjagd lesend nachzuvollziehen ist erfahrungsgemäß mühsam. Es sei daher an dieser Stelle auf die folgende Videoaufzeichnung auf YouTube verwiesen:

`https://www.youtube.com/watch?v=89URY9IpZIg`

Hieraus ergibt sich die Behauptung.

Wir geben noch einen zweiten Beweis. Dieser hat den Vorteil, dass er weniger abstrakt ist, verpasst aber die Gelegenheit etwas über Diagrammjagden zu zeigen. Zu $gK \in G/K$ ist das Komplexprodukt $(gK)N = g(KN) = gN$ (gemäß Adsorptionsregel) ein Element von G/N. Wir erhalten also eine Abbildung $f\colon G/K \to G/N$, $gK \mapsto gN$. Man sieht direkt, dass es sich bei dieser Abbildung um einen Gruppenhomomorphismus handelt. Der erste Isomorphiesatz (Korollar 2.7) liefert sodann $G/N \cong (G/K)/\ker f$ und zum Beweis der im aktuellen Satz behaupteten Isomorphie genügt es daher, $\ker f = N/K$ einzusehen. Das ist allerdings einfach, denn $f(gK) = gN$ ist genau dann $= 1_{G/N} = 1_G N = N$, wenn g in N liegt (siehe Lemma 2.4). Also ist $\ker f = N/K$. □

Bemerkung. Man kann sich die Aussage von Satz 2.12 auch merken, wenn man die Faktorgruppenbildung wie einen Bruchstrich interpretiert und K formal „kürzt“:

$$\text{“}\frac{G/\cancel{K}}{N/\cancel{K}} = \frac{G}{N}\text{.“}$$

Wir schauen uns zur Illustration auch noch die Faktorgruppenbildung am vorliegenden Beispiel genauer an. G/K besteht aus den Nebenklassen gK mit $g \in G$. Beim Übergang zu der Faktorgruppe $(G/K)/(N/K)$ bildet man zu jedem Element gK von G/K die

Nebenklasse $(gK)(N/K)$. Man beachte, dass hierunter aber das *Komplexprodukt* von der einelementigen Menge $\{gK\}$ mit $N/K = \{\, nK : n \in N \,\}$ gemeint ist, also

$$(gK)(N/K) = \{\, gKnK : n \in N \,\} = \{\, (gn)K : n \in N \,\}.$$

Das Objekt rechter Hand erkennen wir als eine Menge von Mengen und sogar (vgl. den Beweis des Satzes von Lagrange, Satz 1.7) als eine *Partition* von gN. Diese Darstellung sollte erklären, dass das „Kürzen von K“ in der folgenden Rechnung formal nicht richtig ist:

$$\text{„}(gK)(N/K) = g\cancel{K}N/\cancel{K} = gN.\text{“}$$

Bemerkung. Die im Beweis von Satz 2.12 angesprochene Diagrammjagd wird durch das „Neunerlemma“ aus der homologischen Algebra verallgemeinert.

2.3. Gruppenoperationen

In diesem Abschnitt besprechen wir, inwiefern Gruppen „Symmetrien“ beschreiben.

2.3.1. Operationen und Homomorphismen nach $\mathrm{Sym}(M)$**.** Es sei $(G, \circ)$ eine Gruppe und M eine beliebige Menge. Unter einer ***Gruppen-Links-Operation von G auf M*** (oder nur ***(Gruppen-)Operation von G auf M***) versteht man eine binäre äußere Verknüpfung $\triangleright\colon G \times M \to M$, welche den folgenden Axiomen genügt:

($\triangleright$.1) Für alle $m \in M$ gilt $1_G \triangleright m = m$.
($\triangleright$.2) Für alle $a, b \in G$ und alle $m \in M$ gilt $a \triangleright (b \triangleright m) = (a \circ b) \triangleright m$.

Eine ***Gruppen-Rechts-Operation*** ist eine binäre äußere Verknüpfung $\triangleleft\colon M \times G \to M$, welche den folgenden Axiomen genügt:

($\triangleleft$.1) Für alle $m \in M$ gilt $m \triangleleft 1_G = m$.
($\triangleleft$.2) Für alle $a, b \in G$ und alle $m \in M$ gilt $(m \triangleleft a) \triangleleft b = m \triangleleft (a \circ b)$.

Statt $g \triangleright m$ mit schreiben wir im Folgenden oft nur gm.[9] Statt $m \triangleleft g$ wird in der Literatur oft die Exponentialnotation m^g gebraucht.

Bemerkung. In der Literatur werden (Gruppen-)*Operationen* auch oft als ***Wirkungen*** oder ***Aktionen*** bezeichnet (auf Englisch: ***(group) action***).

Proposition 2.13. *Es sei $(G, \circ)$ eine Gruppe und M eine beliebige Menge. Die Abbildungen*

$$\{\textit{Gruppenoperationen } \triangleright\colon G \times M \to M\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathrm{Hom}(G, \mathrm{Sym}(M)),$$

[9] Bei der Schreibweise „am“ ist im Fall $G = M$, also wenn die Gruppe G auf sich selbst operiert, Vorsicht geboten, da man Gefahr läuft, unter am das Produkt der Elemente a und m mittels der auf G gegebenen Gruppenverknüpfung verstehen zu können.

gegeben durch

$$\Phi(\triangleright) = \begin{cases} G \to \mathrm{Sym}(M) \\ g \mapsto \begin{cases} M \to M \\ m \mapsto g \triangleright m \end{cases} \end{cases} \qquad \textit{und} \quad \Psi(\varphi) = \begin{cases} G \times M \to M \\ (g,m) \mapsto (\varphi(g))(m), \end{cases}$$

sind zueinander inverse Bijektionen. Wir schreiben auch φ für $\Phi(\triangleright)$ und $\triangleright_\varphi$ für $\Psi(\varphi)$.

Beweis. Die Aussage der Proposition wirkt hier deutlich wilder, als ihr Beweis; jener ergibt sich direkt durch schlichtes Nachrechnen und sei hier ausgespart. (Man sollte hier nachrechnen, dass $\Phi(\triangleright)$ wirklich ein Gruppenhomomorphismus von G nach $\mathrm{Sym}(M)$ ist, $\Psi(\varphi)$ wirklich eine Gruppenoperation $G \times M \to M$ liefert und die Verkettungen $\Psi \circ \Phi$ und $\Phi \circ \Psi$ tatsächlich die identischen Abbildungen auf den jeweiligen Mengen liefert.) □

Bemerkung. Proposition 2.13 zeigt, dass Gruppenoperationen „im Wesentlichen dasselbe“ sind, wie Gruppenhomomorphismen nach $\mathrm{Sym}(M)$. Wir werden daher oft nicht zwischen $\triangleright$ und $\varphi = \Phi(\triangleright)$ unterscheiden. Besitzt die Menge M zusätzliche Struktur (z.B. Vektorraumstruktur oder dergleichen), so schränkt man sich gerne auf Gruppenoperationen ein, welche diese zusätzliche Struktur respektieren; in der obigen Proposition wären das dann genau die Gruppenoperationen, welche zu Homomorphismen von G nach $\mathrm{Aut}(M)$ gehören, wobei $\mathrm{Aut}(M)$ hier die Gruppe der strukturerhaltenden Selbstabbildungen von M bezeichne (für Vektorräume M etwa die Gruppe der bijektiven linearen Abbildungen $M \to M$; für Gruppen kennt man eine ähnliche Situation bereits aus Aufgabe 4.1 zu semidirekten Produkten $G \rtimes_\varphi H$: hier operiert H mittels eines Gruppenhomomorphismus $\varphi\colon H \to \mathrm{Aut}(G)$ auf G).

Eine Gruppenoperation[10] φ heißt ***treu***, falls[11] φ injektiv ist. Zu $m \in M$ schreiben wir

$$G(m) = \{\, g \triangleright_\varphi m : g \in G \,\} \subseteq M$$

für die ***Bahn von m*** (oder ***Orbit von m***) unter (der Operation φ von) G. Die Operation φ heißt ***transitiv***, falls eine (und dann jede!) ihrer Bahnen mit M übereinstimmt. Für jedes $m \in M$ ist $G_m := \{\, g \in G : g \triangleright_\varphi m = m \,\}$ eine Untergruppe von G, der ***Stabilisator von m***. Gilt $G_m = G$, so nennen wir m einen ***Fixpunkt*** der Operation; dann ist die einelementige Menge $\{m\}$ eine Bahn. Ein Element m heißt ***Fixpunkt von $g \in G$***, falls $g \triangleright_\varphi m = m$ gilt. Die ***Menge der Fixpunkte*** eines Elements $g \in G$ bezeichnet man mit

$$M^g := \{\, m \in M : g \triangleright_\varphi m = m \,\}.$$

Beispiele 2.14.

(1) Für jede Gruppe G und jede Menge M existiert die triviale Operation $G \to \mathrm{Sym}(M)$, $g \mapsto \mathrm{id}_M$. Diese Operation ist nur für $\#G = 1$ treu. Alle Elemente von M sind Fixpunkte und daher ist diese Operation nur für $\#M = 1$ transitiv.

[10] Gemeint ist hier eigentlich $\triangleright_\varphi$.

[11] Gemeint ist hier wirklich der Gruppenhomomorphismus $\varphi\colon G \to \mathrm{Sym}(M)$.

(2) Für eine Gruppe $(G, \cdot)$ und $a \in G$ sei $\ell_a \colon G \to G$, $x \mapsto a \cdot x$ die Linksmultiplikation mit a. Dann ist

$$\ell_{a\cdot b} = (x \mapsto a \cdot b \cdot x) = (y \mapsto a \cdot y) \circ (x \mapsto b \cdot x) = \ell_a \circ \ell_b,$$

und also die Abbildung $G \to \mathrm{Sym}(G)$, $a \mapsto \ell_a$, ein Gruppenhomomorphismus. Die hierdurch gestiftete Operation von G auf $M = G$ nennt man die ***links-reguläre Operation von G***. Diese ist treu und transitiv. Konkret sieht diese für $g \in G$ und $m \in M = G$ einfach so aus: $g \triangleright m = gm$.

(3) Wir setzen das Beispiel zur Linksmultiplikation fort und betrachten die Rechtsmultiplikation definiert durch $g \triangleright_{\mathrm{r}} m := mg$. Diese ist im Allgemeinen *keine* Gruppen(links)operation: Das Axiom ($\triangleright$.2) würde nämlich für $g, h \in G$ und $m \in M = G$ die Gleichheit von

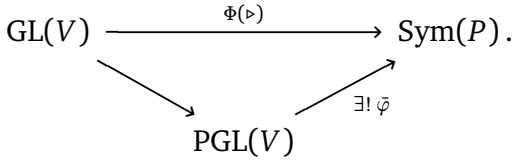
$$h \triangleright_{\mathrm{r}} (g \triangleright_{\mathrm{r}} m) = h \triangleright_{\mathrm{r}} (mg) = mgh \quad \text{und} \quad hg \triangleright_{\mathrm{r}} m = mhg,$$

also $gh = hg$ proklamieren. Für *nicht-abelsche* Gruppen G ist dies nicht für alle g und h erfüllt.

Tatsächlich erhält man aber durch $m \triangleleft g := mg$ eine Gruppen*rechts*operation von G auf sich selbst; Der Nachweis von ($\triangleleft$.2) (und ($\triangleleft$.1)) bereitet dann keine Schwierigkeiten.

Wir verpassen der Rechtsmultiplikation nun noch eine keine Änderung, um aus dieser doch eine Gruppen*links*operation zu machen. Die ***rechts-reguläre Operation von G*** wird durch $a \mapsto (x \mapsto x \cdot a^{-1})$ definiert. (Man beachte hierzu auch Aufgabe 5.1 und die Lösung davon.)

(4) Sei V ein Vektorraum über einem Körper K und P die Menge aller seiner eindimensionalen Unterräume U. Dann operiert die Gruppe $\mathrm{GL}(V)$ aller bijektiven, linearen Abbildungen $f : V \to V$ transitiv auf P via $f \triangleright U := f(U)$. Diese Operation ist aber i.Allg. nicht treu: sowohl id_V wie auch ihre skalaren Vielfachen (mit Skalar $\neq 0$) bewirken die identische Abbildung auf P und dies sind tatsächlich die einzigen linearen Abbildungen, die alle eindimensionalen Unterräume fixieren, wie man sich leicht überlegen kann. Es bezeichne $\mathrm{PGL}(V)$ die Faktorgruppe von $\mathrm{GL}(V)$ nach $Z(\mathrm{GL}(V)) = \{\, \lambda \,\mathrm{id}_V : \lambda \in K \,\}$, die sogenannte ***projektive lineare Gruppe***. Mittels Satz 2.6 erhalten wir ein kommutatives Diagramm



Demnach operiert auch $\mathrm{PGL}(V)$ auf P (via $\bar{\varphi}$) und diese Operation ist sogar treu (siehe Satz 2.6).

(5) Für eine Gruppe $(G,\cdot)$ und $a \in G$ sei $i_a\colon G \to G$, $x \mapsto a \cdot x \cdot a^{-1}$ der durch ***Konjugation mit a*** erhaltene Automorphismus. Dann ist $i : G \to \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, $g \mapsto i_g$ eine Operation auf G, die ***Konjugationsoperation***.

Beispiele hierfür kennt man aus der *linearen Algebra*: Dort ließ man etwa die Gruppe $\mathrm{GL}_n K$ auf $K^{n\times n}$ durch Konjugation operieren. Für Matrizen $A, B \in K^{n\times n}$ bedeutet „B liegt in der Bahn von A unter der Konjugationsoperation von $\mathrm{GL}_n K$ auf $K^{n\times n}$“ genau, dass es eine invertierbare Matrix $T \in \mathrm{GL}_n K$ mit $B = T \triangleright A = TAT^{-1}$ gibt. In der Sprache der *linearen Algebra* heißt dies genau, dass die Matrizen A und B ähnlich zueinander sind. Wann eine Matrix ähnlich zu einer anderen ist wird — jedenfalls für algebraisch abgeschlossene Körper K, wie etwa $K = \mathbb{C}$ — durch die *Jordan-Normalform* von A klassifiziert.

Speziell für $K = \mathbb{C}$ und $n = 2$ zerfällt $K^{n\times n}$ unter Konjugation in die Bahnen von

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

wobei $\{\lambda, \mu\}$ alle zweielementigen Teilmengen von $\mathbb{C}$ durchläuft, und die Bahnen von

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix}, \quad \text{sowie} \quad \begin{pmatrix} \zeta & 1 \\ 0 & \zeta \end{pmatrix},$$

wobei ρ alle komplexen Zahlen durchläuft.

(6) Wir schreiben $(\mathrm{GL}_m K)^{\mathrm{op}}$ für die Gruppe, welche aus der Menge $\mathrm{GL}_m K$ besteht und als Verknüpfung $\bullet$ Matrix-Multiplikation in umgedrehter Reihenfolge hat, also $A \bullet B = BA$. Dann operiert $G = (\mathrm{GL}_n K) \times (\mathrm{GL}_m K)^{\mathrm{op}}$ (mit komponentenweise definierter Verknüpfung $*$) auf $K^{n\times m}$ via $(S,T) \triangleright A := SAT$. Dabei handelt es sich tatsächlich um eine Gruppenoperation. Zum Nachweis von ($\triangleright$.2) beachten wir

$$\begin{aligned}(S',T') \triangleright [(S,T) \triangleright A] &= (S',T') \triangleright (SAT) \\ &= S'(SAT)T' = (S'S)A(TT') \\ &= (S'S, TT') \triangleright A \\ &= (S'S, T' \bullet T) \triangleright A \\ &= [(S',T') * (S,T)] \triangleright A.\end{aligned}$$

(Man beachte den subtilen Tausch von TT' zu $T' \bullet T$, den wir uns durch die mittels $\_^{\mathrm{op}}$ „verdrehte“ Verknüpfung auf $(\mathrm{GL}_m K)^{\mathrm{op}}$ ermöglicht haben.)

Die Operation von G auf $M = K^{n\times m}$ zerlegt M ebenfalls in Bahnen. Aus der *linearen Algebra* weiß man, dass die zugehörigkeit zu den Bahnen über eine einzige numerische Invariante klassifiziert wird: den *Rang* der Matrix! (Stichwort: *Rangnormalform*.) Die Bahnen von M unter G sind also

$$\{A \in K^{n\times m} : \mathrm{rang}\, A = r\}, \quad r = 0, 1, \ldots, \min\{n, m\}.$$

Wir geben beispielhaft für $(n,m) = (2,3)$ Repräsentanten für die 3 Bahnen an:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

(7) (Rotation eines Würfels.) Wir repräsentieren einen Würfel in $\mathbb{R}^3$ durch seine Eckenmenge $M = \{-1,1\}^3 \subset \mathbb{R}^3$ und betrachten die Gruppe $G = \{A \in \mathrm{GL}_3\mathbb{R} : \det A = 1, A^{\mathrm{T}}A = 1, AM = M\}$ aller Drehungen, die diesen Würfel fixieren. Diese operiert treu und transitiv auf M. (Man überlege sich weshalb!) Insbesondere ist G endlich.

Der nächste interessante Satz besagt, dass man jede Gruppe als Untergruppe einer symmetrischen Gruppe wiederfinden kann. In gewisser Weise umfasst das Studium von symmetrischen Gruppen daher das Studium der gesamten Gruppentheorie.

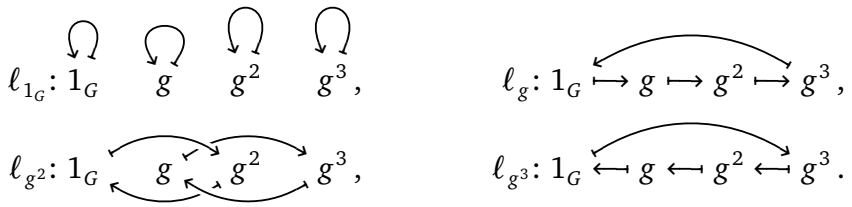
Satz 2.15 (Cayley)**.** *Jede Gruppe G ist isomorph zu einer Untergruppe von* $\mathrm{Sym}(G)$. *Insbesondere, falls G endlich ist, $n = \#G$, ist G isomorph zu einer Untergruppe von $\mathfrak{S}_n$.*

Beweis. Die links-reguläre Operation φ von G aus Beispiel 2.14 (2) ist ein Monomorphismus von G nach $\mathrm{Sym}(G)$ und induziert daher einen Isomorphismus von G auf $\varphi(G) \leq \mathrm{Sym}(G)$. Die Zusatzbemerkung ist wegen $\mathrm{Sym}(G) \cong \mathfrak{S}_{\#G}$ klar. □

Bemerkung. Ernsthaft brauchbar ist Satz 2.15 leider nicht: Die fraglichen symmetrischen Gruppen wachsen sehr rasant mit der Ordnung von G und sind allenfalls schwieriger zu verstehen, als die Gruppe G selbst, mit der man gestartet ist. Beispielsweise würde der Satz uns die symmetrische Gruppe $\mathfrak{S}_n$ in $\mathrm{Sym}(\mathfrak{S}_n) \cong \mathfrak{S}_{n!}$ einbetten — eine Gruppe der Ordnung $n!$!. Zur Illustration:

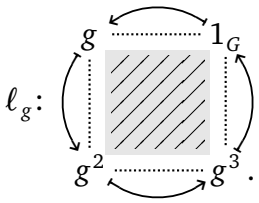
$3! = 6,$	$3!! = 720,$
$4! = 24,$	$4!! = 620.448.401.733.239.439.360.000,$
$5! = 120,$	$5!! = 6.689.502.91\ldots00.000$ (199 Ziffern).

Beispiel. Es sei $(G,\bullet)$ eine multiplikativ geschriebene, zyklische Gruppe der Ordnung 4. (Dann ist G natürlich isomorph zu $\mathbb{Z}/4\mathbb{Z} \cong C_4$ laut Korollar 2.8.) Ist g ein Erzeuger von G, so haben wir $G = \{1_G, g, g^2, g^3\}$. Die Elemente $\ell_{g^k} \in \mathrm{Sym}(G)$ nehmen dann die folgende Gestalt an:



Beschriftet man die Seiten eines Quadrats (regelmäßiges Viereck) mit 1, g, g^2 und g^3, so beschreibt ℓ_g genau eine Drehung des Quadrats um 90° um seinen Mittelpunkt;

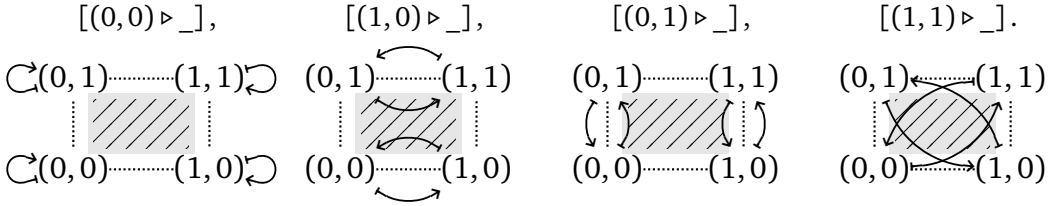
ℓ_{g^2} beschreibt eine Drehung um $2 \cdot 90° = 180°$, ℓ_{g^2} eine Drehung um $3 \cdot 90° = 270°$ und ℓ_{1_G} beschreibt eine Drehung um $0° = 4 \cdot 90°$:



Allgemein beschreibt die zyklische Gruppe $C_n \cong \mathbb{Z}/n\mathbb{Z}$ der Ordnung n die Drehungen eines regelmäßigen n-Ecks, welches jenes n-Eck in sich selbst überführen.

Bemerkung. Operieren zwei Gruppen G und H auf einer Menge M (via $\triangleright_G$) respektive N (via $\triangleright_H$), so operiert das direkte Produkt $G \times H$ durch $(g,h) \triangleright (m,n) := (g \triangleright_G m, h \triangleright_H n)$ auf dem kartesischen Produkt $M \times N$.

Beispiel. Die Gruppe C_2 kommt mit einer transitiven Operation auf der zweielementigen Menge $\{0,1\}$ (vgl. das vorangegangene Beispiel bzw. den Satz von Cayley und dessen Beweis). Dementsprechend operiert die Kleinsche Vierergruppe $V = C_2 \times C_2$ auf der Menge $\{0,1\}^2$:



Man kann sich diese Operation als *Symmetrien eines nichtquadratischen Rechtecks* vorstellen, wenn man dessen Ecken mit den Elementen von $\{0,1\}^2$ beschriftet (siehe oben).

Satz 2.16. *Die Gruppe G operiere auf einer Menge M. Dann gilt:*

(1) Durch $m \sim m' :\Longleftrightarrow (\exists g \in G\colon gm = m')$ wird eine Äquivalenzrelation auf M gestiftet. Die Äquivalenzklassen davon sind genau die Bahnen unter der Operation von G auf M.

(2) Die Bahnen von M unter G bilden eine Partition von M:

$$M = \bigcup_{\text{Bahnen } B}{\cdot}\, B.$$

*(3) (**Bahnformel**:) Ist G endlich und $m \in M$, so ist*

$$\#G(m) = [G : G_m] = \#G/\#G_m.$$

*(Merkspruch: „**Bahnlänge = Stabilisatorindex**“.)*

Beweis. Die erste Aussage rechnet man unmittelbar nach. Die zweite Aussage folgt sofort aus der ersten. Zum Beweis der dritten Aussage sei $m \in M$ fixiert. Die Abbildung

$$E\colon G \to G(m), \quad g \mapsto g \triangleright m,$$

ist surjektiv und für jedes $g \in G$ ist $E^{-1}(g \triangleright m) = gG_m$ wegen

$$\begin{aligned} h \in E^{-1}(g \triangleright m) &\iff E(h) = g \triangleright m \iff h \triangleright m = g \triangleright m \\ &\iff g^{-1} \triangleright (h \triangleright m) = g^{-1} \triangleright (g \triangleright m) \\ &\iff (g^{-1} \circ h) \triangleright m = (g^{-1} \circ g) \triangleright m \\ &\iff (g^{-1} \circ h) \triangleright m = 1_G \triangleright m = m \\ &\iff g^{-1} \circ h \in G_m \\ &\iff h \in gG_m. \end{aligned}$$

Ist G endlich, so ist $\#E^{-1}(g \triangleright m) = \#gG_m = \#G_m$. Die Urbilder $E^{-1}(n) \subseteq G$ mit $n \in G(m) \subseteq M$ bilden eine Partition von G und daher gilt

$$\#G = \sum_{n \in G(m)} \#E^{-1}(n) = \sum_{n \in G(m)} \#G_m = \#G(m) \cdot \#G_m. \qquad \square$$

Beispiel 2.17. In Fortsetzung unserer Überlegungen zur Rotation des Würfels aus Beispiel 2.14 (7) (repräsentiert durch seine Eckenmenge $M = \{-1, 1\}^3 \subset \mathbb{R}^3$) bestimmen wir nun $\#G$. Für ein beliebiges $m \in M$ ist $\#G_m = 3$ (Drehungen um die Gerade $\mathbb{R}m$) und $G(m) = M$ (wegen Transitivität) und also $\#G = 24$ nach Satz 2.16 (3).

Bemerkung. Sei $\triangleright\colon G \times M \to M$ eine Linksoperation. Dann schreibt man auch $G \setminus M$ für die Menge der Bahnen von M unter $\triangleright$. (Man sei explizit im Bezug auf etwaige Verwechslungsgefahr mit der mengentheoretischen Komplementbildung gewarnt, falls $G \subseteq M$ gilt.) Ist $\triangleleft\colon M \times G \to M$ eine Rechtsoperation, so schreibt man M/G für die Menge der Bahnen von M unter $\triangleright$.

Jede Untergruppe $U \leq G$ operiert von rechts auf G durch Rechtsmultiplikation. Bei der Menge G/U von Bahnen unter dieser Operation handelt es sich genau um die bereits vom Satz von Lagrange (Satz 1.7) bekannten und in § 2.2 weiter studierten *Linksnebenklassen* von U in G.

Wir bemerken, dass Satz 2.16 die Idee aus dem Beweis vom Satz von Lagrange verallgemeinert.

Beweis von Satz 1.7 (Satz von Lagrange). Die Gruppe G operiert durch elementweise Verknüpfung auf der Menge $M = G/U$ aller Linksnebenklassen gU ($g \in G$). Satz 2.16 liefert nun $\#G(U) = \#G/\#G_U$. Wegen $\#G_U = \#U$ folgt daraus die Behauptung. $\square$

Das nächste Ergebnis ist auch als „***Lemma von Burnside***“ bekannt, stammt allerdings nicht ursprünglich von Burnside:

Satz 2.18 (Cauchy–Frobenius)**.** *Eine endliche Gruppe G operiere auf einer endlichen Menge M. Dann ist*

$$\#\{\textit{Bahnen der Operation}\} = \frac{1}{\#G} \sum_{g \in G} \#M^g.$$

Beweis. Es ist

$$\sum_{g\in G}\#M^g=\sum_{\substack{g\in G\\ g\triangleright m=m}}\sum_{m\in M}1=\sum_{\substack{m\in M\\ g\triangleright m=m}}\sum_{g\in G}1=\sum_{m\in M}\#G_m=\sum_{m\in M}\frac{\#G}{\#G(m)},$$

wobei die letzte Gleichung durch Anwendung von Satz 2.16 (3) entsteht. Gruppiert man nun die Summationsvariable $m\in M$ gemäß der Bahnen, so sieht man, dass jeder Term $\#G/\#G(m)$ zur Bahn $G(m)$ genau $\#G(m)$ mal auftritt; Jede Bahn liefert also einen Beitrag $\#G$ und die gesamte Summe ist darum $\#G$ mal die Anzahl der Bahnen:

$$\sum_{g\in G}\#M^g=\sum_{\text{Bahnen } B}\sum_{m\in B}\frac{\#G}{\#B}=\sum_{\text{Bahnen } B}\#G=\#\{\text{Bahnen der Operation}\}\cdot\#G.$$

Hieraus folgt die behauptete Gleichung. □

2.3.2. Operation einer Gruppe auf sich selbst. Wir schließen diesen Abschnitt mit einer Anwendung von Gruppenoperationen zum Studium von Gruppen selbst. Betrachte hierzu die Konjugationsoperation i aus Beispiel 2.14 (5). Zu $m\in G$ nennt man die Bahn $\{ama^{-1}:a\in G\}$ die ***Konjugationsklasse von m***. Ihre Elemente nennen wir ***konjugiert*** zu m. (Man vergleiche dieses Konzept mit der aus der linearen Algebra bekannten Ähnlichkeit von Matrizen.) Der ***Zentralisator*** $\mathrm{Cs}_G(m)=\{a\in G: am=ma\}$ ist der Stabilisator von m unter der Konjugationsoperation (und somit insbesondere eine Untergruppe von G). Das ***Zentrum von G*** ist

$$\begin{aligned}Z(G)=\bigcap_{m\in G}\mathrm{Cs}_G(m)&=\{a\in G:\forall m\in G \text{ ist } am=ma\}\\&=\{a\in G: i_a=\mathrm{id}_G\}\\&=\ker i\end{aligned}$$

mit der Konjugationsoperation $i\colon G\to\mathrm{Sym}(G)$ aus Beispiel 2.14 (5). Gemäß Korollar 2.5 ist $Z(G)$ ein Normalteiler von G.

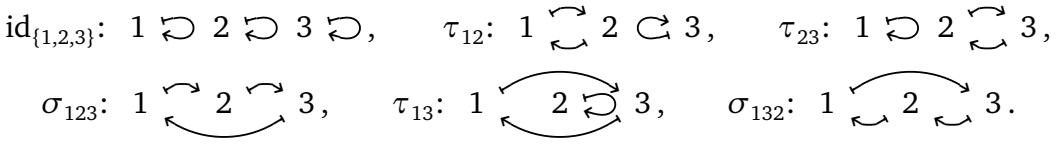
Korollar 2.19 (Klassengleichung)**.** *Sei G eine endliche Gruppe und $m\in G$. Dann hat die Konjugiertenklasse von m genau $[G:\mathrm{Cs}_G(m)]$ viele Elemente. Überdies gilt die sogenannte **Klassengleichung**:*

$$\#G=\#Z(G)+\sum_K\#K,$$

wobei K alle nicht-einelementigen Konjugiertenklassen durchläuft.

Beweis. Die Behauptungen sind ein Spezialfall der Aussagen (3) und (2) in Satz 2.16 für die Konjugationsoperation i unter Beachtung dessen, die Konjugiertenklasse von m genau die Bahn von m unter der Konjugationsoperation ist und dessen, dass das Zentrum $Z(G)$ genau die Menge der $g\in G$ ist, deren Bahn unter i einelementig ist. □

Beispiel. Die symmetrische Gruppe $\mathfrak{S}_3$ besteht bekanntlich aus den folgenden sechs Elementen:

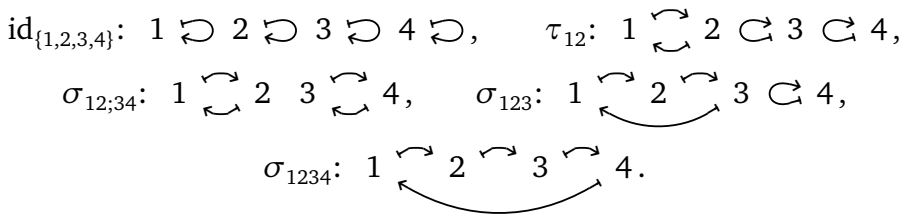


$\mathfrak{S}_3$ zerfällt in drei Konjugationsklassen:

$$Z(\mathfrak{S}_3) = \{\mathrm{id}_{\{1,2,3\}}\}, \quad \{\tau_{12}, \tau_{13}, \tau_{23}\} \quad \text{und} \quad \{\sigma_{123}, \sigma_{132}\}.$$

(Das könnte man an dieser Stelle von Hand nachrechnen. Allerdings folgt dies auch direkt aus Korollar 4.3 (2); Ein Ergebnis, welches wir später beweisen.) Die Klassengleichung liest sich hier als „$6 = 1 + 3 + 2$“.

Beispiel. Die symmetrische Gruppe $\mathfrak{S}_4$ hat $4! = 24$ Elemente. Sie zerfällt in fünf Konjugationsklassen (was man wieder unter Vorgriff auf Korollar 4.3 (2) bestätigen kann). *Repräsentanten* eben jener Klassen sind beispielsweise wie folgt gegeben:



Die zugehörigen Konjugationsklassen haben (wie man sich überlegen kann; der Reihe nach) 1, 6, 3, 8 und 6 Elemente. Es gilt $1 + 6 + 3 + 8 + 6 = 24$.

Die Klassengleichung (Korollar 2.19) kann zur Charakterisierung von Gruppen mit Ordnung p^2 (p prim) benutzt werden:

Korollar 2.20. *Für jede endliche Gruppe G mit Primzahlpotenzordnung $p^n > 1$ ist $Z(G) \supsetneq \{1_G\}$. Ist außerdem $n \leq 2$, so ist G abelsch.*

Beweis. Das ist Aufgabe 5.3. □

2.4. Färbungen und der Satz von Pólya–Redfield

Es sei $M = \{\bullet_1, \bullet_2, \bullet_3, \bullet_4, \ldots, \bullet_k\}$ eine endliche Menge. Wir wollen nun die Elemente von M mit einer Menge $F = \{\text{Rot}, \text{Blau}, \ldots, \text{Grün}\}$ färben, z.B.

$$\bullet_1,\ \bullet_2,\ \bullet_3,\ \bullet_4,\ \ldots,\ \bullet_k.$$

Dies korrespondiert zu einer *Abbildung* $f\colon M \to F$ mit

$$f(\bullet_1) = \text{Blau},\ f(\bullet_2) = \text{Grün},\ f(\bullet_3) = \text{Rot},\ f(\bullet_4) = \text{Rot},\ \ldots,\ f(\bullet_k) = \text{Blau}.$$

Die *Anzahl solcher Abbildungen* — und damit die Anzahl solcher Färbungen — ist $(\#F)^{\#M}$, denn für jedes Element von M hat man genau $\#F$ viele Möglichkeiten zum Färben:

$$\mathrm{Abb}(M,F) \xrightarrow[f\mapsto(\bullet\mapsto f(m))_m]{1:1} \prod_{m\in M} \mathrm{Abb}(\{\bullet\},F) \xrightarrow[(\bullet\mapsto c_m)_m\mapsto(c_m)_m]{1:1} \prod_{m\in M} F\,.$$

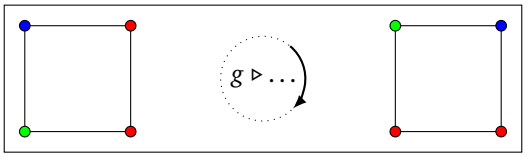


Abbildung 14. Färbung f der Ecken eines Quadrats und Färbung $g \curvearrowright f$, wobei g durch Drehung des Quadrats um 90° im Uhrzeigersinn operiert.

Bemerkung. Man beachte, dass gemäß unserer Interpretation eine Färbung mit Farben aus einer Menge F auch in offensichtlicher Weise eine Färbung mit jeder Menge $F' \supseteq F$ ist: nicht jede Farbe aus der Farbmenge muss auch wirklich vorkommen (vgl. etwa die beiden Randfälle in Beispiel 2.22).

Nun operiere eine endliche Gruppe $(G,\circ)$ auf M mittels $\triangleright$. Dann operiert G auch auf der Menge der Färbungen via

$$g \curvearrowright f := [m \mapsto f(g^{-1} \triangleright m)]. \tag{2.5}$$

(Siehe Abbildung 14 für eine Veranschaulichung hierzu.) Dies ist tatsächlich eine Operation: ($\triangleright$.1) ist klar und zum Nachweis von ($\triangleright$.2) beachte man

$$\begin{aligned}(g\circ h)\curvearrowright f &= [m\mapsto f([g\circ h]^{-1}\triangleright m)]\\ &= [m\mapsto f([h^{-1}\circ g^{-1}]\triangleright m)]\\ &= [m\mapsto f(h^{-1}\triangleright[g^{-1}\triangleright m])]\\ &= g\curvearrowright(h\curvearrowright f).\end{aligned}$$

Bemerkung (Kontravarianz von $\mathrm{Abb}(\_,F)$)**.** Dass man in (2.5) die Inversion tatsächlich „braucht“, um eine Operation zu erhalten, wird klarer, wenn man statt Bijektionen $M\to M$ (Elemente von $\mathrm{Sym}(M)$) auf Abbildungen $M\to M'$ zwischen zwei Mengen M und M' schaut. Jede solche Abbildung $M \xrightarrow{\sigma} M'$ induziert nämlich eine Abbildung

$$\_\circ\sigma\colon\ \mathrm{Abb}(M',F)\longrightarrow\mathrm{Abb}(M,F),\quad (M'\xrightarrow{f}F)\longmapsto(M\xrightarrow{\sigma}M'\xrightarrow{f}F).$$

Indes induziert eine Verkettung $\tau\circ\sigma\colon M\xrightarrow{\sigma}M'\xrightarrow{\tau}M''$ eine Abbildung

$$\mathrm{Abb}(M'',F)\xrightarrow{\_\circ\tau}\mathrm{Abb}(M',F)\xrightarrow{\_\circ\sigma}\mathrm{Abb}(M,F)\,.$$

Um dieses „Umdrehen von Pfeilen“ zu beheben, schaut man zu jeder Bijektion(!) $\sigma\colon M \to M'$ nicht auf die von σ induzierte Abbildung $\mathrm{Abb}(M', F) \to \mathrm{Abb}(M, F)$, sondern auf die von σ^{-1} induzierte Abbildung $\mathrm{Abb}(M, F) \to \mathrm{Abb}(M', F)$.

Kehrt man zurück zu der Operation in (2.5), so sieht man für zwei Färbungen $f, f' \in \mathrm{Abb}(M, F)$

$$\begin{aligned} f' \in G(f) &\iff \exists g \in G\colon f' = g \curvearrowright f \\ &\iff \exists g \in G\colon f' = [m \mapsto f(g^{-1} \triangleright m)] \\ &\iff \exists g \in G\ \forall m \in M\colon f'(m) = f(g^{-1} \triangleright m) \\ &\iff \exists g \in G\ \forall m \in M\colon f'(g \triangleright m) = f(m). \end{aligned}$$

Zwei Färbungen liegen darum genau dann in derselben Bahn unter G, wenn es ein Element $g \in G$ gibt, welches eine Permutation der Elemente von M derart bewirkt, dass die eine Färbung auf den permutierten Elementen mit der zweiten Färbung auf den unpermutierten Elementen übereinstimmt. Wir betrachten dann zwei Färbungen als „dieselbe“ Färbung, falls jene Färbungen in derselben Bahn der Operation von G liegen. Wir sind jetzt daran interessiert, die Anzahl der „tatsächlich verschiedenen“ Färbungen zu bestimmen, d.h. die Anzahl der Bahnen unter der Operation von G zu bestimmen.

Satz 2.21 (Pólya–Redfield)**.** *Eine endliche Gruppe $(G, \circ)$ operiere auf einer endlichen Menge M mittels $\triangleright$. Es sei F eine weitere endliche Menge. Dann ist die Anzahl der Bahnen von G auf* $\mathrm{Abb}(M, F)$ *bezüglich der in (2.5) definierten Operation gegeben durch*

$$\frac{1}{\#G} \sum_{g \in G} (\#F)^{\varrho(g)},$$

wobei $\varrho(g)$ die Anzahl der Bahnen der induzierten Operation

$$\langle g \rangle \xhookrightarrow{\text{Inkl.}} G \xrightarrow{\Phi(\triangleright)} \mathrm{Sym}(M)$$

bezeichnet (d.h. $\triangleright|_{\langle g \rangle \times M}\colon \langle g \rangle \times M \to M$).

Beweis. Mit Blick auf den Satz von Cauchy–Frobenius (Satz 2.18) genügt es einzusehen, dass $(\#F)^{\varrho(g)}$ die Anzahl der von g fixierten Elemente von $\mathrm{Abb}(M, F)$ ist. Offensichtlich ist

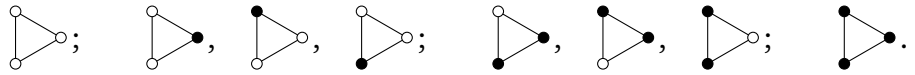
$$\begin{aligned} f = g \curvearrowright f &\iff \forall m \in M\colon f(g \triangleright m) = f(m) \\ &\iff f \text{ ist konstant auf jeder } g\text{-Bahn.} \end{aligned}$$

Es gilt also die Anzahl der Abbildungen $f\colon M \to F$ zu bestimmen, die konstant auf jeder g-Bahn[12] sind; für jede Bahn hat man dabei $\#F$ Möglichkeiten einen Funktionswert zu wählen und somit insgesamt $(\#F)^{\varrho(g)}$ solche Abbildungen, wie behauptet. □

[12] Gemeint sind die Bahnen, in welche M bezüglich der induzierten Operation $\Phi(\triangleright)|_{\langle g \rangle}$ zerfällt.

Wir illustrieren Satz 2.21 anhand eines Beispiels; eine Variante hiervon ist Aufgabe 6.1.

Beispiel 2.22 (Schwarz–Weiß-Färbungen von Dreiecken)**.** Es gibt $2^3 = 8$ Färbungen der Ecken eines gleichseitigen Dreiecks mit den Farben[13] Schwarz und Weiß:



Die Gruppe C_3 operiert durch Drehung auf dem Dreieck und somit auf den Färbungen. Die hierbei entstehenden Bahnen sind durch Semikola abgetrennt; es sind genau vier Stück. — Wir wollen die Antwort „4“ auf die Frage nach der Anzahl der hier gezählten Färbungen auch mittels Satz 2.21 erhalten. $C_3 = \{0, 1, 2\}$ besitzt drei Elemente:

- das neutrale Element 0, welches eine Drehung des Dreiecks um 0° bewirkt und somit alle Ecken fixiert (die Anzahl der 0-Bahnen ist also 3, da jede Ecke eine eigene Bahn bildet) und
- die beiden C_3-erzeugenden Elemente 1 und 2, welche transitive Operationen auf den Ecken induzieren.

Die Anzahl der essentiell verschiedenen Färbungen der Ecken eines gleichseitigen Dreiecks mit k Farben ist also

$$\frac{1}{\#C_3}(k^{\varrho(0)} + k^{\varrho(1)} + k^{\varrho(2)}) = \frac{1}{\#C_3}(k^3 + k^1 + k^1) = \frac{1}{3}(k^3 + 2k).$$

Speziell für $k = 2$ erhalten wir $\frac{1}{3}(8 + 2 \cdot 2) = \frac{12}{3} = 4$, wie erwartet.

[13] Ob man Schwarz und Weiß als „Farben“ bezeichnen darf, sei an dieser Stelle zu ignorieren.

KAPITEL 3

Sätze von Sylow

Zum besseren Verständnis einer Gruppe G ist man vielleicht versucht die Untergruppen von G zu verstehen und sich so „vom Kleinen zum Großen“ vorzuarbeiten. Wir interessieren uns vorwiegend für endliche Gruppen. Hier schränkt der Satz von Lagrange (Satz 1.7) unsere Suche nach Untergruppen schon weiter ein. Gibt es stets zu jedem Teiler d von $\#G$ eine Untergruppe U von G mit $\#U = d$? — Nein, im Allgemeinen nicht! (Das kleinste Beispiel hierzu liefert die noch später zu definierende 12-elementige Gruppe $G = A_4 \leq \mathfrak{S}_4$ mit $d = 6$; siehe Seite 71.) Die Sätze von Sylow hingegen erlauben für *gewisse Teiler* d aber *doch* eine Umkehrung des Satzes von Lagrange und geben gegebenenfalls auch feinere Information über die Anzahl der fraglichen Untergruppen.

3.1. Sätze über p-Untergruppen

Satz 3.1 (Sylow 1872). *Sei G eine endliche Gruppe und p^n eine Primzahlpotenz, die $\#G$ teilt. Dann hat G eine Untergruppe der Ordnung p^n.*

Der Spezialfall des obigen Satzes für $n = 1$ ist auch als *Satz von Cauchy* bekannt. Wir geben einen eleganten Beweis von Wielandt (1959), der sich eine der gesuchten Gruppen als Stabilisator eines Elementes unter einer geeigneten Gruppenoperation beschafft.

Wir benötigen noch ein Lemma über Teilbarkeit durch Primzahlen:

Lemma 3.2 (Lemma von Euklid). *Teilt eine Primzahl*[1] *p ein Produkt ab ganzer Zahlen a und b, so teilt diese auch a oder b.* *($p \mid ab$, p prim $\Longrightarrow$ $p \mid a$ oder $p \mid b$.)*

Beweis. Es gelte $p \nmid a$. Dann sind p und a teilerfremd. Nach dem Lemma von Bézout (Lemma 1.6) gibt es Zahlen $x, y \in \mathbb{Z}$ mit $1 = xp + ya$. Multiplikation mit b liefert $b = xpb + yab$. Gilt nun $p \mid ab$, so folgt hieraus $p \mid b$ und das Lemma ist bewiesen. □

Wir wenden Lemma 3.2 weiter unten auf (3.3) an. Um Missverständnisse über dabei benutzte Schlussweise zu vermeiden, beleuchten wir die Situation an einem konkreten Zahlenbeispiel: Die Zahl

$$100 = 75 \cdot \frac{4}{3} \tag{3.1}$$

[1] Achtung: die Aussage des Lemmas ist für nicht-Primzahlen (sogenannte ***zusammengesetzte*** Zahlen) i.Allg. falsch: $6 \mid 2 \cdot 3$, aber $6 \nmid 2, 3$.

ist durch 2 teilbar. Natürlich können wir Lemma 3.2 nicht anwenden um zu sagen, dass 2 den Bruch $\frac{4}{3}$ teilen müsse, weil 2 ja nicht den Faktor 75 teilt. — Der Bruch $\frac{4}{3}$ ist nämlich gar keine ganze Zahl und Lemma 3.2 lässt sich so nicht anwenden. Wir können allerdings sagen, dass 2 den *Zähler* 4 von fraglichem Bruch teilen *muss*, denn nach Multiplikation mit dem Nenner schreibt sich (3.1) ja als

$$100 \cdot 3 = 75 \cdot 4$$

und 2 teilt die linke Seite, aber nicht den Faktor 75 auf der rechten Seite, und teilt also laut Lemma 3.2 den zweiten Faktor auf der rechten Seite. (Dass 2 ein Teiler von 4 ist, sehen wir natürlich auch ganz ohne Lemma 3.2 sofort, aber unser Argument von oben zeigt, dass eine Primzahl p, welche ein Produkt $u\frac{a}{b} \in \mathbb{Z}$ teilt, schon u oder a teilen muss, auch wenn $\frac{a}{b}$ selbst nicht ganzzahlig ist. Das Argument verallgemeinert sich auch leicht auf Produkte mit mehreren Brüchen.)

Das soeben anhand eines Beispiels aufgezeigte Phänomen, dass Faktorisierungen in $\mathbb{Z}$ sich auch auf Faktorisierungen in $\mathbb{Q}$, dem Quotientenkörper von $\mathbb{Z}$ (siehe später!), ausweiten, wird in uns in Kapitel 9 noch in größerer Allgemeinheit bei der Betrachtung lokaler Exponentialbewertungen $\nu_p(\,\cdot\,)$ wieder begegnen (siehe Proposition 9.1).

Beweis von Satz 3.1. (Das folgende schöne Argument stammt von H. Wielandt [47].) Es bezeichne M die Menge aller p^n-elementigen Teilmengen von G. Dann operiert G auf M durch Linksmultiplikation. Für jedes $m \in \mathscr{M} \in M$ ist die Abbildung $G_{\mathscr{M}} \to \mathscr{M}$, $g \mapsto g \circ m$, injektiv und daher

$$\#G_{\mathscr{M}} \leq \#\mathscr{M} = p^n. \tag{3.2}$$

Hätte man Gleichheit in (3.2), so wäre $G_{\mathscr{M}} \leq G$ eine der gesuchten Untergruppen mit p^n Elementen. Zwar gilt hier leider im Allgemeinen keine Gleichheit, wie das unten folgende Beispiel belegt, doch kann man zeigen, dass Gleichheit *wenigstens für ein* $\mathscr{M}_0 \in M$ gelten muss.

Wir schreiben nun $\#G = p^n u$ mit $u \in \mathbb{N}$ und schreiben p^r für die höchste p-Potenz die noch in u aufgeht. Nun ist

$$\#M = \binom{\#G}{p^n} = \binom{p^n u}{p^n} = \prod_{j=0}^{p^n-1} \frac{p^n u - j}{p^n - j} = u \prod_{j=1}^{p^n-1} \frac{p^n u - j}{p^n - j}. \tag{3.3}$$

Offenbar ist $\#M$ nur dann durch p^{r+1} teilbar, wenn p einen Zähler im hinteren Produkt über j teilt. Letzteres ist allerdings nach vollständigem Kürzen nicht der Fall, denn jede p-Potenz p^k, die im j-ten Faktor den Zähler teilt, teilt auch j (beachte $k < n$, denn $j/p^n \notin \mathbb{Z}$ für $1 \leq j \leq p^n - 1$ und also $p^n \nmid (p^n u - j)$; also gilt $p^k \mid p^n u$ und somit $p^k \mid j$) und somit den Nenner. (Bei dieser Überlegung, welche Teilbarkeit eines Produktes auf Teilbarkeit der Faktoren zurückführt, geht Lemma 3.2 ein.)

Da die Summe der Bahnlängen gleich $\#M$ ist (Satz 2.16 (2)), sieht man nun, dass es eine Bahn $G(\mathscr{M}_0)$ geben muss, deren Länge *nicht* durch p^{r+1} geteilt wird. Nach Satz 2.16 (3) ist p^n also ein Teiler von $\#G_{\mathscr{M}_0}$ (siehe Aufgabe 6.3 für mehr Details

dazu). Zusammen mit (3.2) folgt dann $\#G_{\mathscr{M}_0} = p^n$ und wir haben eine p^n-elementige Untergruppe von G gefunden. □

Bemerkung. Für das Zahlenbeispiel $\#G = 6$, $p^n = 3^1$ und $u = 2$ nimmt (3.3) die Gestalt

$$\binom{6}{3} = 2 \prod_{j=1}^{2} \frac{3^1 2 - j}{3^1 - j} = 2 \cdot \frac{6-1}{3-1} \cdot \frac{6-2}{3-2} = 2 \cdot \frac{5}{2} \cdot \frac{4}{1} \quad (= 20 \in \mathbb{Z})$$

an. Der hierin auftretende Bruch $5/2$ zeigt, dass mit Teilbarkeitsargumenten angewandt auf (3.3) Vorsicht geboten ist: Die dort im Produkt auftretenden *Faktoren* sind im Allgemeinen *keine ganzen Zahlen*, sondern lediglich *rationale* Zahlen.

Beispiel. Wir betrachten die zyklische Gruppe $(C_4, \oplus)$, welche wir im Folgenden auch als G notieren. Die folgende Tabelle zeigt, wie G mittels Linksverknüpfung auf der Menge M der 2-elementigen Teilmengen $\mathscr{M}$ von G operiert.

2-Teilmenge $\mathscr{M} \subset G$	$\{0,1\}$	$\{0,2\}$	$\{0,3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$
Stabilisator $G_{\mathscr{M}} \leq G$	$\{0\}$	$\{0,2\}$	$\{0\}$	$\{0\}$	$\{0,2\}$	$\{0\}$
Ordnung $\#G_{\mathscr{M}}$	1	2	1	1	2	1

Man sieht deutlich, dass nicht alle Stabilisatoruntergruppen Ordnung 2 haben,[2] es aber trotzdem eine solche gibt (die hier für zwei $\mathscr{M}$ auftritt). Man bestätigt ebenfalls mühelos, dass es bezüglich der Operation von G auf M zwei Bahnen gibt, nämlich die zweielementige Bahn $\{\{0,2\},\{1,3\}\}$ und eine weitere (vierelementige) Bahn.

Es sei nun G eine endliche Gruppe und p^m eine Primzahlpotenz mit $p^m \mid \#G$ und $p^{m+1} \nmid \#G$. Eine Untergruppe $P \leq G$ mit Ordnung p^m heißt ***p*-Sylowgruppe von *G***. Die Menge aller p-Sylowgruppen von G bezeichnen wir mit

$$\mathrm{Syl}_p G := \{ P \leq G : \#P = p^m \}.$$

Satz 3.1 garantiert, dass $\mathrm{Syl}_p G$ nicht leer ist.

Eine endliche Gruppe H heißt ***p*-Gruppe** (p prim), falls $\#H = p^k$ für ein $k \in \mathbb{N}_0$ gilt. Die einelementige Gruppe ist wegen $1 = p^0$ auch eine p-Gruppe. Untergruppen $H \leq G$ einer Gruppe G nennt man auch ***p*-Untergruppen**, falls diese p-Gruppen sind.

Satz 3.3 (Sylow). *Es sei G eine endliche Gruppe, p prim und $\#G = p^m u$ mit $p \nmid u$.*

(1) Jede p-Untergruppe von G liegt in einer p-Sylowgruppe.

(2) Je zwei p-Sylowgruppen sind konjugiert in G.

(3) Die Anzahl $\#\mathrm{Syl}_p G$ der p-Sylowgruppen von G ist

(a) ein Teiler von u und

(b) von der Form $1 + kp$ mit einem $k \in \mathbb{N}_0$.

[2] D.h. in (3.2) kann die Ungleichung „$\leq$“ strikt sein.

Beweis. Wir beginnen mit einer Vorbetrachtung. Laut Satz 3.1 gibt es eine p-Sylowgruppe $P \leq G$. Wir betrachten dann die Menge

$$M = \{ gPg^{-1} : g \in G \} = \{ i_g(P) : g \in G \}.$$

(Bei den Elementen von M handelt es sich als Bilder von $P \leq G$ unter $i_g \in \mathrm{Aut}(G)$ natürlich selbst um Untergruppen von G.) Nach Definition operiert G durch Konjugation transitiv auf M mit dem Stabilisator

$$G_P = \{ g \in G : gPg^{-1} = P \},$$

welcher auch als ***Normalisator*** bezeichnet wird. Der Turmsatz (Aufgabe 2.2) angewandt auf $P \leq G_P \leq G$ zeigt:

$$\#M = \#G(P) = [G : G_P] \quad \text{teilt} \quad [G : G_P][G_P : P] = [G : P]. \tag{3.4}$$

Wegen $p \nmid [G : P] = \#G/\#P$ (nach Definition der p-Sylowgruppen) ist $\#M$ somit auch nicht durch p teilbar.

(1): Es sei $U \leq G$ eine p-Gruppe. Dann operiert auch U durch Konjugation auf M. Laut Satz 2.16 (3) ist dann aber jede Bahnlänge unter dieser Operation eine Potenz von p. Da die Summe aller Bahnlängen aber $\#M$ ist und nicht von p geteilt wird, muss es mindestens eine Bahn der Länge $1 = p^0$, also einen Fixpunkt $Q \in M$ (unter der Operation von U auf M), geben. Für alle $u \in U$ gilt dann $uQu^{-1} = Q$, also $uQ = Qu$ und somit $UQ = QU$. Aus Aufgabe 3.3 ergibt sich dann, dass UQ eine Untergruppe von G, — ja sogar eine p-Gruppe, — ist. Wegen $Q \leq UQ$ und $Q \in \mathrm{Syl}_p G$ folgt $Q = UQ$, also $U \leq Q$.

(2): Nun sei U eine beliebige p-Sylowgruppe von G. Die eben für den Beweis von Teil (1) benutzte Argumentation liefert die Existenz eines $Q = i_g(P) \in M$ mit $U \leq Q$. Wegen $\#U = \#Q$ gilt dann aber $U = Q$ und wir haben $M = \mathrm{Syl}_p G$, wie behauptet.

(3): Die Aussage „$\#\mathrm{Syl}_p G \mid u$“ folgt direkt aus (3.4) unter Berufung auf die mittlerweile bekannte Gleichheit $M = \mathrm{Syl}_p G$. Zum Schluss beachte man, dass auch P durch Konjugation auf $\mathrm{Syl}_p G$ operiert und $P \in \mathrm{Syl}_p G$ als Fixpunkt hat. Tatsächlich ist P auch der *einzige* Fixpunkt unter dieser Operation, da für jeden Fixpunkt Q ja $P \leq Q$ (wähle $U = P$ im obigen Beweis zu (1)) und also $P = Q$ (aus Kardinalitätsgründen) folgt. Alle anderen Bahnen haben daher eine Länge der Form p^r mit $r \geq 1$. Da die Bahnen ja $\mathrm{Syl}_p G$ partitionieren, gilt also $\#\mathrm{Syl}_p G = 1 + k \cdot p$ mit einem $k \in \mathbb{N}_0$. □

Korollar 3.4. *Sei G eine endliche Gruppe, p prim und $P \in \mathrm{Syl}_p G$. Genau dann ist $\#\mathrm{Syl}_p G = 1$ wenn P ein Normalteiler von G ist.*

Beweis. Wegen Satz 3.3 (2) ist $\mathrm{Syl}_p G = \{P\} \iff \forall g \in G\colon gPg^{-1} = P \iff P \trianglelefteq G$. □

3.2. Anwendung: Gruppen kleiner Ordnung

Wir betrachten Gruppen G der Ordnung $n = pq$ mit Primzahlen $p > q$, also

$$\begin{aligned} n \in \{&\_\_\_\_\_ 6, \_\_\_ 10, \_\_\_ 14, 15, \_\_\_\_\_ 21, 22, \_\_\_ 26, \_\_\_\_ \ldots\} \\ &= \{6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62, \ldots\}. \end{aligned}$$

Proposition 3.5. *Es sei G eine Gruppe der Ordnung $n = pq$ mit Primzahlen $p > q$. Dann gelten die folgenden Aussagen:*

(1) Es ist $G \cong C_p \rtimes_\varphi C_q$ mit einem Gruppenhomomorphismus $\varphi\colon C_q \to \mathrm{Aut}(C_p)$.

(2) Gilt zudem $q \nmid p-1$, so ist $C \cong C_{pq}$.

Beweis. Gemäß Satz 3.3 (3) ist $\#\mathrm{Syl}_p G$ ein Teiler von q und von der Form $1 + kp$, also gleich 1. Korollar 3.4 liefert, dass die (eindeutige) p-Sylowgruppe P von G ein Normalteiler ist.

Wir wählen nun eine q-Sylowgruppe Q von G. (Hiervon kann es mehrere geben!) Da die Ordnung eines Elementes im Schnitt $P \cap Q$ sowohl p wie auch q teilt (Satz von Lagrange, Satz 1.7), folgt $P \cap Q = \{1_G\}$. Mit Aufgabe 3.3 folgt nun $G = PQ$ und das Komplexprodukt PQ ist laut Aufgabe 4.1 isomorph zu $P \rtimes Q$, wobei der hierbei zu verwendende Homomorphismus $Q \to \mathrm{Aut}(P)$ der Konjugationsoperation entspricht.

Mit Korollar 1.8 und Korollar 2.8 erhält man $P \cong C_p$ sowie $Q \cong C_q$. Es ergibt sich also

$$G = PQ \cong P \rtimes Q \cong C_p \rtimes_\varphi C_q$$

mit einem Gruppenhomomorphismus $\varphi\colon C_q \to \mathrm{Aut}(C_p)$, wie behauptet.

Nun gelte $q \nmid p-1$. Da $\#\mathrm{Syl}_q G$ ein Teiler von p ist, ist $\#\mathrm{Syl}_q G = \{1, p\}$. Der Fall $\#\mathrm{Syl}_q G = p$ kann allerdings nicht eintreten, da $\#\mathrm{Syl}_q G$ ja von der Form $1 + \tilde{k}q$ ist und dies der Annahme $q \nmid p-1$ widerspräche. Korollar 3.4 liefert die Normalität von Q in G und Aufgabe 4.1 impliziert dann

$$G = PQ \cong P \rtimes Q \cong P \times Q \cong C_p \times C_q.$$

Aufgabe 3.1 impliziert aber $C_p \times C_q \cong C_{pq}$ und wir sind fertig. □

Bemerkung 3.6. Im Hinblick auf Proposition 3.5 stellt sich die Frage, wie viele verschiedene (nicht-isomorphe) Gruppen $C_p \rtimes_\varphi C_q$ man bekommen kann, wenn q ein Teiler von $p-1$ ist und φ alle Homomorphismen $C_q \to \mathrm{Aut}(C_p)$ durchläuft. Der triviale Homomorphismus $C_q \to \mathrm{Aut}(C_p)$, $x \mapsto \mathrm{id}_{C_p}$, liefert $C_p \times C_q$. Man kann zeigen, dass es unter den hier gemachten Voraussetzungen stets noch mindestens einen nicht-trivialen Homomorphismus $\varphi\colon C_q \to \mathrm{Aut}(C_p)$ gibt und für jeden anderen nicht-trivialen Homomorphismus $\psi\colon C_q \to \mathrm{Aut}(C_p)$ die Gruppen $C_p \rtimes_\varphi C_q$ und $C_p \rtimes_\psi C_q$ isomorph sind. Da diese im Gegensatz zu $C_p \times C_q$ nicht abelsch sind, hat man also genau zwei nicht-isomorphe Gruppen der Ordnung pq mit Primzahlen $p > q$ und $q \mid p-1$. Dieser Satz stammt von E. Netto (1882(?)). Ähnliche, obgleich anstrengendere, Untersuchungen hat zum Beispiel O. Hölder [26] angestellt, um Gruppen der Ordnungen p^3, pq^2, pqr und p^4 zu klassifizieren. (p, q und r bezeichnen hier Primzahlen.)

Bemerkungen 3.7. (1) Die Zahlen n, für welche Proposition 3.5 (2) Anwendung findet, sind genau

$$n \in \{15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95, 115, 119, 123, 133, 141, \ldots\}.$$

Insbesondere sind alle Gruppen der Ordnung 15 isomorph zu C_{15}.

(2) Landau [34] zeigte 1900 für die Anzahl $\pi_2(x)$ der natürlichen Zahlen $n \leq x$, welche sich als Produkt $n = pq$ von zweier Primzahlen $p > q$ schreiben lassen, die asymptotische Formel

$$\pi_2(x) \sim \frac{x \log\log x}{\log x} \quad (x \longrightarrow \infty).$$

(Das bedeutet, dass der Quotient aus linker und rechter Seite für $x \to \infty$ gegen 1 konvergiert.)

(3) Gilt in der Situation von Proposition 3.5 hingegen $q \mid p-1$, so kann man sich mit etwas mehr Arbeit noch überlegen, dass alle nicht-trivialen Gruppenhomomorphismen $\varphi\colon C_q \to \mathrm{Aut}(C_p)$ zu isomorphen semidirekten Produkten $C_p \rtimes_\varphi C_q$ führen. Es gibt also (bis auf Isomorphie) genau eine nicht-abelsche Gruppe der Ordnung pq (p, q prim, $q \mid p-1$).

Wegen Korollar 1.8 und Korollar 2.8 kennen wir allerdings auch alle Gruppen mit Primzahlordnung bis auf Isomorphie: ist $\#G = p$ prim, so ist $G \cong C_p$. Insgesamt kennen[3] wir darum alle Gruppen der Ordnung n mit

$$n \in \{1, 2, 3, \_\ 5, 6, 7, \_\_\ 10, 11, \_\ 13, 14, 15, \_\ 17, \_\ 19, \_\ 21, 22, 23, \_\_\ 26, \_\ \ldots\}.$$

Aus Aufgabe 5.3 kennen wir auch alle Gruppen der Ordnung p^2 mit primem p bis auf Isomorphie: C_{p^2} und $C_p \times C_p$. Dies liefert eine Kenntnis aller Gruppen der Ordnung n mit

$$n \in \{1, \ldots, 7, \_\ 9, 10, 11, \_\ 13, 14, 15, \_\ 17, \_\ 19, \_\ 21, 22, 23, \_\ 25, 26, \_\ \ldots\}.$$

Man beachte insbesondere auch Tabelle 1.

[3] Die Tatsache, dass wir die semidirekten Produkte in Proposition 3.5 (1) nicht näher beschrieben haben, soll uns hier nicht stören.

n	#	Liste von Isomorphietypen	Begründung
1	1	C_1	Trivial
2	1	C_2	p: Korollar 1.8 und Korollar 2.8
3	1	C_3	p
4	2	C_4, $C_2 \times C_2$	p^2: Aufgabe 5.3 (d)
5	1	C_5	p
6	2	C_6, $C_3 \rtimes C_2 \cong D_{2\cdot 3} \cong \mathfrak{S}_3$	pq: Bemerkung 3.6
7	1	C_7	p
8	5	*(ausgelassen)*	[14, Groups of order p^3]
9	2	C_9, $C_3 \times C_3$	p^2
10	2	C_{10}, $D_{2\cdot 5}$	pq
11	1	C_{11}	p
12	5	*(ausgelassen)*	[14, Groups of order 12]
13	1	C_{13}	p
14	2	C_{14}, $D_{2\cdot 7}$	pq
15	1	C_{15}	pq und Proposition 3.5 (2)
16	14	*(ausgelassen)*	[14, Groups of order 16]
17	1	C_{17}	p
18	5	*(ausgelassen)*	— (Hier ohne Begründung)
19	1	C_{19}	p
20	5	*(ausgelassen)*	—
21	2	C_{21}, $C_7 \rtimes C_3$	pq
22	2	C_{22}, $D_{2\cdot 11}$	pq
23	1	C_{23}	p
24	15	*(ausgelassen)*	—
25	2	C_{25}, $C_5 \times C_5$	p^2
26	2	C_{26}, $D_{2\cdot 13}$	pq

Tabelle 1. Gruppen mit Ordnung $n \leq 26$. Für gegebenes n ist jeweils die Anzahl (#) von Isomorphietypen solcher Gruppen angegeben. Bei auftretenden semidirekten Produkten ist stets ein solches mit nichttrivaler Operation des rechten Faktors auf dem linken gemeint. Für $n \in \{8, 12, 16\}$ wird auf Conrad [14] verwiesen. Für $n \in \{18, 20, 24\}$ geben wir die Anzahl ohne weitere Begründung; Siehe [26].

KAPITEL 4

Symmetrische Gruppen

Sei G eine Gruppe, die treu auf einer endlichen Menge M operiert. Dann kann man G vermöge der Operation als Untergruppe von $\mathrm{Sym}(M) \cong \mathfrak{S}_{\#M}$ auffassen[1] und man gelangt zur Aufgabe, die symmetrischen Gruppen $\mathfrak{S}_n$ ($n = 1, 2, 3, \ldots$) besser zu verstehen. Die hier gewonnenen Einsichten werden sich in der Vorlesung *„Algebra“* noch als nützlich erweisen: Darin beleuchten wir die sogenannte ***Galois-Theorie***, welche algebraische Abhängigkeiten zwischen Nullstellen von Polynomen quantifiziert, indem diesen gewisse Gruppen zugeordnet werden. Für eine Erklärung, welchen Nutzen dies hat, sei auf die *„Algebra“*-Vorlesung verwiesen. Hier sei nur erwähnt, dass die darin auftretenden Gruppen insbesondere auf den Nullstellen von den Polynomen operieren, aus denen sie erwachsen. Durch diese Operation kann man jene Gruppen dann „sehen“ und ein besseres Verständnis von $\mathfrak{S}_n$ erlaubt in günstigen Fällen sogar deren Bestimmung. (Für Details sei auf [45, § 5.4] verwiesen.)

4.1. Zyklen und Zyklenzerlegung

Unser erstes Ziel ist es, die Zerlegung von Elementen der symmetrischen Gruppe $\mathfrak{S}_n$ in einfachere „Bausteine“. Hierzu sei $\{a_1, a_2, \ldots, a_k\}$ eine beliebige k-elementige Teilmenge von $\{1, 2, \ldots, n\}$. Wir schreiben dann $(a_1\ a_2\ \ldots\ a_k)$ für die Permutation $\sigma \in \mathfrak{S}_n$ gegeben durch

$$\sigma(m) = \begin{cases} a_1 & \text{falls } m = a_k, \\ a_{j+1} & \text{falls } \exists 1 \leq j < k\colon m = a_j, \\ m & \text{sonst;} \end{cases}$$

Wir nennen solche Permutationen ***k-Zyklus***, oder kurz ***Zyklus***. Die Zahl k nennen wir hier die ***Länge*** des Zyklus $(a_1\ a_2\ \ldots\ a_k)$. Das Element $1_{\mathfrak{S}_n} = \mathrm{id}_{\{1,\ldots,n\}}$ notieren wir gelegentlich auch als leeren Zyklus ( ). Ein einelementiger Zyklus (a) stimmt stets mit ( ) überein. Ferner lassen sich die Einträge $a_1, \ldots, a_k$ in $(a_1\ a_2\ \ldots\ a_k)$ beliebig *zyklisch* permutieren, z.B.

$$(1\ 2\ 3\ 4) = (4\ 1\ 2\ 3) = (3\ 4\ 1\ 2) = (2\ 3\ 4\ 1),$$

[1] Vgl. auch Satz 2.15, wofür benutzt wurde, dass jede Gruppe vermöge der linksregulären Operation treu auf der Menge ihrer Elemente operiert.

aber eine willkürliche Permutation der Einträge liefert im Allgemeinen verschiedene Zyklen, z.B.

$$(\underline{1\,2}\,3\,4) \neq (\underline{2\,1}\,3\,4).$$

Bei der Verkettung von Zyklen unterdrückt man gern das Symbol $\circ$ und schreibt so etwa kurz $(1\,2)(3\,4)$ statt $(1\,2)\circ(3\,4)$.

Bemerkung. Man beachte, dass die Notation für Zyklen in $\mathfrak{S}_n$ nicht das n mitführt. Es ist also notationsbedingt unklar, ob $(1\,2)$ ein Element von $\mathfrak{S}_2$ oder etwa von $\mathfrak{S}_{2021}$ darstellen soll. In welchem $\mathfrak{S}_n$ sich die Rechnungen abspielen wird allerdings stets vom Kontext klar sein.

Für einen Zyklus $\sigma = (a_1\ \dots\ a_k) \in \mathfrak{S}_n$ nennt man

$$\operatorname{supp}\sigma := \{\,1 \le m \le n : \sigma(m) \neq m\,\} = \begin{cases} \{a_1,\dots,a_k\} & \text{falls } k \ge 2, \\ \emptyset & \text{falls } k = 1, \end{cases}$$

den ***Träger*** von σ (Engl.: ***support***). Zwei Zyklen $(a_1\ \dots\ a_k)$ und $(b_1\ \dots\ b_\ell)$ heißen ***disjunkt***, falls ihre Träger disjunkt sind. (D.h. die Zyklen sind disjunkt genau dann wenn $\{a_1,\dots,a_k\} \cap \{b_1,\dots,b_\ell\} = \emptyset$ oder $1 \in \{k,\ell\}$ gilt.) Ein 2-Zyklus heißt ***Transposition***.

Beispiele.

(1) $\operatorname{supp}(1\,2\,3) = \{1,2,3\}$, $\operatorname{supp}(4\,5) = \{4,5\}$, $\operatorname{supp}(1) = \emptyset$.
(2) Die Zyklen $(1\,2\,3)$ und $(4\,5)$ sind disjunkt.
(3) Die Zyklen $(1\,2\,3)$ und $(6\,2\,8)$ sind nicht disjunkt.
(4) Die Zyklen $(1\,2\,3)$ und $(1) = (\,)$ sind disjunkt.

Lemma 4.1.

(1) Für zwei disjunkte Zyklen $\sigma, \tilde\sigma$ gilt $\sigma\circ\tilde\sigma = \tilde\sigma\circ\sigma$.
(2) Jeder k-Zyklus mit $k \ge 2$ ist ein Produkt von Transpositionen.
(3) Jeder k-Zyklus hat Ordnung k.
(4) Zwei Zyklen sind genau dann in $\mathfrak{S}_n$ konjugiert zueinander, wenn diese dieselbe Länge haben.

Beweis. (1) überlegt man sich direkt, indem man bestätigt, dass für jedes $1 \le m \le n$ die Permutationen $\sigma\circ\tilde\sigma \in \mathfrak{S}_n$ und $\tilde\sigma\circ\sigma \in \mathfrak{S}_n$ auf m beide den Wert

$$\begin{cases} \sigma(m) & \text{falls } m \in \operatorname{supp}\sigma, \\ \tilde\sigma(m) & \text{falls } m \in \operatorname{supp}\tilde\sigma, \\ m & \text{sonst} \end{cases}$$

annehmen. (2) folgt aus $(a_1\,a_2\,a_3\ \dots\ a_k) = (a_1\,a_2)\circ(a_2\,a_3)\circ\dots\circ(a_{k-1}\,a_k)$. (3) folgt sofort durch „scharfes Hinsehen“. Für (4) bestätigt man zunächst die Formel

$$f\circ(a_1\,a_2\,a_3\ \dots\ a_k)\circ f^{-1} = (f(a_1)\,f(a_2)\,f(a_3)\ \dots\ f(a_k)) \tag{4.1}$$

für $f \in \mathfrak{S}_n$. Die Behauptung folgt unmittelbar daraus. □

Beispiele.

(1) Disjunkte Zyklen kommutieren (Lemma 4.1 (1)); Zum Beispiel:

$$(1\ 2) \circ (3\ 4) = (3\ 4) \circ (1\ 2).$$

(2) Nicht-disjunkte Zyklen *können* kommutieren; Zum Beispiel:

$$(1\ 2\ 3) \circ (3\ 2\ 1) = ( ) = (3\ 2\ 1) \circ (1\ 2\ 3).$$

Allerdings kommutieren (ab $n \geq 3$) nicht alle nicht-disjunkten Zyklen

$$(1\ 2) \circ (2\ 3) = (1\ 2\ 3) \neq (3\ 2\ 1) = (3\ 2) \circ (2\ 1) = (2\ 3) \circ (1\ 2).$$

(3) Wir berechnen Potenzen von $(1\ 2\ 3\ 4)$:

- $(1\ 2\ 3\ 4)^2 = (1\ 3) \circ (2\ 4)$,
- $(1\ 2\ 3\ 4)^3 = (1\ 2\ 3\ 4) \circ (1\ 3) \circ (2\ 4) = (1\ 4\ 3\ 2)$,
- $(1\ 2\ 3\ 4)^4 = (1\ 2\ 3\ 4) \circ (1\ 4\ 3\ 2) = ( )$.

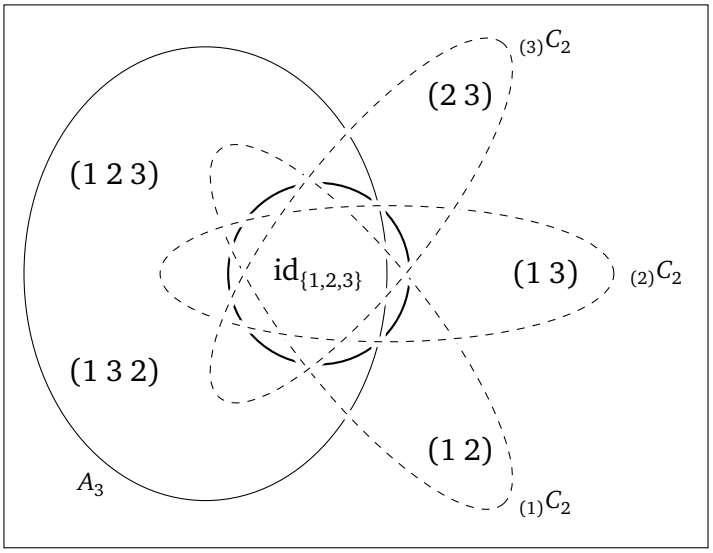


Abbildung 15. Alle 6 Untergruppen von $\mathfrak{S}_3$. Neben den beiden trivialen Untergruppen ($\{\mathrm{id}_{\{1,2,3\}}\}$ und $\mathfrak{S}_3$) sind dies $_{(i)}C_2 \cong C_2$ und $A_3 \cong C_3$.

Beispiel (Untergruppen von $\mathfrak{S}_3$)**.** In Abbildung 15 sieht man alle $3! = 6$ Elemente von $\mathfrak{S}_3$. Durch scharfes Hinsehen bestimmt man damit auch leicht alle Untergruppen von $\mathfrak{S}_3$.

Beispiel (Untergruppen von $\mathfrak{S}_4$)**.** In Abbildung 16 sieht man alle 30 Untergruppen von $\mathfrak{S}_4$. Diese wurden mit einem Computer bestimmt.

Proposition 4.2 (Zyklenzerlegung)**.** *Jedes Element von $\mathfrak{S}_n$ lässt sich als Produkt von disjunkten Zyklen schreiben und diese Darstellung ist bis auf Vertauschung der Faktoren eindeutig, wenn man triviale Zyklen (Länge* 0 *oder* 1*) ignoriert.*

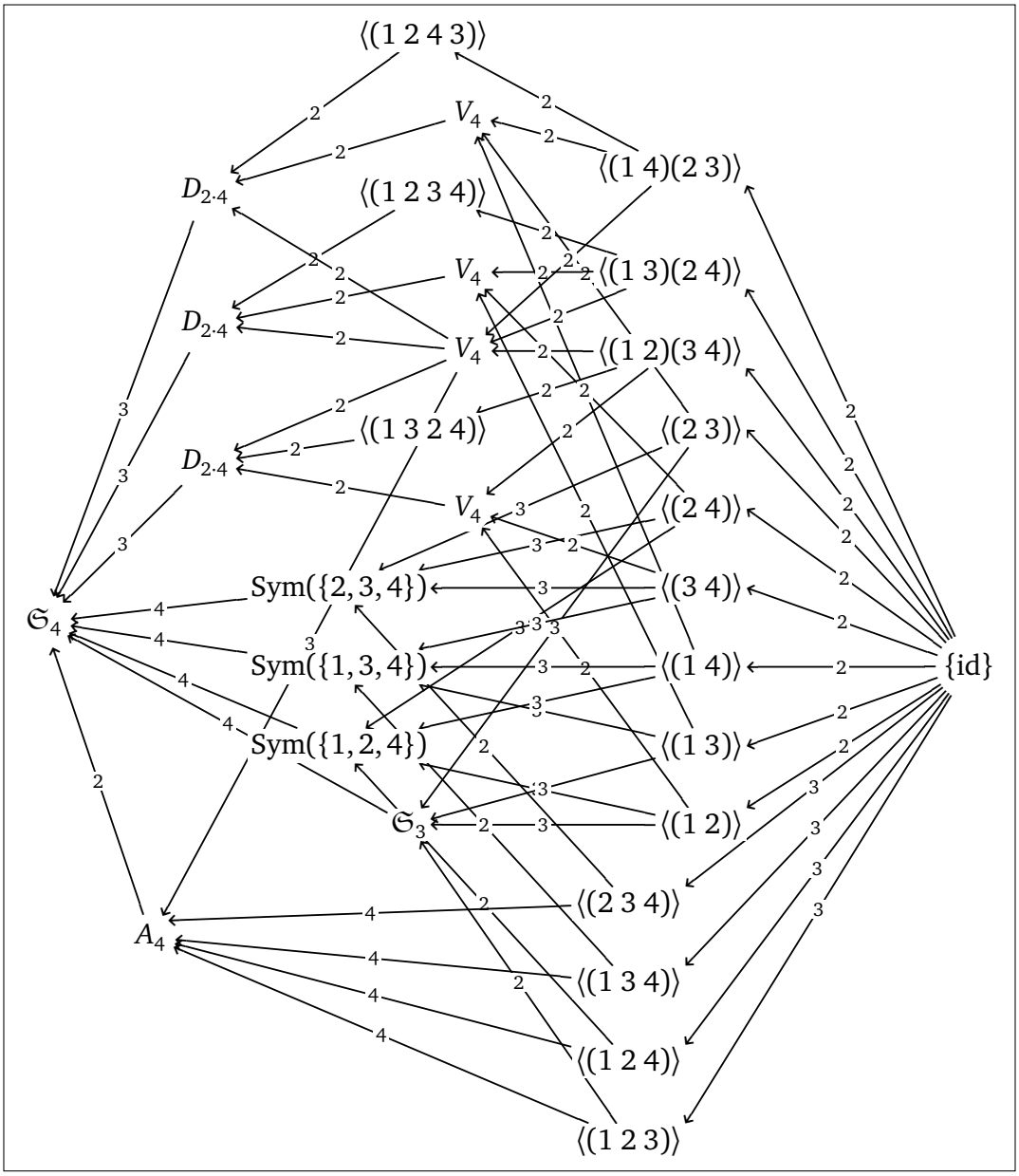


Abbildung 16. Der Untergruppenverband von $\mathfrak{S}_4$. Doppelte Bezeichnungen stehen für verschiedene, aber isomorphe Untergruppen. Die Pfeile bedeuten Inklusionen und sind mit dem jeweiligen Untergruppenindex beschriftet. Die nichttrivialen Normalteiler von $\mathfrak{S}_4$ sind A_4 und die (eine) in A_4 enthaltene V_4.

Beweis. Für jedes $\sigma \in \mathfrak{S}_n$ operiert $\langle\sigma\rangle$ auf $M = \{1, \ldots, n\}$ in der offensichtlichen Weise (durch Funktionsauswertung). Laut Satz 2.16 (2) zerfällt M nun in Bahnen

bezüglich dieser Operation. Mit Argumenten wie im Beweis von Lemma 1.9 zeigt sich, dass jede solche Bahn B die Form

$$B = \{\, \sigma^k(m) : k \in \mathbb{Z} \,\} = \{m, \sigma(m), \sigma^2(m), \ldots, \sigma^{(\#B)-1}(m)\}$$

hat und man sieht außerdem, dass $\sigma|_B \colon B \to B$ mit dem Zyklus

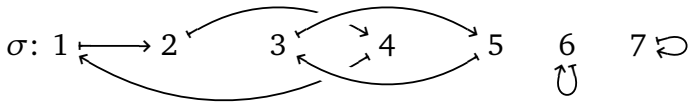
$$(m\ \sigma(m)\ \sigma^2(m)\ \ldots\ \sigma^{(\#B)-1}(m))|_B \colon B \to B$$

übereinstimmt. Da der obige Zyklus (nach Aufhebung der Einschränkung auf B) disjunkt zu den anderen den Bahnen zugeordneten Zyklen ist, schreibt sich σ wirklich als Produkt von diesen.

Die Eindeutigkeit der Zyklenzerlegung aus der Proposition sieht man sofort daraus, dass jeder solche Zyklus offensichtlich eine Bahn von M unter der Operation von $\langle g \rangle$ repräsentiert. □

Beispiel. Wir wollen die Permutation $\sigma \in \mathfrak{S}_n$ gegeben durch

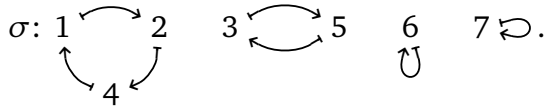
(4.2)



als Produkt disjunkter Zyklen schreiben. Der Beweis von Proposition 4.2 zeigt, dass man hierzu die Bahnen der Elemente von $M = \{1, 2, 3, 4, 5, 6, 7\}$ zu betrachten hat: wir starten mit $1 \in M$. Anwenden von σ liefert $\sigma(1) = 2$. An σ ist also ein Zyklus der Form $(1\ 2\ \ldots)$ mit noch näher zu bestimmendem hinteren Teil beteiligt. Wegen $\sigma(2) = 4$ hat dieser die Form $(1\ 2\ 4\ \ldots)$ und wegen $\sigma(4) = 1$ handelt es sich um den Zyklus $(1\ 2\ 4)$. Die Zahlen 2 und 4 brauchen wir nun nicht mehr zu betrachten, da diese schon durch Betrachtung der Bahn $\{1, 2, 4\}$ von 1 abgehandelt sind. Eine ähnliche Betrachtung liefert den Zyklus $(3\ 5)$ und die beiden (trivialen) Zyklen (6) und (7). Demnach ist

$$\sigma = (1\ 2\ 4) \circ (3\ 5) \circ (6) \circ (7) = (1\ 2\ 4) \circ (3\ 5).$$

Visuell sieht man diese Zerlegung auch schon anhand der Darstellung von σ in (4.2). Um dies noch weiter zu verdeutlichen vertauschen wir in dieser Darstellung noch die Positionen von 3 und 4. Nun sehen wir die Zyklenzerlegung von σ klar vor uns:



Korollar 4.3. *Es gelten die folgenden Aussagen:*

(1) $\mathfrak{S}_n$ *wird von den Transpositionen erzeugt.*

(2) Zwei Permutationen $\sigma, \sigma' \in \mathfrak{S}_n$ *sind genau dann konjugiert in* $\mathfrak{S}_n$ *wenn ihre Zyklenzerlegungen vom* ***gleichen Typ*** *sind, d.h. beide Zyklenzerlegungen enthalten gleich viele k-Zyklen für jedes* $k > 1$.[2]

[2] Beispielsweise sind $(1\ 2\ 3) \circ (4\ 5\ 6\ 7)$ und $(1\ 2\ 3) \circ (4\ 5) \circ (6\ 7)$ *nicht* konjugiert.

(3) Ist $\sigma = \sigma_1 \circ \ldots \circ \sigma_t$ ein Produkt von paarweise disjunkten Zyklen σ_k, so ist die Ordnung von σ das kleinste gemeinsame Vielfache der Ordnungen (Zykluslängen) der σ_k.

Beweis. (1): Jedes $\sigma \in \mathfrak{S}_n$ schreibt sich als Produkt (disjunkter) Zyklen und jeder solche Zyklus ist laut Lemma 4.1 (2) ein Produkt von Transpositionen.

(2): Das folgt leicht aus (4.1), indem man in der Zyklenzerlegung zwischen je zwei Zyklen einen Faktor $(\,) = f \circ f^{-1}$ einschmuggelt.

(3): Da disjunkte Zyklen kommutieren, ist $\sigma^m = \sigma_1^m \circ \ldots \circ \sigma_t^m$ und dies ist genau dann gleich $(\,)$, wenn m alle Ordnungen $\operatorname{ord}(\sigma_k)$ für $k = 1, \ldots, m$ teilt. □

4.2. Signum von Permutationen und alternierende Gruppen

In diesem Abschnitt konstruieren wir einen speziellen Homomorphismus von $\mathfrak{S}_n \to \{\pm 1\}$ (Lemma 4.4) und beschaffen uns über jenen eine besondere Untergruppe von $\mathfrak{S}_n$ (§ 4.2.2).

4.2.1. Signum von Permutationen. Jede Gruppe G der Ordnung 2 ist isomorph zu C_2 (Korollar 1.8 und Korollar 2.8). Tatsächlich ist ein Gruppenisomorphismus $G \to C_2$ auch schon eindeutig bestimmt, da ein solcher ja 1_G auf das neutrale Element 0 in $(C_2, \oplus)$ abbilden muss und dann das eine übrige Element in $G \setminus \{1_G\}$ automatisch auf das übrige Element in $C_2 \setminus \{0\}$ abgebildet werden muss. Wir schreiben nun $\{\pm 1\}$ für die Gruppe $(\{-1, 1\}, \cdot)$ mit der bekannten Multiplikation. Diese ist nach unseren Überlegungen notwendigerweise auf eindeutige Art und Weise isomorph zu C_2.

Lemma 4.4. *Für $n \geq 2$ gibt es genau einen nicht-trivialen Gruppenhomomorphismus $\mathfrak{S}_n \to \{\pm 1\}$.*

Beweis. Zunächst zur *Eindeutigkeit*. Gemäß Proposition 4.2 und Lemma 4.1 (2) wird $\mathfrak{S}_n$ von Transpositionen erzeugt. Jeder Gruppenhomomorphismus $f\colon \mathfrak{S}_n \to \{\pm 1\}$ ist also schon eindeutig durch seine Bilder auf den Transpositionen aus $\mathfrak{S}_n$ festgelegt. Tatsächlich reicht hierzu sogar schon das Bild einer einzigen Transposition, denn da $\{\pm 1\}$ abelsch ist haben wir

$$\begin{aligned} f(\sigma \circ \tau \circ \sigma^{-1}) &= f(\sigma) \cdot f(\tau) \cdot f(\sigma^{-1}) = f(\sigma) \cdot f(\sigma^{-1}) \cdot f(\tau) \\ &= f(\sigma \circ \sigma^{-1}) \cdot f(\tau) = 1 \cdot f(\tau) = f(\tau) \end{aligned}$$

für alle $\sigma, \tau \in \mathfrak{S}_n$. Also ist f konstant auf allen Konjugationsklassen von $\mathfrak{S}_n$ und nach Lemma 4.1 (4) sind alle Transpositionen konjugiert zueinander. Ist nun $f((1\ 2)) = 1$ (das neutrale Element in $\{\pm 1\}$), so ist f automatisch der triviale Homomorphismus. Ist $f((1\ 2)) = -1$ (das andere Element in $\{\pm 1\}$), so ist f nicht-trivial, aber eben auch schon eindeutig bestimmt.

Nun zur *Existenz*: Wir schreiben $\mathscr{I} = \{(i, j) : 1 \leq i < j \leq n\}$. Für $\sigma \in \mathfrak{S}_n$ sei

$$\operatorname{sgn}\sigma := \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}, \quad \text{mit} \quad \prod_{i<j} := \prod_{(i,j)\in\mathscr{I}}.$$

Man rechnet nach, dass es sich dabei tatsächlich um einen Gruppenhomomorphismus handelt; dieser ist wegen $\operatorname{sgn}(1\,2) = -1 \neq +1$ nicht trivial. Zunächst zum Wert von sgn bei der Transposition $\tau = (1\,2)$. Da τ nur die Elemente 1 und 2 bewegt, kürzt sich der Bruch im sgn-definierenden Produkt für alle Indizes $(i,j) \in \mathscr{I}$, welche weder 1 noch 2 enthalten. Damit folgt

$$\begin{aligned}\operatorname{sgn}\tau &= \prod_{i<j:\ \{1,2\}\cap\{i,j\}\neq\emptyset} \frac{\tau(j)-\tau(i)}{j-i} = \left(\prod_{j=2}^{n} \frac{\tau(j)-\tau(1)}{j-1}\right) \times \prod_{j=3}^{n} \frac{\tau(j)-\tau(2)}{j-2} \\ &= \left(\frac{1-2}{2-1} \times \prod_{j=3}^{n} \frac{j-2}{j-1}\right) \times \prod_{j=3}^{n} \frac{j-1}{j-2} = -1.\end{aligned}$$

Zum Nachweis der Homomorphismus-Eigenschaft für sgn beachte man für $\sigma, \rho \in \mathfrak{S}_n$

$$\begin{aligned}\operatorname{sgn}(\sigma\circ\rho) &= \prod_{i<j} \left(\frac{(\sigma\circ\rho)(j)-(\sigma\circ\rho)(i)}{j-i} \frac{\rho(j)-\rho(i)}{\rho(j)-\rho(i)} \right) \\ &= \left(\prod_{i<j} \frac{\sigma(\rho(j))-\sigma(\rho(i))}{\rho(j)-\rho(i)} \right) \times \prod_{i<j} \frac{\rho(j)-\rho(i)}{j-i}.\end{aligned}$$

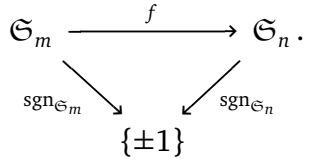
In der letzten Zeile ist das zweite Produkt offenbar gleich $\operatorname{sgn}\rho$. Schreiben wir Π für das eingeklammerte Produkt in der letzten Zeile, so gilt es nun $\Pi = \operatorname{sgn}\sigma$ nachweisen. Die Abbildung

$$\rho^*\colon \mathscr{I} \to \mathscr{I}, \quad (i,j) \mapsto \begin{cases} (\rho(i),\rho(j)), & \text{falls } \rho(i) < \rho(j), \\ (\rho(j),\rho(i)), & \text{falls } \rho(i) > \rho(j), \end{cases}$$

ist offensichtlich eine Bijektion. Damit sieht man schließlich

$$\begin{aligned}\Pi &= \left(\prod_{\substack{i<j \\ \rho(i)<\rho(j)}} \frac{\sigma(\rho(j))-\sigma(\rho(i))}{\rho(j)-\rho(i)} \right) \times \prod_{\substack{i<j \\ \rho(i)>\rho(j)}} \frac{\sigma(\rho(i))-\sigma(\rho(j))}{\rho(i)-\rho(j)} \\ &= \prod_{(k,\ell)\in\rho^*(\mathscr{I})} \frac{\sigma(\ell)-\sigma(k)}{\ell-k} = \prod_{(k,\ell)\in\mathscr{I}} \frac{\sigma(\ell)-\sigma(k)}{\ell-k} = \operatorname{sgn}\sigma. \qquad \square\end{aligned}$$

Den in Lemma 4.4 beschriebenen Homomorphismus bezeichnen wir — wie im Beweis — mit sgn für ***Signum*** (auch ***Signatur*** oder ***Vorzeichen*** [einer Permutation] genannt). Darin den Bezug auf $\mathfrak{S}_n$ zu unterdrücken ist nicht ungerechtfertigt: für jeden Gruppenhomomorphismus $f\colon \mathfrak{S}_m \to \mathfrak{S}_n$ zwischen symmetrischen Gruppen, sodass $\operatorname{sgn}_{\mathfrak{S}_n} \circ f$ nicht-trivial ist, gilt $\operatorname{sgn}_{\mathfrak{S}_n} \circ f = \operatorname{sgn}_{\mathfrak{S}_m}$ (Indizes zur besseren Übersichtlichkeit hinzugefügt):



Man beachte insbesondere die folgende Anwendung der obigen Bemerkung: für $n \geq m \geq 2$ erhält man einen Homomorphismus $f\colon \mathfrak{S}_m \to \mathfrak{S}_n$, indem man die Elemente von $\mathfrak{S}_m$ in der offensichtlichen Weise zu Permutationen von $\{1,\dots,m,\dots,n\}$ fortsetzt (auf $\{m+1,\dots,n\}$ identisch abbildend). Dieser bildet Transpositionen auf Transpositionen ab, womit $\operatorname{sgn}_{\mathfrak{S}_n} \circ f$ nicht der triviale Homomorphismus ist. Demnach ist $\operatorname{sgn}_{\mathfrak{S}_n} \circ f = \operatorname{sgn}_{\mathfrak{S}_m}$. Man mag sich an dieser Stelle an die Bemerkung auf Seite 64 erinnern, welche darauf hinweist, dass die in § 4.1 eingeführte Zyklen-Notation den Bezug auf die umgebende symmetrische Gruppe unterdrückt. Der Übergang von einem Element von $\mathfrak{S}_m$ in Zyklen-Notation zu dem Element von $\mathfrak{S}_n$, welches auf dieselbe Weise dargestellt wird, entspricht genau einer Anwendung des soeben konstruierten Homomorphismus f. Ob man das fragliche Element nun also als Element von $\mathfrak{S}_m$ oder von $\mathfrak{S}_n$ auffasst, ist für die Berechnung von dessen Signums unerheblich.

Bemerkung. Die oben gestellte Voraussetzung, dass $\operatorname{sgn}_{\mathfrak{S}_n} \circ f$ nicht trivial sei, ist tatsächlich notwendig, um $\operatorname{sgn}_{\mathfrak{S}_n} \circ f = \operatorname{sgn}_{\mathfrak{S}_m}$ zu bekommen. Dies beruht darauf, dass man $\mathfrak{S}_m$ homomorph in $\mathfrak{S}_{m+2}$ einbetten kann derart, dass das Bild unter diesem Homomorphismus komplett im Kern von $\operatorname{sgn}_{\mathfrak{S}_{m+2}}$ enthalten ist. Ein solcher Homomorphismus ist, wie man leicht nachrechnen kann, etwa wie folgt gegeben:

$$f\colon \mathfrak{S}_m \to \mathfrak{S}_{m+2}, \quad \sigma \mapsto \begin{cases} \sigma^{\mathrm{ext}} & \text{falls } \operatorname{sgn}_{\mathfrak{S}_m} = +1, \\ \sigma^{\mathrm{ext}} \circ \tau & \text{falls } \operatorname{sgn}_{\mathfrak{S}_m} = -1, \end{cases}$$

wobei τ die Transposition $((m+1)\,(m+2)) \in \mathfrak{S}_{m+2}$ bezeichne und zu $\sigma \in \mathfrak{S}_m$ sei σ^{ext} das Element von $\mathfrak{S}_{m+2}$ mit

$$\sigma^{\mathrm{ext}}(k) = \begin{cases} \sigma(k) & \text{falls } k \in \{1,\dots,m\}, \\ k & \text{falls } k \in \{m+1, m+2\}. \end{cases}$$

Korollar 4.5. *Ist σ ein Produkt von genau k Transpositionen, so ist* $\operatorname{sgn}\sigma = (-1)^k$.

Beweis. Es genügt einzusehen, dass das Signum einer jeden Transposition gleich -1 ist. Dies haben wir im Beweis von Lemma 4.4 allerdings schon gesehen. □

Wir erhalten auch das folgende Korollar, welches in der Literatur oft auch als Zwischenschritt bewiesen wird, um die Existenz des Signum-Homomorphismus zu zeigen.

Korollar 4.6. *Ist* $\mathrm{id}_{\{1,\dots,n\}} = \tau_1 \circ \cdots \circ \tau_k$ *ein Produkt von k Transpositionen in $\mathfrak{S}_n$, so ist k gerade.*

Beweis. Wendet man auf beide Seiten von $\mathrm{id}_{\{1,\dots,n\}} = \tau_1 \circ \cdots \circ \tau_k$ die Signum-Funktion an, so folgt mit Korollar 4.5 sofort $1 = (-1)^k$. Also ist k gerade. (Wenn man den Einsatz der Signum-Funktion vermeiden möchte, kann man eine Induktion über k führen, muss dann allerdings ein wenig rechnen.) □

4.2.2. Alternierende Gruppe A_n. Im Folgenden sei stets $n \geq 2$. Der Kern

$$A_n := \ker(\operatorname{sgn}\colon \mathfrak{S}_n \to \{-1, 1\}) \trianglelefteq \mathfrak{S}_n$$

heißt ***Alternierende Gruppe***. (Alternative Schreibweise: $\mathfrak{A}_n$ mit „Fraktur A“.) Wegen $\mathfrak{S}_n/A_n \cong \{-1, 1\}$ ist $\#\mathfrak{S}_n/\#A_n = 2$, also $\#A_n = n!/2$. Für eine Illustration hierzu siehe Tabelle 1 und Tabelle 2.

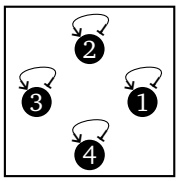
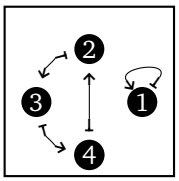
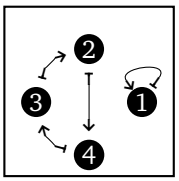
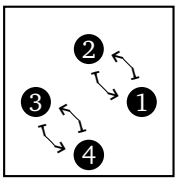
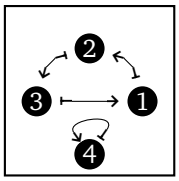
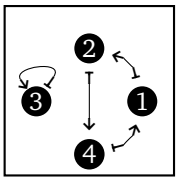
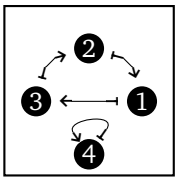
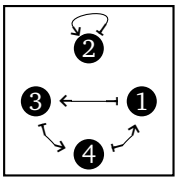
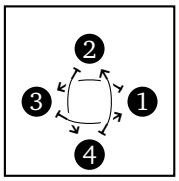
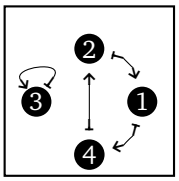
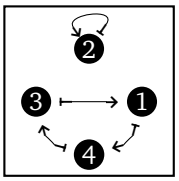
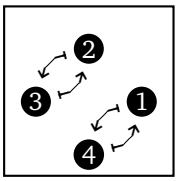
σ	$\operatorname{ord}(\sigma)$	σ	$\operatorname{ord}(\sigma)$	σ	$\operatorname{ord}(\sigma)$	σ	$\operatorname{ord}(\sigma)$
	1		3		3		2
	3		3		3		3
	2		3		3		2

Tabelle 1. Alle Elemente σ von A_4 und deren Ordnungen.

Bemerkung. Wir zeigen nun die Eingangs in Kapitel 3 behauptete Aussage, dass die 12-elementige Gruppe A_4 ($4!/2 = 12$) keine Untergruppe mit Ordnung 6 besitzt. Angenommen, das wäre falsch und U wäre eine solche Untergruppe. Wir zeigen, dass U alle Elemente von A_4 mit ungerader Ordnung enthalten muss. Ein Blick auf Tabelle 1 verrät, dass U also mindestens 9 Elemente, also zu viele, enthält — ein Widerspruch! Sei also $\sigma \in A_4$ ein Element mit ungerader Ordnung k. U hat Index 2 in A_4 und ist daher gemäß Aufgabe 5.3 (c) normal. Wir bezeichnen mit $\pi\colon A_4 \to A_4/U$, $\rho \mapsto \rho U$, die kanonische Projektion. Wegen $\pi(\rho)^k = \pi(\rho^k) = \pi(1_{A_4}) = 1_{A_4/U}$ ist $\operatorname{ord}(\pi(\rho))$ ein Teiler von k. Nach dem Satz von Lagrange (Satz 1.7) ist $\operatorname{ord}(\pi(\rho))$ aber ein Teiler der Gruppenordnung von A_4/U, also von 2. Das impliziert $\operatorname{ord}(\pi(\rho)) = 1$ und also $\rho \in \ker \pi = U$.

4.2.3. Signum via Determinanten. Wenn man Determinanten und die Determinanten-Multiplikationsformel in der *linearen Algebra* ohne Diskussion der Signum-Funktion eingeführt hat (wovon wir allerdings nicht ausgehen), kann man dies auch

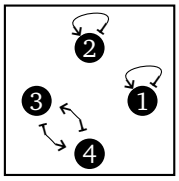
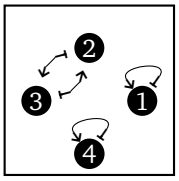
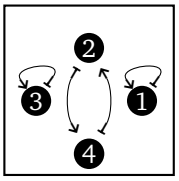
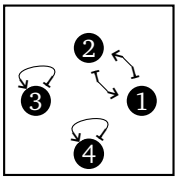
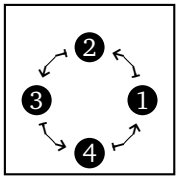
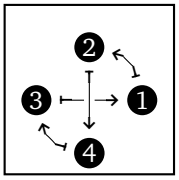
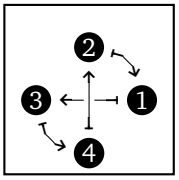
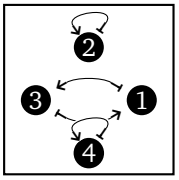
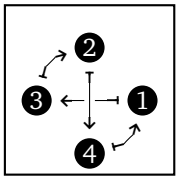
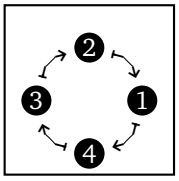
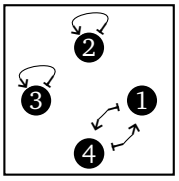
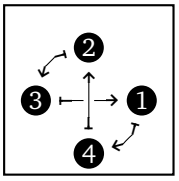
σ	ord(σ)	σ	ord(σ)	σ	ord(σ)	σ	ord(σ)
	2		2		2		2
	4		4		4		2
	4		4		2		4

Tabelle 2. Alle Elemente σ von $\mathfrak{S}_4 \setminus A_4$ und deren Ordnungen.

benutzen, um die Existenz der Signum-Funktion zu zeigen. Bezeichnet e_i den i-ten Standardeinheitsvektor im $\mathbb{Q}^n$, so kann man $\mathfrak{S}_n$ durch

$$\iota\colon \mathfrak{S}_n \to \mathrm{GL}_n(\mathbb{Q}), \quad \sigma \mapsto \begin{pmatrix} | & \dots & | \\ e_{\sigma(1)} & \dots & e_{\sigma(n)} \\ | & \dots & | \end{pmatrix},$$

in $\mathrm{GL}_n(\mathbb{Q})$ einbetten. Das ist ein Gruppenhomomorphismus. Die Verkettung $\det \circ \iota\colon \mathfrak{S}_n \to \mathbb{Q}^\times$ bildet in eine abelsche Gruppe ab und ist daher — wie wir im Beweis des Eindeutigkeitsteils von Lemma 4.4 gesehen haben — entweder der triviale Homomorphismus, oder stimmt mit der Signum-Funktion überein. Wegen

$$(\det \circ \iota)((1\,2)) = \det \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right) = -\det \left(\begin{array}{cc|ccc} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right) = -1$$

tritt der letztgenannte Fall ein. Also ist $(\det \circ \iota)(\sigma) = \operatorname{sgn}\sigma$ für alle $\sigma \in \mathfrak{S}_n$. Wir fassen diesen Sachverhalt durch die Kommutativität des folgenden Diagramms zusammen:

$$\begin{array}{ccc} \mathfrak{S}_n & \xhookrightarrow{\ \iota\ } & \mathrm{GL}_n(\mathbb{Q}) \\ \downarrow{\scriptstyle \operatorname{sgn}} & & \downarrow{\scriptstyle \det} \\ \{-1,1\} & \xhookrightarrow{\ \text{Inkl.}\ } & \mathbb{Q}^\times . \end{array}$$

Der oben benutzte Homomorphismus ι transportiert das Studium von $\mathfrak{S}_n$ auf Fragestellungen in der *linearen Algebra*. Ganz allgemein ist man vielleicht versucht, Gruppen G mithilfe von Homomorphismen $G \to \mathrm{GL}(V)$ in die generelle lineare Gruppe eines Vektorraums V zu studieren. Derartige Homomorphismen nennt man auch ***lineare Darstellungen (von G)*** und ihre systematische Untersuchung und Ausnutzung ist Gegenstand der sogenannten ***Darstellungstheorie***. (Homomorphismen $G \to \mathrm{Sym}(M)$, also Operationen von G auf einer Menge M, bezeichnet man manchmal auch als ***Permutationsdarstellungen***.)

4.3. Einfache Gruppen

Eine endliche Gruppe heißt ***einfach***, falls sie genau zwei Normalteiler besitzt. (Achtung: Die einelementige Gruppe ist nach dieser Definition nicht einfach.) Einfachheit bedeutet nicht „einfach zu verstehen," sondern deutet eher auf die Rolle dieser Gruppen als Grundbausteine endlicher Gruppen an: nicht-einfache Gruppen lassen sich oft durch das Studium ihrer Faktorgruppen besser verstehen. (Faktorgruppenbildung nach nicht-trivialen Normalteilern führt auf kleinere Gruppen!) Einfache Gruppen lassen hingegen keine nicht-triviale Faktorgruppenbildung zu.

Satz 4.7. *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Beweis. Das ist Aufgabe T7.2 (c). □

Bemerkung. Satz 4.7 hat bemerkenswerte *zahlentheoretische Konsequenzen*! Mit dessen Hilfe und mit Galois-Theorie kann man nämlich zeigen, dass es keine allgemeine Lösungsformel zur Berechnung von Nullstellen von Polynomen von einem Grad ≥ 5 geben kann, wenn man für Formeln nur die üblichen arithmetischen Operationen, die Koeffizienten des fraglichen Polynoms und das Ziehen beliebiger Wurzeln zulässt. Die tatsächliche Präzisierung und Begründung dieser Aussage ist jedoch nicht trivial und benötigt noch deutlich mehr Arbeit. Für Details siehe [45, § 5.6].

Die ***Klassifikation der endlichen einfachen Gruppen*** war ein großes Ziel der Gruppentheorie im 20. Jahrhundert und gilt seit 2004 als vollständig und umfasst mehrere tausend Seiten, die über einzelne Artikel in diversen Zeitschriften verteilt sind. Die dabei auftretenden Gruppen sind klassifiziert in drei unendliche Familien: zyklische Gruppen von Primzahlordnung (vgl. Satz 1.12), alternierende Gruppen A_n mit $n \geq 5$ (siehe Satz 4.7) und „Gruppen vom Lie-Typ". Zusätzlich gibt es noch genau 26 (oder 27, je nachdem, ob man eine der auftretenden Gruppen noch zum Lie-Typ zählt oder nicht) Gruppen, die in keine der drei genannten unendlichen Familien passen. Diese Gruppen nennt man ***sporadische Gruppen***.

KAPITEL 5

Endlich erzeugte abelsche Gruppen

Die bisher entwickelte Theorie erlaubt es uns, alle endlichen abelschen Gruppen bis auf Isomorphie zu klassifizieren. Als Vorstufe davon zeigen wir in Proposition 5.1, dass jede endlich erzeugte abelsche Gruppe isomorph zu einem direkten Produkt zyklischer Gruppen ist. Die zyklischen Gruppen sind uns dank Korollar 2.8 bereits erschöpfend bekannt. Die Hauptaufgabe besteht dann darin, direkte Produkte von zyklischen Gruppen voneinander unterscheiden zu können. Dies funktioniert auch in der größeren Allgemeinheit von endlich erzeugten abelschen Gruppen noch sehr gut, ist aber aufwändiger (siehe Satz 5.6). Wir wenden uns diesem Thema in der *Algebra*-Vorlesung noch in größerer Allgemeinheit zu (siehe [45, Kapitel 8]). Im hier vorliegenden Kapitel schöpfen wir die Eindeutigkeitsaussage im Falle *endlicher* abelscher Gruppen aus unserem Verständnis von Sylow-Gruppen (siehe Satz 5.3).

Gründe für das Interesse an *endlich erzeugten* abelschen Gruppen gibt es viele; Etwa die singulären Homologiegruppen *kompakter* Mannigfaltigkeiten liefern solche (siehe [23]). Für diese Vorlesung soll uns das hier noch zu beweisende Strukturergebnis jedoch auch noch gute Dienste leisten, etwa in § 6.3.4 für einen Satz von Gauß (Satz 6.21), welcher die Struktur der Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ bestimmt. Der Beweis benutzt ein allgemeines Ergebnis über die Zyklizität der Einheitengruppe endlicher Körper (Korollar 7.7), dessen wahre Signifikanz erst in der *Algebra*-Vorlesung zum Tragen kommen wird (siehe [45, Kapitel 4]).

5.1. Endlich erzeugte abelsche Gruppen

Proposition 5.1. *Jede von n Elementen erzeugte abelsche Gruppe ist isomorph zu einem direkten Produkt von höchstens n zyklischen Gruppen.*

Beweis. Wir beweisen die Aussage per Induktion über die Anzahl n der Erzeuger. Für $n = 1$ ist G schon selbst zyklisch und es ist nichts zu zeigen. Für den Induktionsschritt sei nun $g_1, \ldots, g_n, g_{n+1}$ ein $n+1$-elementiges Erzeugendensystem von $(G, +)$ und $U = \langle g_1, \ldots, g_n \rangle$. (Man beachte, dass wir im Folgenden die Gruppe G *additiv* schreiben. Dementsprechend schreiben wir 0_G für das neutrale Element von G und mg statt g^m für $g \in G$ und $m \in \mathbb{Z}$.) Wir setzen außerdem $g := g_{n+1}$.

Schritt 1: gilt $\langle g \rangle \cap U = \{0_G\}$, so ist[1] $G = \langle g \rangle + U$. Dies ist allerdings isomorph zu $\langle g \rangle \times U$, da der Gruppenepimorphismus $\langle g \rangle \times U \to \langle g \rangle + U$, $(\gamma, u) \mapsto \gamma + u$,

[1] Für eine multiplikativ geschriebene Gruppe hätten wir hier $G = \langle g \rangle U$ notiert; Gemeint ist das *Komplexprodukt* von $\langle g \rangle$ und U im Sinne von § 2.2.1.

den (trivialen!) Kern $\langle g\rangle \cap U = \{0_G\}$ besitzt und also injektiv ist. Anwenden der Induktionsvoraussetzung auf U liefert die Behauptung.

Schritt 2: Wir zeigen, dass man stets ein n+1-elementiges Erzeugendensystem von G wählen kann, welches die Voraussetzung aus Schritt 1 erfüllt. Hierzu dürfen wir annehmen, dass es zu *jedem* n+1-elementigen Erzeugendensystems $g_1, \ldots, g_n, g$ von G ein kleinstes $m \in \mathbb{N}$ mit $mg \in U = \langle g_1, \ldots, g_n\rangle$ gibt, da wir sonst schon gemäß Schritt 1 fertig wären. Wir wählen m nun minimal unter allen solchen Erzeugendensystemen und gehen davon aus, dass $g_1, \ldots, g_n, g$ ein dazu passendes Erzeugendensystem bezeichnet. Wir konstruieren daraus nun ein neues Erzeugendensystem passend zu Schritt 1.

Es gibt nun $m_1, \ldots, m_n \in \mathbb{Z}$ mit

$$mg = m_1 g_1 + \ldots + m_n g_n = \sum\nolimits_i m_i g_i.$$

(Indizes i und j seien im Folgenden als zwischen 1 und n eingeschränkt angenommen.) Wir schreiben nun $m_i = q_i m + r_i$ mit $0 \leq r_i < m$ mittels Division mit Rest und definieren

$$g' = g - \sum\nolimits_i q_i g_i. \tag{5.1}$$

Dann ist $g \in \langle g_1, \ldots, g_n, g'\rangle$, weswegen es sich bei $g_1, \ldots, g_n, g'$ auch um ein Erzeugendensystem von G handelt. Offensichtlich gilt

$$mg' - \sum\nolimits_i r_i g_i = mg - \sum\nolimits_i mq_i g_i - \sum\nolimits_i r_i g_i = mg - \sum\nolimits_i m_i g_i = 0_G. \tag{5.2}$$

Wäre nun $r_i > 0$ für einen Index i, so erhalten wir durch Umstellen von (5.2)

$$r_i g_i = mg' - \sum_{j \neq i} r_j g_j \in \langle \{g'\} \cup \{g_j : j \neq i\}\rangle.$$

Dies ist aber unmöglich, da man sonst die Rollen von g und g_i vertauschen könnte und einen Widerspruch zur minimalen Wahl von m bekäme.

Also gilt $r_i = 0$ für alle Indizes i. Gleichung (5.2) vereinfacht sich dann zu $mg' = 0_G$. Da allerdings gemäß der minimalen Wahl von m auch kein Vielfaches $m'g'$ mit $1 \leq m' < m$ in $U \setminus \{0_G\}$ liegt, ist $g_1, \ldots, g_n, g'$ doch ein Erzeugendensystem von G wie in Schritt 1. Damit sind wir fertig. □

Beispiel. Wir illustrieren den Beweis von Proposition 5.1 anhand des folgenden Beispiels:

$$G = C_3 \times C_3 \times C_2 = \left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\rangle =: \langle g_1, g_2, g\rangle.$$

Hier ist $U = \langle g_1, g_2\rangle = C_3 \times C_3 \times \{0\}$ und $\langle g\rangle \cap U$ enthält das von 0_G verschiedene Element

$$2g = \begin{pmatrix}1 \oplus_{C_3} 1\\ 1 \oplus_{C_3} 1\\ 1 \oplus_{C_2} 1\end{pmatrix} = \begin{pmatrix}2\\2\\0\end{pmatrix} = 2g_1 + 2g_2.$$

Die hier vorliegende Situation gehört im obigen Beweis also *Fall 2* an. Man beachte auch $U \times \langle g \rangle \ncong G$ allein schon aus Ordnungsgründen:

$$\#(U \times \langle g \rangle) = 3 \cdot 3 \cdot 6 \neq 3 \cdot 3 \cdot 2 = \#G.$$

In der Notation des obigen Beweises ist $m_1 = m_2 = 2$ und $q_1 = q_2 = 1$. Wir ersetzen nun, wie im obigen Beweis, das Element g durch ein neues Element g' mit $\langle g_1, g_2, g \rangle = \langle g_1, g_2, g' \rangle$. Unser neues Element g' nimmt hier die folgende Form an:

$$g' = g - q_1 g_1 - q_2 g_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Offensichtlich gilt $G \cong U \times \langle g' \rangle$.

Bemerkung. Die Schwierigkeit im Beweis zu Proposition 5.1 rührt von zyklischen „Faktoren“ mit endlicher Ordnung her: Am Ende von Schritt 2, wenn man auf die in Schritt 1 betrachtete Situation reduziert hat, spaltet man nämlich (mittels Schritt 1) einen zyklischen Faktor $\langle g' \rangle$ ab. Das Element g' hat wegen $mg' = 0_G$ aber endliche Ordnung. Nun ist entweder schon $g' = 0_G$ (und somit mit Blick auf (5.1) der Erzeuger $g \in \langle g_1, \ldots, g_n \rangle$ überflüssig!), oder g' hat endliche, aber positive Ordnung. In den (endlich erzeugten, abelschen) Gruppen $\mathbb{Z}^{n+1}$ ($n \in \mathbb{N}_0$) gibt es jedoch keine derartigen Elemente.

Beispiel. Wir betrachten den Homomorphismus

$$f : \mathbb{Z}^2 \to \mathbb{Z}^4, \quad (a, b) \mapsto (4a, 2a, a + b, a - b),$$

sowie seinen zugehörigen ***Cokern*** $\operatorname{coker} f = \mathbb{Z}^4 / \operatorname{im} f$. Offensichtlich handelt es sich bei $\operatorname{coker} f$ um eine abelsche Gruppe, ja sogar um eine endlich erzeugte, denn $\mathbb{Z}^4$ wird ja schon von $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ und $(0,0,0,1)$ erzeugt, womit die zugehörigen Restklassen modulo $\operatorname{im} f$ natürlich den Cokern erzeugen. Man kann

$$\operatorname{coker} f \cong \mathbb{Z}^2 \times C_2$$

zeigen, was tatsächlich ein Produkt von zyklischen Gruppen ist, wie von Proposition 5.1 proklamiert wird. Wie man darauf kommt und wie man sogar einen solchen Isomorphismus explizit findet, besprechen wir in der *Algebra*-Vorlesung [45].

5.2. Endliche abelsche Gruppen

Wir erinnern an das folgende bereits aus den Übungen bekannte Ergebnis:

Lemma 5.2. *Für $n, m \in \mathbb{N}$ ist $C_n \times C_m$ genau dann zyklisch (und somit isomorph zu C_{nm}), wenn n und m teilerfremd sind.*

Beweis. Das ist Aufgabe 3.1 (a). □

Häufig schreibt man direkte Produkte $G \times H$ von *abelschen* Gruppen G und H auch als *direkte Summen* $G \oplus H$, was wir hier allerdings nicht tun möchten. (Wichtiger wird der Unterschied, wenn man direkte Summen $\prod_i G_i$ über eine unendliche Indexmenge betrachtet. Dann ist $\bigoplus_i G_i$ die Teilmenge der Elemente von $\prod_i G_i$ die in allen bis auf höchstens endlich vielen Einträgen nur 0_{G_i} stehen haben.)

Satz 5.3. *Jede endliche abelsche Gruppe ist isomorph zu einer Gruppe*

$$C_{q_1} \times C_{q_2} \times \ldots \times C_{q_t}$$

mit $t \in \mathbb{N}_0$ und Primzahlpotenzen $q_1, \ldots, q_t > 1$. Dabei sind t und die Primzahlpotenzen (bis auf Umnummerierung) durch G eindeutig bestimmt.

Beweis. Nach Proposition 5.1 ist jede endliche abelsche Gruppe G isomorph zu einem direkten Produkt $C_{n_1} \times \ldots \times C_{n_\ell}$. Die Zahlen n_j müssen dabei zwar noch keine Primzahlpotenzen sein, jedoch lässt sich dies durch weiteres Aufspalten leicht einrichten. Jedes $n = n_j$ lässt sich nämlich als ein Produkt von Primzahlpotenzen schreiben, $n = \prod_k p_k^{\nu_k}$ (mit $p_k \neq p_{\tilde{k}}$ für verschiedene $k, \tilde{k}$) und Lemma 5.2 liefert dann $C_n \cong \prod_k C_{p_k^{\nu_k}}$, denn mittels Lemma 3.2 folgert man leicht

$$\operatorname{ggT}\Big(p_{\tilde{k}}^{\nu_{\tilde{k}}}, \prod_{k \neq \tilde{k}} p_k^{\nu_k}\Big) = 1.$$

Hieraus ergibt sich die behauptete Isomorphie.

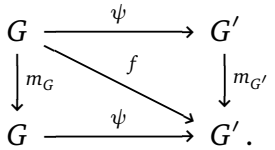
Nun zur *Eindeutigkeitsaussage*. Hierzu genügt es aus

$$G := C_{q_1} \times \ldots \times C_{q_t} \cong C_{q_1'} \times \ldots \times C_{q_{t'}'} =: G' \tag{5.3}$$

die Gleichheit von t und t', sowie von $(q_1, \ldots, q_t)$ und $(q_1', \ldots, q_t')$ bis auf Umordnung zu zeigen, wobei es sich bei $q_1, \ldots, q_t, q_1', \ldots, q_{t'}'$ um Primzahlpotenzen > 1 handle. Es sei $n = q_1 \cdots q_t = q_1' \cdots q_{t'}'$ und p ein Primteiler von $\#G$. Weil das direkte Produkt der C_{q_i} mit $p \mid q_i$ die eindeutige p-Sylowgruppe der Gruppe linker Hand in (5.3) ist (siehe Korollar 3.4) und eine ähnliche Aussage für die rechte Seite gilt, sieht man, dass sich der Isomorphismus in (5.3) zu einem Isomorphismus der jeweiligen p-Sylowgruppen links und rechts einschränkt. Wir dürfen daher im Folgenden davon ausgehen, dass es sich bei den q_i und q_i' jeweils um Potenzen derselben Primzahl p handelt.

Der in (5.3) angedeutete Isomorphismus sei nun mit $\psi\colon G \to G'$ bezeichnet. Für eine beliebige abelsche Gruppe H schreiben wir $m_H = m_{H,p}$ für die „Multiplikation-mit-p-Abbildung“ $m_H\colon H \to H$, $h \mapsto ph$. Man bestätigt leicht unter Ausnutzung der Abelizität von H, dass es sich bei m_H um einen Homomorphismus handelt. Wir betrachten nun den Homomorphismus $f\colon G \to G'$ gegeben durch $f := m_{G'} \circ \psi = \psi \circ m_G$:

(5.4)



Gemäß Korollar 2.7 ist

$$G/\ker f \cong \operatorname{im} f \tag{5.5}$$

und wir wollen beide Seiten näher bestimmen. Wegen der Injektivität von ψ haben wir

$$\begin{aligned}\ker f &= \{\, g \in G : \psi(m_G(g)) = 0_{G'} \,\} \\ &= \{\, g \in G : m_G(g) = 0_G \,\} \\ &= \ker m_G.\end{aligned}$$

Zur weiteren Bestimmung von $\ker f$ beachte man, dass die Verknüpfung in G komponentenweise definiert ist (siehe (5.3)). Demnach ist

$$\ker f = \ker m_G = \prod_{i \le t} \ker m_{C_{q_i}} \subseteq G.$$

Bei dem mittleren Produkt handelt es sich aber offensichtlich genau um den Kern des surjektiven Homomorphismus

$$G \to \prod_{i \le t} \frac{C_{q_i}}{\ker m_{C_{q_i}}}, \quad (g_1, \ldots, g_t) \mapsto \big(g_1 + \ker m_{C_{q_1}}, \ldots g_t + \ker m_{C_{q_t}}\big).$$

Korollar 2.7 liefert somit

$$\frac{G}{\ker f} = \frac{G}{m_G} \cong \prod_{i \le t} \frac{C_{q_i}}{\ker m_{C_{q_i}}}. \tag{5.6}$$

Analog (mittels Kommutativität von (5.4), Surjektivität von ψ und der komponentenweise definierten Verknüpfung auf G') sieht man

$$\operatorname{im} f = \operatorname{im}(\psi \circ m_G) = \operatorname{im}(m_{G'} \circ \psi) = \operatorname{im}(m_{G'}) = \prod_{k \le t'} \operatorname{im} m_{C_{q'_k}}.$$

Durch *komponentenweise* Anwendung von Korollar 2.7 sehen wir

$$\operatorname{im} f \cong \prod_{k \le t'} \frac{C_{q'_k}}{\ker m_{C_{q'_k}}}. \tag{5.7}$$

Durch Kombination von Gleichungen (5.5) bis (5.7) erhalten wir

$$\prod_{i \le t} \frac{C_{q_i}}{\ker m_{C_{q_i}}} \cong \prod_{k \le t'} \frac{C_{q'_k}}{\ker m_{C_{q'_k}}}. \tag{5.8}$$

Die auf beiden Seiten auftretenden Kerne bestehen jeweils genau aus dem neutralen Element und den Elementen der Ordnung p in den jeweiligen Gruppen. Gemäß Satz 1.12 (2) bestehen darum alle diese Kerne jeweils aus genau p Elementen.

Die auftretenden Faktorgruppen sind ebenfalls zyklisch (denn $C_u = \langle 1 \rangle$ und daher $\langle 1 + \ker m_{C_u} \rangle = C_u / \ker m_{C_u}$) und wir haben

$$\#\left(\frac{C_{q_i}}{\ker m_{C_{q_i}}}\right) = \frac{q_i}{p} < q_i, \quad \text{sowie} \quad \#\left(\frac{C_{q'_k}}{\ker m_{C_{q'_k}}}\right) = \frac{q'_k}{p} < q'_k. \tag{5.9}$$

Damit lässt sich die gewünschte Eindeutigkeitsaussage also durch eine Induktion über die Gruppenordnung beweisen. Der Fall von einelementiger Gruppen ist trivial und ist die Eindeutigkeitsaussage nun für alle abelschen Gruppen mit Ordnung $< \#G$ gezeigt, so folgt diese auch für alle abelschen Gruppen der Ordnung $\#G$, denn die Induktionsvoraussetzung angewendet auf (5.8) zeigt $t = t'$ und $q_{\sigma(i)}/p = q'_i/p$ (via (5.9)) für eine Permutation $\sigma \in \mathfrak{S}_t$ und alle $i = 1, \ldots, t$. Multiplikation mit p liefert $q_{\sigma(i)} = q'_i$ für $i = 1, \ldots, t$ und wir sind fertig. □

Beispiel 5.4 (Abelsche Gruppen mit Ordnung p^2q^3)**.** Wir bestimmen die Anzahl verschiedener Isomorphietypen abelscher Gruppen der Ordnung p^2q^3 mit zwei verschiedenen Primzahlen p und q. Nach Satz 5.3 gilt es direkte Produkte der Gruppen C_p, C_{p^2}, C_q, C_{q^2} und C_{q^3} zu betrachten. Wegen $2 = 1 + 1$ (zwei Zerlegungen) und $3 = 2 + 1 = 1 + 1 + 1$ (drei Zerlegungen) erhält man $2 \cdot 3 = 6$ Fälle:

(1)	$C_{p^2} \times C_{q^3}$,	(2)	$C_p \times C_p \times C_{q^3}$,
(3)	$C_{p^2} \times C_{q^2} \times C_q$,	(4)	$C_p \times C_p \times C_{q^2} \times C_q$,
(5)	$C_{p^2} \times C_q \times C_q \times C_q$,	(6)	$C_p \times C_p \times C_q \times C_q \times C_q$.

Satz 5.3 garantiert nun, dass jede abelsche Gruppe mit Ordnung p^2q^3 isomorph zu einer und nur einer der hier aufgeführten sechs Gruppen ist.

Beispiel 5.5 ((Abelsche) Gruppen mit Ordnung p^2)**.** Gemäß der zwei Zerlegungen $2 = 1 + 1$ reproduziert man auch das bereits aus Aufgabe 5.3 (d) bekannte Ergebnis, dass jede abelsche Gruppe der Ordnung p^2 (mit p prim) isomorph zu genau einer der beiden Gruppen C_{p^2} oder $C_p \times C_p$ ist. (In Aufgabe 5.3 (d) wird allerdings noch etwas mehr bewiesen nämlich, dass überhaupt schon jede Gruppe der Ordnung p^2 abelsch ist und folglich isomorph zu einer der beiden oben genannten Gruppen ist.)

5.3. Noch mal endlich erzeugte abelsche Gruppen

In diesem Abschnitt beweisen wir die folgende Verallgemeinerung von Satz 5.3. Der Unterschied besteht darin, dass wir statt endlichen abelschen Gruppen nun auch endlich erzeugte abelsche Gruppen (wie zum Beispiel $(\mathbb{Z}, +)$) zulassen:

Satz 5.6 (Hauptsatz über endlich erzeugte abelsche Gruppen)**.** *Jede endlich erzeugte abelsche Gruppe ist isomorph zu einer Gruppe*

$$\mathbb{Z}^k \times C_{q_1} \times C_{q_2} \times \ldots \times C_{q_t}$$

mit $k, t \in \mathbb{N}_0$ und Primzahlpotenzen $q_1, \ldots, q_t > 1$. Dabei sind k, t und die Primzahlpotenzen (bis auf Umnummerierung) durch G eindeutig bestimmt.

Beweis. Proposition 5.1 liefert bereits den fraglichen Isomorphismus, wenn man die zyklischen Faktoren, die isomorph zu $\mathbb{Z}$ sind, alle an den Anfang schreibt. Es gilt daher lediglich die Eindeutigkeitsaussage über k, t und die qs zu beweisen.

Wie im Beweis von Satz 5.3 (vgl. (5.3)) sei daher

$$G := \mathbb{Z}^k \times \underbrace{C_{q_1} \times \ldots \times C_{q_t}}_{=:T} \cong \mathbb{Z}^{k'} \times \underbrace{C_{q'_1} \times \ldots \times C_{q'_{t'}}}_{=:T'} =: G' \tag{5.10}$$

mit $k, t, k', t' \in \mathbb{N}_0$ und Primzahlpotenzen $q_1, \ldots, q_t, q'_1, \ldots, q'_{t'}$. Es gilt $k = k'$, $t = t'$ und $q_i = q'_i$ für $i = 1, \ldots, t$ einzusehen.

Für eine abelsche Gruppe H bezeichne $\mathrm{Tor}(H)$ die Menge der Elemente von H mit endlicher Ordnung. Dabei handelt es sich um eine Untergruppe von H.[2] Da Gruppenisomorphismen Ordnungen von Elementen invariant lassen, folgt aus (5.10)

$$\mathrm{Tor}(G) = \mathrm{Tor}(\mathbb{Z}^k \times T) = \{0\}^k \times T \cong T$$

und selbiges für G', also $T \cong T'$. Die Eindeutigkeitsaussage in Satz 5.3 liefert nun $t = t'$ und $q_i = q'_i$ für $i = 1, \ldots, t$.

Es verbleibt also nur noch, $k = k'$ einzusehen. Hierfür wenden wir $\mathrm{Hom}(\_, \mathbb{Q})$ auf (5.10) an. Wir beachten dabei, dass die Menge $\mathrm{Hom}(H, \mathbb{Q})$ für jede abelsche Gruppe H eine $\mathbb{Q}$-Vektorraumstruktur trägt: Vektoraddition und Skalarmultiplikation sind dabei einfach punktweise erklärt (für $f, g \in \mathrm{Hom}(H, \mathbb{Q})$ und $\lambda \in \mathbb{Q}$ ist $f + g := (h \mapsto f(h) + g(h))$ und $\lambda f := (h \mapsto \lambda f(h))$). Es gilt:

(1) Die Abbildung
$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) \longrightarrow \mathbb{Q}, \quad (f : \mathbb{Z} \mapsto \mathbb{Q}) \longmapsto f(1),$$
ist ein Isomorphismus von $\mathbb{Q}$-Vektorräumen.

(2) $\mathrm{Hom}(C_q, \mathbb{Q}) = \{\text{Nullabbildung}\}$ für $q \in \mathbb{N}$, denn jedes $f \in \mathrm{Hom}(C_q, \mathbb{Q})$ muss den Erzeuger 1 von C_q auf ein Element von $\mathbb{Q}$ mit endlicher Ordnung abbilden. Das einzige Element von $\mathbb{Q}$ mit endlicher Ordnung ist allerdings die 0. Insbesondere ist $\mathrm{Hom}(C_q, \mathbb{Q})$ isomorph zum Nullvektorraum $\mathbb{Q}^0$.

(3) Für abelsche Gruppen H und H' ist die Abbildung
$$\begin{aligned} &\mathrm{Hom}(H \times H', \mathbb{Q}) \longrightarrow \mathrm{Hom}(H, \mathbb{Q}) \times \mathrm{Hom}(H', \mathbb{Q}), \\ &(f : H \times H' \mapsto \mathbb{Q}) \longmapsto (f(\_, 1_{H'}), f(1_H, \_)), \end{aligned}$$
ein Isomorphismus von $\mathbb{Q}$-Vektorräumen.

(4) Ist $\phi : H \to H'$ ein Isomorphismus zweier abelscher Gruppen, so ist
$$\mathrm{Hom}(H', \mathbb{Q}) \longrightarrow \mathrm{Hom}(H, \mathbb{Q}), \quad (H' \xrightarrow{f} \mathbb{Q}) \longmapsto (H \underbrace{\xrightarrow{\phi} H' \xrightarrow{f}}_{f \circ \phi} \mathbb{Q}),$$
ein Isomorphismus von $\mathbb{Q}$-Vektorräumen.

[2] Hierfür ist die Abelizität von H wichtig, um sicherzustellen, dass Produkte von Elementen aus $\mathrm{Tor}(H)$ wieder in $\mathrm{Tor}(H)$ liegen. Siehe auch Aufgabe 1.3 für ein Beispiel einer (nicht-abelschen!) Gruppe in der das Produkt zweier Elemente von endlicher Ordnung selbst unendliche Ordnung hat.

Wir betrachten nun G aus (5.10). Dann erhalten wir

$$\operatorname{Hom}(G,\mathbb{Q}) \cong \operatorname{Hom}(\mathbb{Z},\mathbb{Q})^k \times \prod_{i\le t} \operatorname{Hom}(C_{q_i},\mathbb{Q}) \cong \mathbb{Q}^k \times \prod_{i\le t} \mathbb{Q}^0.$$

Diese Überlegung zusammen mit dem Isomorphismus aus (5.10) zeigt sodann

$$k = \dim_{\mathbb{Q}} \operatorname{Hom}(G,\mathbb{Q}) = \dim_{\mathbb{Q}} \operatorname{Hom}(G',\mathbb{Q}) = k',$$

wie gewünscht. Das beendet den Beweis. □

Teil 2

Ringtheorie

KAPITEL 6

Ringe

In diesem und den folgenden Kapiteln widmen wir uns der Ringtheorie. Diese bildet das Fundament für die Vorlesung *Algebra*. Wir verzichten darauf, hier viel Motivation zu geben und liefern diese dafür später, wenn wir die Theorie hinreichend weit entwickelt haben. In Kapitel 10 untersuchen wir die Lösbarkeit einiger ausgewählter Gleichungen in den ganzen Zahlen. (Das führt auf Fragestellungen, die im Rahmen der *Analysis* nur unzureichend gelöst werden können.) In Kapitel 11 geben wir einen Vorgeschmack auf die Inhalte der *Algebra*-Vorlesung und behandeln klassische geometrische Konstruktionsprobleme mit Zirkel und Lineal. In Anhang A stellen wir eine kryptographische Anwendung vor und besprechen Primzahltests. Insbesondere diese Anwendungen sind bereits mit dem Wissen aus dem hiesigen Kapitel zugänglich.

6.1. Definition und erste Eigenschaften

Ein ***Ring*** ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R zusammen mit zwei binären inneren Verknüpfungen $+\colon R \times R \to R$ („***Addition***“) und $\cdot\colon R \times R \to R$ („***Multiplikation***“), welche den folgenden Axiomen genügen:

(1) $(R, +)$ ist eine abelsche Gruppe. (Das zugehörige neutrale Element werde im Folgenden mit 0_R oder kurz 0 bezeichnet und heißt auch ***Nullelement von R***.)
(2) Die Verknüpfung $\cdot$ ist assoziativ und es existiert ein Element $1_R \in R$ (auch kurz mit 1 bezeichnet, auch ***Einselement von R*** genannt), sodass für alle $a \in R$ die Gleichungen $a \cdot 1_R = a = 1_R \cdot a$ erfüllt sind.
(3) Es gelten die beiden ***Distributivgesetze***:
   (a) $\forall a, b, c \in R\colon a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
   (b) $\forall a, b, c \in R\colon (a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Wie schon bei Gruppen überlegt man sich, dass man Produkte in R beliebig klammern darf. (Der Existenz inverser Elemente bezüglich $\cdot$, welche wir hier *nicht* fordern, bedarf es dafür nicht.) Wir folgen der schon bei multiplikativ geschriebenen Gruppen benutzten Konvention, das Symbol für die Multiplikation oft nicht zu schreiben, wenn dies nicht für das bessere Verständnis wichtig scheint. Mithin schreiben wir also oft nur ab statt $a \cdot b$. Überdies rechnen wir „*Punkt vor Strich*“: Ausdrücke wie $a \cdot b + c$ sind dementsprechend als $(a \cdot b) + c$ zu verstehen. Statt $(R, +, \cdot)$ sprechen wir oft nur

von einem „Ring R“, genau so, wie wir auch zuvor oft schon von einer „Gruppe G“ statt $(G, \circ)$ gesprochen haben.

Das zu $a \in R$ bezüglich $+$ inverse Element bezeichnen wir (wie schon bei additiv geschriebenen Gruppen) mit $-a$. Ein Element $b \in R$ mit $a \cdot b = 1_R$ nennen wir ***rechtsinvers zu a*** (oder ***Rechtsinverses zu a***). ***Linksinverse*** sind analog zu definieren. Besitzt ein Element $a \in R$ ein Rechtsinverses b, welches auch Linksinvers ist,[1] $a \cdot b = 1_R = b \cdot a$, so nennen wir a ***invertierbar*** und schreiben a^{-1} für b. Wir sagen auch a sei eine ***Einheit***. Die Menge

$$R^\times = \{\text{Einheiten } a \in R\}$$

bildet mit $\cdot|_{R^\times \times R^\times} \colon R^\times \times R^\times \to R^\times$ eine Gruppe mit $1_R = 1_{R^\times}$ als neutrale Element, die ***Einheitengruppe von R***.

Ist die Multiplikation $\cdot$ kommutativ (d.h. für alle $a, b \in R$ gilt $a \cdot b = b \cdot a$), so nennt man den Ring R ***kommutativ***. Falls R ein kommutativer Ring ist, $\cdot$ sich zu einer inneren Verknüpfung auf $R \setminus \{0_R\}$ einschränken lässt und $R \setminus \{0_R\}$ zusammen mit dieser eine Gruppe bildet, nennen wir R einen ***Körper***.

Bemerkung. In der Literatur sind verschiedene Definitionen des Ringbegriffs im Gebrauch. Manche Autoren fordern nicht die Existenz eines multiplikativ neutralen Elements 1_R und nennen das, was wir hier als Ringe bezeichnen, „unitäre Ringe“. (Andere Autoren nennen solche „Ringe“ zur besseren Abgrenzung auch „Rnge“. — Man beachte hier die Auslassung des Buchstabens „i“ als Hinweis auf die fehlende multiplikative Identität [Engl. „identity element“].) In der Literatur zur kommutativen Algebra und algebraischen Geometrie treten vornehmlich kommutative Ringe auf, weswegen dort unter dem Ring-Begriff zumeist automatisch der des kommutativen Rings verstanden wird.

Beispiele 6.1.

(1) Es sei $\mathbf{0}$ eine beliebige einelementige Menge. Dann gibt es genau eine binäre innere Verknüpfung auf $\mathbf{0}$ und wählt man diese als Addition und Multiplikation, so bekommt $\mathbf{0}$ die Struktur eines kommutativen Rings. In diesem sogenannten ***Nullring*** gilt $0_{\mathbf{0}} = 1_{\mathbf{0}}$. Dieser ist kein Körper, da $\mathbf{0} \setminus \{0_{\mathbf{0}}\}$ leer ist und also keine Gruppe bilden kann. Ist R ein Ring mit $0_R = 1_R$, so folgt $a = a \cdot 1_R = a \cdot 0_R = 0_R$ gemäß Proposition 6.2 (siehe unten) für alle $a \in R$ und R ist einelementig. Dann gilt $R \cong \mathbf{0}$ im Sinne der noch später zu definierenden Isomorphie von Ringen und der zugehörige Isomorphismus ist notwendigerweise sogar eindeutig (denn dieser muss ja 0_R auf $0_{\mathbf{0}}$ abbilden und ist dadurch schon vollständig bestimmt). Wir sagen in diesem Fall auch R sei „der“ Nullring, auch wenn die zugrundeliegenden einelementigen Mengen verschieden sind.

(2) $\mathbb{Z}$ ist ein kommutativer Ring. $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind jeweils Körper.

[1] Tatsächlich genügt es, die Existenz eines rechtsinversen Elements r zu a und eines Linksinversen ℓ zu fordern. Dann gilt nämlich schon automatisch $r = \ell$ und a ist eine Einheit, denn $r = r1_R = ra\ell = 1_R\ell = \ell$.

(3) Ist R ein Ring, so ist der Polynomring $R[X]$ in einer Unbestimmten/Variablen mit Koeffizienten aus R ein Ring. Für die genaue Definition von $R[X]$ siehe Kapitel 7.

(4) Sind R und S zwei Ringe, so ist auch das ***direkte Produkt*** $R \times S$ ein Ring mit komponentenweise zu definierenden Verknüpfungen (d.h. $(r,s)+(r',s') := (r+r', s+s')$ und $(r,s)\cdot(r',s') := (r\cdot r', s\cdot s')$). Wir haben $0_{R\times S} = (0_R, 0_S)$ und $1_{R\times S} = (1_R, 1_S)$.

(5) Ist R ein Ring und $n \in \mathbb{N}$, so ist die Menge $R^{n\times n}$ der $n\times n$-Matrizen mit Einträgen aus R ein Ring mit der üblichen Addition und Multiplikation von Matrizen. Speziell für Körper R kennt man dieses Objekt bereits sehr gut aus der linearen Algebra.
Für $m \in \mathbb{N}$, $m \neq n$, bildet die Menge $R^{m\times n}$ der $m\times n$-Matrizen mit Einträgen aus R *keinen* Ring, da keine Multiplikation zweier $m\times n$-Matrizen miteinander erklärt ist.

(6) Analog zu Matrizen, sei V ein Vektorraum. Dann ist die Menge $\mathrm{End}(V)$ der Endomorphismen von V (lineare Selbstabbildungen $V \to V$) zusammen mit punktweiser Addition und Verkettung von Abbildungen als Multiplikation ein Ring. Tatsächlich funktioniert diese Konstruktion schon mit einer beliebigen abelschen Gruppe G und der Menge $\mathrm{End}(G)$ der Gruppenendomorphismen von G.

(7) Es sei $A = \prod_{i\in\mathbb{N}} \mathbb{Z}$ die abelsche Gruppe aller Folgen ganzer Zahlen und $R = \mathrm{End}(A)$ die Menger ihrer Gruppenendomorphismen. Diese bildet, wie schon eben angemerkt, einen Ring mit punktweise definierter Addition und Verknüpfung von Abbildungen als Multiplikation. Das zugehörige Einselement ist $1_R = \mathrm{id}_A$. Man betrachte den Links- und den Rechtsshift

$$s_{\leftarrow}\colon A \to A, \quad (a_1, a_2, a_3, \ldots) \mapsto (a_2, a_3, \ldots),$$
$$s_{\rightarrow}\colon A \to A, \quad (b_1, b_2, b_3, \ldots) \mapsto (0, b_1, b_2, b_3, \ldots).$$

Dann ist $s_{\leftarrow} \circ s_{\rightarrow} = 1_R$, aber $s_{\rightarrow} \circ s_{\leftarrow}$ ist die Abbildung

$$(a_1, a_2, a_3, \ldots) \mapsto (0, a_2, a_3, \ldots).$$

Tatsächlich gibt es, da $s_{\leftarrow}$ nicht injektiv ist, kein $r \in R$ mit $r \circ s_{\leftarrow} = 1_R$. Ganz analog gibt es, da $s_{\rightarrow}$ nicht surjektiv ist, kein $r \in R$ mit $s_{\rightarrow} \circ r = 1_R$. Dieses Beispiel zeigt, dass es bei der Definition von Einheiten nicht unerheblich ist, zu fordern, dass jene *beidseitige* Inverse besitzen.

(8) Die Teilmenge $\mathbb{Z}[\mathrm{i}] = \{\, a + \mathrm{i}b \in \mathbb{C} : a, b \in \mathbb{Z} \,\}$ von $\mathbb{C}$ ist (mit der offensichtlichen Addition und Multiplikation) der kleinste Unterring von $\mathbb{C}$, der $\mathbb{Z}$ als Unterring enthält und auch i enthält,[2] der sogenannte ***Ring der ganzen Gaußschen Zahlen***; die Definition von „Unterring“ ist hier ganz analog zur Definition von Untergruppen in der Gruppentheorie, mit einem Zusatz: eine

[2]Achtung: z.B. $\mathbb{Z}[\sqrt[3]{2}] = \{\, a + \sqrt[3]{2}b + \sqrt[3]{4}c \in \mathbb{C} : a, b, c \in \mathbb{Z} \,\}$ ist nicht gleich $\{\, a + \sqrt[3]{2}b \in \mathbb{C} : a, b \in \mathbb{Z} \,\}$, da die letzte Menge kein Ring ist, da sie $\sqrt[3]{2}$ aber nicht $\sqrt[3]{4} = (\sqrt[3]{2})^2$ enthält.

Teilmenge $S \subseteq R$ heißt ***Unterring von R*** (oder ***Teilring von R***), falls sich die Verknüpfungen $+\colon R \times R \to R$ und $\cdot\colon R \times R \to R$ zu Verknüpfungen $S \times S \to S$ einschränken lassen, S mit diesen einen Ring bildet und 1_R in S enthalten ist.[3]

Bemerkung (Moduln und Vektorräume)**.** In der Gruppentheorie waren Gruppenoperationen sehr wichtig und vermochten viel Einsicht für das Studium von Gruppen zu liefern. Betrachtet man statt einer Gruppe G und einer Menge M einen Ring R und eine abelsche Gruppe M, so ist $\mathrm{End}(M)$ ein Ring und Ringhomomorphismen[4] $R \to \mathrm{End}(M)$ liefern ein Pendant zu Gruppenoperationen für die Ringtheorie. Im Gewand der Analogie aus Proposition 2.13 führt dies zum Begriff des ***R-Moduls***, den wir in der Vorlesung „Algebra“ noch näher studieren werden. Speziell für *Körper K* handelt es sich bei den K-Moduln um nichts anderes als ***K-Vektorräume***. Mit Anwendungen der (bekannten!) Vektorraumtheorie auf die Körpertheorie beschäftigen wir uns tatsächlich aber auch schon in der aktuellen Vorlesung und zwar später in Kapitel 11.

Proposition 6.2. *Es seien R ein Ring und $a, b \in R$ beliebig. Dann gilt:*

(1) Die additive bzw. multiplikativ neutralen Elemente 0_R und 1_R sind eindeutig bestimmt.
(2) $a \cdot 0_R = 0_R = 0_R \cdot a$.
(3) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$.
(4) $(-a) \cdot (-b) = a \cdot b$.

Beweis. Die erste Aussage folgt mit demselben Argument wie in Proposition 1.1 (1). Für die übrigen Aussagen beachte man

(2) $0_R = a \cdot 0_R - a \cdot 0_R = a \cdot (0_R + 0_R) - a \cdot 0_R = (a \cdot 0_R + a \cdot 0_R) - a \cdot 0_R = a \cdot 0_R$,
$0_R = 0_R \cdot a - 0_R \cdot a = \ldots = 0_R \cdot a$,
(3) $0_R = a \cdot 0_R = a \cdot (b - b) = a \cdot b + a \cdot (-b)$, also $a \cdot (-b) = -(a \cdot b)$,
$0_R = 0_R \cdot b = (a - a) \cdot b = a \cdot b + (-a) \cdot b$, also $(-a) \cdot b = -(a \cdot b)$,
(4) $(-a) \cdot (-b) = -(-(a \cdot b)) = a \cdot b$, wobei sich die letzte Gleichung aus Proposition 1.1 (5) angewandt auf die Gruppe $(R, +)$ ergibt. □

6.2. Homomorphismen, Ideale und Faktorringe

In diesem Abschnitt übertragen wir den bereits für Gruppen in § 2.1 studierten Homomorphismus-Begriff, sowie die aus § 2.2 für Gruppen bekannte Faktorbildung auf die Ringtheorie.

[3] $\mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z}$ ist *kein* Teilring von $\mathbb{Z} \times \mathbb{Z}$: das Element $(1, 0)$ übernimmt in $\mathbb{Z} \times \{0\}$ zwar die Rolle eines multiplikativ neutralen Elements, stimmt allerdings nicht mit $1_{\mathbb{Z}\times\mathbb{Z}} = (1, 1) \notin \mathbb{Z} \times \{0\}$ überein.

[4] Die zugehörige Definition folgt in § 6.2.1.

6.2.1. Homomorphismen. Eine Abbildung $f: R \to S$ zwischen Ringen R und S heißt ***(Ring-)Homomorphismus***, falls die folgenden Eigenschaften erfüllt sind:[5]

(1) $\forall a, b \in R$: $f(a+b) = f(a) + f(b)$,
(2) $\forall a, b \in R$: $f(a \cdot b) = f(a) \cdot f(b)$,
(3) $f(1_R) = 1_S$.

Bemerkung. Wir fordern hier nicht extra $f(0_R) = 0_S$, da die vorhandenen Axiome bereits garantieren, dass f ein Gruppenhomomorphismus von $(R,+)$ nach $(S,+)$ ist und Lemma 2.1 dann schon $f(0_R) = 0_S$ liefert. Hierfür war die Existenz inverser Elemente wichtig, was in den zugehörigen additiven Gruppen natürlich gewährleistet ist, für die Multiplikation allerdings nicht der Fall zu sein braucht. Man beachte etwa das Beispiel $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $n \mapsto (n, 0)$, welches kein Ringhomomorphismus ist.

Analog wie bei Gruppen (siehe § 2.1 auf Seite 27) definiert man ***Ring-{Mono/Iso-/Endo/Auto}-morphismen***. Zwei Ringe R und S heißen ***isomorph***, — in Zeichen $R \cong S$ —, falls es einen Ringisomorphismus $f: R \to S$ gibt. Wir definieren auch $\mathrm{Hom}(R,S)$, $\mathrm{End}(R)$, $\mathrm{Aut}(R)$ analog.

Proposition 6.3. *Für jeden Ring R gibt es genau einen Ringhomomorphismus $R \to \mathbf{0}$ in den Nullring $\mathbf{0}$ und genau einen Ringhomomorphismus $\mathbb{Z} \to R$.*

Beweis. Die erste Aussage ist klar, da es überhaupt nur eine *Abbildung* $R \to \mathbf{0}$ gibt und diese trivialerweise ein Ringhomomorphismus ist. Für die zweite Aussage beachte man, dass ein Ringhomomorphismus $f: \mathbb{Z} \to R$ wegen $f(1) = 1_R$ und $\mathbb{Z} = \langle 1 \rangle$ (als abelsche Gruppen) bereits vollständig bestimmt ist. Umgekehrt rechnet man leicht nach, dass durch

$$f(0) := 0_R, \quad f(n) := \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ mal}}, \quad f(-n) := -f(n)$$

($n \in \mathbb{N}$) ein Ringhomomorphismus $f: \mathbb{Z} \to R$ gegeben ist. □

6.2.2. Ideale. Als nächstes Ziel fassen wir ins Auge, die in § 2.2 entwickelte Theorie der Faktorgruppen (deren Nützlichkeit wir uns mittlerweile schon bewusst geworden sind) auch für Ringe brauchbar zu machen. Hier diskutieren wir zunächst die Unterstrukturen, nach denen eine Faktorbildung bei Ringen möglich ist (sogenannte „Ideale“). Die Definition von Faktorringen folgt im Anschluss (in § 6.2.3). Wir modellieren unsere Diskussion an der zuvor geführten Diskussion von Normalteilern in § 2.2.1.

[5] Leserinnen und Lesern sollte klar sein, dass bei „+“ in $f(a+b)$ die Addition in R und bei „+“ in $f(a) + f(b)$ die Addition in S gemeint ist. Bei Gruppen waren wir oft noch bemüht derartige Doppeldeutigkeiten durch anders gewählte Symbole zu vermeiden, doch hier bei Ringen wird dies schnell lästig: jeder Ring kommt mit zwei inneren Verknüpfungen und bei zwei Ringen bräuchte man dann schon vier verschiedene Symbole usw.

Ist $f: R \to S$ ein Ringhomomorphismus, so handelt es sich bei dem ***Kern*** $\ker f := f^{-1}(\{0_S\})$ in aller Regel *nicht* um einen Unterring[6] von R, denn sonst müsste ja $1_R \in \ker f$ gelten und dann hätten wir für alle $a \in R$ die Gleichung

$$f(a) = f(1_R \cdot a) = f(1_R) \cdot f(a) = 0_S \cdot f(a) = 0_S,$$

also $\ker f = R$ und f bildet jedes Element $a \in R$ trivial auf 0_S ab. Wir wollen uns nun trotzdem überlegen, welche Struktur $\ker f$ besitzt. Jedenfalls ist $\ker f$ eine Untergruppe von $(R,+)$, ja sogar ein Normalteiler, da $(R,+)$ aber abelsch ist, liefert dies keine neue Information. Überdies gilt für $a \in \ker f$ und $r \in R$

$$f(a \cdot r) = f(a) \cdot f(r) = 0_S \cdot f(r) = 0_S, \quad \text{also} \quad a \cdot r \in \ker f.$$

Analog folgt auch $r \cdot a \in \ker f$.

Eine Teilmenge $\mathfrak{a} \subseteq R$, die eine Untergruppe von $(R,+)$ bildet und

$$\forall a \in \mathfrak{a}\ \forall r \in R\colon ar \in \mathfrak{a} \text{ und } ra \in \mathfrak{a}$$

erfüllt, nennt man ***Ideal von R*** und schreibt hierfür auch $\mathfrak{a} \trianglelefteq R$. Mit dem wie bei Gruppen definierten Komplexprodukt schreibt sich die obige Bedingung als $\mathfrak{a}R \subseteq \mathfrak{a}$ und $R\mathfrak{a} \subseteq \mathfrak{a}$. (Fordert man nur eine der beiden Inklusionen, so spricht man von ***Rechts-*** bzw. ***Linksidealen***. Wir werden diese hier jedoch nicht näher betrachten.)

Der Schnitt $\mathfrak{a} \cap \mathfrak{b}$ zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von R ist wieder ein Ideal. Sei $a \in R$. Analog wie bei Gruppen definiert man $\langle a \rangle$ als das (bezüglich der durch Mengeninklusion gegebenen partiellen Ordnung) kleinste Ideal von R welches a enthält. Wie bei Gruppen sieht man, dass $\langle a \rangle$ mit dem Schnitt aller a-enthaltenden Ideale übereinstimmt. Man nennt $\langle a \rangle$ das von a erzeugte ***Hauptideal***. Allgemein nennt man ein Ideal $\mathfrak{a} \trianglelefteq R$ ***Hauptideal***, falls $\mathfrak{a}$ von der Form $\mathfrak{a} = \langle a \rangle$ für ein $a \in R$ ist. Ist R ein *kommutativer* Ring, so ist $\langle a \rangle = aR = \{ ar : r \in R \}$.

Ist nun allgemeiner $A \subseteq R$ eine beliebige Teilmenge von R, so schreibt man $\langle A \rangle$ für das kleinste Ideal von R, welches A enthält, und nennt dieses das ***von A erzeugte*** Ideal. Ein Ideal $\mathfrak{a} \trianglelefteq R$ heißt ***endlich erzeugt***, falls $\mathfrak{a} = \langle A \rangle$ für eine *endliche* Teilmenge $A \subseteq R$ ist. Ist R wieder als kommutativ vorausgesetzt, so ist

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} a_i r_i : n \in \mathbb{N}_0 \text{ und } a_i \in A,\ r_i \in R \text{ für alle } i = 1, \ldots, n \right\}.$$

Speziell im endlich erzeugten Fall ist

$$\langle a_1, \ldots, a_k \rangle = a_1 R + \ldots + a_k R.$$

Beispiel 6.4. Die Ideale von $\mathbb{Z}$ sind genau die Mengen $\langle n \rangle = n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ (siehe Proposition 1.11).

[6] Dieser Defekt ist mitunter einer der Gründe, den manche Autoren für das Aussparen der Existenz von 1_R in der Definition von Ringen anführen.

Beispiel 6.5. (Hier sei davon ausgegangen, dass die Leserinnen und Leser bereits grundlegend mit Polynomen vertraut sind. Wir behandeln diese später aber noch ausführlich.) Für $R = \mathbb{Z}$ ist $\langle 6, 4\rangle = 6\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$ (siehe Lemma 1.6). Für $R = \mathbb{Z}[X]$ ist $\langle 2, X\rangle = 2\mathbb{Z}[X] + X\mathbb{Z}[X] = \{ p \in \mathbb{Z}[X] : 2 \mid p(0) \}$ kein Hauptideal, denn ein etwaiger Erzeuger a müsste Grad 0 haben und durch 2 teilbar, aber dann wäre $\langle 2, X\rangle \ni 2 + X \notin \langle a\rangle$.

Ein kommutativer Ring R ist genau dann ein Körper, wenn $\{0_R\}$ und R die einzigen Ideale von R sind und $R \neq \{0_R\}$ ist.

6.2.3. Faktorringe. Es sei R ein Ring und $\mathfrak{a} \trianglelefteq R$ ein Ideal. Dann lässt sich die Faktorgruppe $R/\mathfrak{a}$ von $(R, +)$ nach der Untergruppe $\mathfrak{a}$ auch mit einer Multiplikation ausstatten:

$$(r + \mathfrak{a}) \cdot (r' + \mathfrak{a}) := (r \cdot r') + \mathfrak{a}.$$

(Achtung: die linke Seite ist i.Allg. kein Komplexprodukt der zugehörigen [additiven] Linksnebenklassen: $(0 + 2\mathbb{Z})(0 + 2\mathbb{Z}) = 4\mathbb{Z} \neq 0 + 2\mathbb{Z} = (0 + 2\mathbb{Z}) \cdot (0 + 2\mathbb{Z})$.) Die eben definierte Multiplikation ist wirklich wohl-definiert, d.h. unabhängig von den gewählten Repräsentanten r und r' der Nebenklassen $r + \mathfrak{a}$ und $r' + \mathfrak{a}$, denn je zwei solche Repräsentanten unterscheiden sich gemäß Lemma 2.4 nur um Addition mit einem Element von $\mathfrak{a}$ und für $a, a' \in \mathfrak{a}$ ist

$$(r + a) \cdot (r' + a') = (r + a) \cdot r' + (r + a) \cdot a' = r \cdot r' + \underbrace{a \cdot r' + r \cdot a' + a \cdot a'}_{\in \mathfrak{a}}.$$

Also repräsentieren $r \cdot r'$ und $r \cdot r' + a \cdot r' + r \cdot a' + a \cdot a'$ tatsächlich dieselbe Nebenklasse bezüglich $\mathfrak{a}$.

Man rechnet nun unmittelbar nach, dass die Faktorgruppe $R/\mathfrak{a}$ zusammen mit der soeben definierten Multiplikation wirklich einen Ring bildet, den ***Faktorring von R nach*** $\mathfrak{a}$. Die kanonische Projektion $\pi\colon R \to R/\mathfrak{a}$, $r \mapsto r + \mathfrak{a}$, ist nicht nur ein Homomorphismus der zugrundeliegenden additiven Gruppen, sondern sogar ein Ringhomomorphismus (die Gleichung $\pi(r \cdot r') = \pi(r) \cdot \pi(r')$ entnimmt man direkt der Definition der Multiplikation und $\pi(1_R) = 1_R + \mathfrak{a} = 1_{R/\mathfrak{a}}$ ist auch klar).

Der Kern von π ist (weil dies schon auf Ebene der zugrundeliegenden additiven Gruppen bekannt ist) genau $\mathfrak{a}$. Zusammen mit unseren Überlegungen, die uns auf die Definition von Idealen führten, erhalten wir nun die folgende Variante von Korollar 2.5 für Ringe:

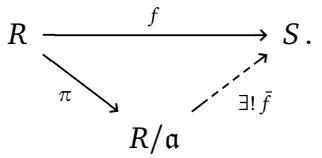
Korollar 6.6. *Sei R ein Ring. Dann sind die Ideale von R genau die Kerne von Ringhomomorphismen mit Definitionsbereich R:*

$$\{\textit{Ideale } \mathfrak{a} \textit{ von } R\} = \{ \ker f : S \textit{ Ring}, f \in \mathrm{Hom}(R, S) \}.$$

Bemerkung. Der Vergleich von Korollar 6.6 mit Korollar 2.5 zeigt, dass der Ideal-Begriff in der Ringtheorie genau die Rolle des Normalteiler-Begriffs aus der Gruppentheorie übernimmt.

Wir haben die folgende Variante von Satz 2.6 für Ringe:

Satz 6.7. *Es sei $\mathfrak{a}$ ein Ideal eines Rings R und $f\colon R \to S$ ein Ringhomomorphismus in einen Ring S. Ferner sei $\mathfrak{a} \subseteq \ker f$. Dann gibt es genau einen Ringhomomorphismus $\bar{f}\colon R/\mathfrak{a} \to S$, der das folgende Diagramm kommutativ macht:*



Die Zuordnung $f \mapsto \bar{f}$ stiftet also eine 1:1-Korrespondenz

$$\{\, f \in \mathrm{Hom}(R,S) : \mathfrak{a} \trianglelefteq \ker f \,\} \xrightarrow{1:1} \mathrm{Hom}(R/\mathfrak{a}, S)\,.$$

Ist $\mathfrak{a} = \ker f$, so ist $\bar{f}$ injektiv.

Beweis. Auf Ebene der additiven Gruppen ist die Aussage des Satzes bereits aus Satz 2.6 bekannt; insbesondere ist Existenz und Eindeutigkeit von $\bar{f}$ als Gruppenhomomorphismus von $(R/\mathfrak{a}, +)$ nach $(S, +)$ schon gesichert und wir müssen nur noch prüfen, dass $\bar{f}$ auch wirklich ein Ringhomomorphismus ist. Wegen

$$\begin{aligned}\bar{f}((r+\mathfrak{a})\cdot(r'+\mathfrak{a})) &= \bar{f}(\pi(r)\cdot\pi(r')) = \bar{f}(\pi(r\cdot r')) = f(r\cdot r')\\ &= f(r)\cdot f(r') = \bar{f}(\pi(r))\cdot\bar{f}(\pi(r')) = \bar{f}(r+\mathfrak{a})\cdot\bar{f}(r'+\mathfrak{a})\end{aligned}$$

und $\bar{f}(1_{R/\mathfrak{a}}) = \bar{f}(\pi(1_R)) = f(1_R) = 1_S$ ist dies jedoch klar.

Der Zusatz über $\mathrm{Hom}(R/\mathfrak{a}, S)$ war bereits in der Situation von Satz 2.6 eine formale Konsequenz aus der darüber gemachten Aussage mit dem Diagramm und überträgt sich ohne Weiteres auf die hiesige Situation mit Ringen. □

6.2.4. Isomorphie- und Korrespondenzsatz. Wir übertragen nun den bereits aus der Gruppentheorie bekannten (ersten) Isomorphiesatz (Korollar 2.7), sowie den Korrespondenzsatzes (Satz 2.9) von Faktorgruppen auf Faktorringe.

Korollar 6.8 (Erster Isomorphiesatz)**.** *Es sei $f\colon R \to S$ ein Ringhomomorphismus zwischen Ringen R und S. Dann ist $R/\ker f \cong f(R)$.*

Beweis. Der Beweis verläuft wie schon der Beweis von Korollar 2.7, aber wir wiederholen diesen dennoch. Die f zugeordnete Abbildung $\bar{f}\colon R/\ker f \to S$ aus Satz 6.7 ist injektiv und bildet natürlich surjektiv auf ihr Bild ab; dieses stimmt mit dem Bild von f überein, weshalb die eingeschränkte Abbildung $\bar{f}\colon R/\ker f \to f(R)$ ein Ringisomorphismus ist. □

Satz 6.9 (Korrespondenzsatz)**.** *Es sei R ein Ring, $\mathfrak{a} \trianglelefteq R$ ein Ideal von R und $\pi\colon R \to R/\mathfrak{a}$, $r \mapsto r + \mathfrak{a}$, bezeichne die kanonische Projektion. Dann handelt es sich bei der Abbildung*

$${}^{\mathfrak{a}}\pi\colon \begin{cases}\{\text{Ideale } \mathfrak{b} \trianglelefteq R/\mathfrak{a}\} \to \{\text{Ideale } \mathfrak{c} \trianglelefteq R \text{ mit } \mathfrak{c} \supseteq \mathfrak{a}\},\\ \mathfrak{b} \mapsto \pi^{-1}(\mathfrak{b}),\end{cases}$$

um eine inklusionserhaltende Bijektion.

Beweis. Aus Satz 2.9 (bzw. Aufgabe 4.2) ist bereits bekannt, dass $U \mapsto \pi^{-1}(U)$ eine entsprechende Bijektion von Untergruppen U von $(R/\mathfrak{a}, +)$ auf Untergruppen V von $(R, +)$ stiftet. Man braucht hier also nur zu prüfen, dass sich alles geeignet auf Ideale einschränkt. Die Details seien der geneigten Leserin oder dem geneigten Leser zur freiwilligen Übung überlassen. □

6.2.5. Einfachheit. Sei R ein Ring. Ein Ideal $\mathfrak{m}$ von R heißt maximal, wenn $\mathfrak{m} \neq R$ ist und es kein Ideal $\mathfrak{a}$ von R mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$ gibt. Ein Ring R, der nicht der Nullring ist, heißt ***einfach***, falls $\{0_R\}$ und R die einzigen Ideale von R sind. (Es handelt sich um das natürliche Analogon des aus § 4.3 bekannten Einfachheitsbegriffs für Gruppen.)

Ein *kommutativer* Ring R ist genau dann einfach, wenn er ein Körper ist. (Denn ist R einfach, so ist für jedes $a \neq 0_R$ das Ideal $\langle a \rangle = aR$ notwendigerweise gleich R und es gibt ein $r \in R$ mit $ra = ar = 1_R$. Also ist a eine Einheit. Umgekehrt sieht man auch, dass in einem Körper K jedes Ideal $\mathfrak{a} \trianglelefteq K$ entweder das Nullideal ist, oder ein Element $a \neq 0_K$ enthält, welches dann, da es invertierbar ist, das Ideal $K = \langle a \rangle \subseteq \mathfrak{a} \subseteq K$ erzeugt. Also folgt $\mathfrak{a} = K$.)

Korollar 6.10. *Es sei R ein Ring und $\mathfrak{m}$ ein Ideal von R. Genau dann ist $\mathfrak{m}$ ein maximales Ideal, wenn $R/\mathfrak{m}$ einfach ist. Speziell für kommutative Ringe ist $\mathfrak{m}$ genau dann ein maximales Ideal, wenn $R/\mathfrak{m}$ ein Körper ist.*

Beweis. Das folgt unmittelbar aus dem Korrespondenzsatz (Satz 6.9) zusammen mit der vorangegangenen Überlegung. □

Beispiel 6.11 (Der Körper $\mathbb{F}_p$)**.** Der Ring $\mathbb{Z}/n\mathbb{Z}$ (mit $n \in \mathbb{N}$) ist genau dann ein Körper, wenn n eine Primzahl ist: In der Tat sind die Ideale von $\mathbb{Z}$ genau die Mengen $n\mathbb{Z}$ (siehe Beispiel 6.4) und Proposition 1.11 zeigt, dass $n\mathbb{Z}$ genau dann ein maximales Ideal ist, wenn n prim ist. Die Behauptung über $\mathbb{Z}/n\mathbb{Z}$ folgt also aus Korollar 6.10. Ist p prim, so ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ also ein Körper mit genau p Elementen. In der *Algebra*-Vorlesung wird gezeigt, dass es genau dann einen Körper mit n Elementen gibt, wenn n eine Primzahlpotenz ist. Überdies sind je zwei endliche Körper mit derselben Mächtigkeit isomorph (siehe [45, Satz 4.1]).

Beispiel ($\mathbb{Q}^{2\times 2}$ ist einfach)**.** Es sei R ein beliebiger kommutativer Ring. Wir schreiben hier zur Abkürzung 0 und 1 für 0_R bzw. 1_R. Dann ist $R^{2\times 2}$ nicht kommutativ:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Wir behaupten nun, dass jedes beidseitige Ideal $\mathfrak{A}$ von $R^{2\times 2}$ von der Form

$$\mathfrak{A} = \begin{pmatrix} \mathfrak{a} & \mathfrak{a} \\ \mathfrak{a} & \mathfrak{a} \end{pmatrix} := \mathfrak{a}^{2\times 2} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathfrak{a} \right\}$$

mit einem geeigneten Ideal $\mathfrak{a}$ von R ist und umgekehrt jedes Ideal $\mathfrak{a}$ von R auch so ein Ideal $\mathfrak{A}$ von $R^{2\times 2}$ produziert. (Eine analoge Aussage gilt für Ideale von $R^{n\times n}$ für

alle $n \in \mathbb{N}$.) Die letzte Behauptung rechnet man leicht nach. Wir kümmern uns daher nur um die erste. Sei $\mathfrak{A}$ also ein Ideal von $R^{2\times 2}$. Wir behaupten, dass

$$\mathfrak{a} = \left\{ a \in R : \exists b, c, d \in R \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{A} \right\}$$

die oben genannte Eigenschaft hat. Dabei ist $\mathfrak{a}$ sicher ein Ideal von R, denn für $a, a' \in \mathfrak{a}$ ist offensichtlich $a + a' \in \mathfrak{a}$ und für $r \in R$ zeigt

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix},$$

dass auch $ar = ra$ ein Element von $\mathfrak{a}$ ist. Für

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{A}$$

zeigen die Rechnungen

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix},$$

dass a, b, c und d in $\mathfrak{a}$ enthalten sind. Also ist $\mathfrak{A} \subseteq \mathfrak{a}^{2\times 2}$. Für die umgekehrte Inklusion sei

$$\begin{pmatrix} a & a' \\ a'' & a''' \end{pmatrix} \in \mathfrak{a}^{2\times 2}.$$

Die Rechnungen von oben zeigen, dass

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{A}.$$

für $x = a, a', a'', a'''$ gilt. Durch Links- und Rechts-Multiplikation mit geeigneten Permutationsmatrizen erhält man daraus

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \in \mathfrak{A}.$$

Also ist

$$\begin{pmatrix} a & a' \\ a'' & a''' \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a' \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a'' & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a''' \end{pmatrix} \in \mathfrak{A}.$$

Das zeigt $\mathfrak{A} \supseteq \mathfrak{a}^{2\times 2}$. Insgesamt ist also $\mathfrak{A} = \mathfrak{a}^{2\times 2}$, wie gewünscht.

Unsere Ausführungen zeigen, dass $\mathbb{Q}^{2\times 2}$ einfach ist. Es handelt sich hierbei allerdings, *mangels Kommutativität*, *nicht* um einen Körper.

Beispiel (Hamiltonsche Quaternionen)**.** $\mathbb{Q}^{2\times 2}$ aus dem obigen Beispiel ist einfach, aber nicht kommutativ. Tatsächlich ist auch nicht jedes von der Nullmatrix verschiedene Element von $\mathbb{Q}^{2\times 2}$ invertierbar: Betrachte etwa die *singuläre* Matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{Q}^{2\times 2}.$$

Ringe R, für welche jedes Element $r \in R \setminus \{0_R\}$ eine Einheit ist, nennt man auch ***Schiefkörper***. *Kommutative* Schiefkörper sind natürlich genau Körper. Andererseits gibt es auch *nichtkommutative* Schiefkörper, wie zum Beispiel die ***Hamiltonschen Quaternionen*** $\mathbb{H}$. Diese lassen sich als Unterring von $\mathbb{C}^{2\times 2}$ wie folgt konstruieren:

$$\mathbb{H} := \left\{ \begin{pmatrix} a+b\mathrm{i} & c+d\mathrm{i} \\ -c+d\mathrm{i} & a-b\mathrm{i} \end{pmatrix} \in \mathbb{C}^{2\times 2} : a,b,c,d \in \mathbb{R} \right\}.$$

Wir identifizieren reelle Zahlen a mit der Matrix $a\mathbf{1}_2 = a1_{\mathbb{H}} \in \mathbb{H}$. Dies stiftet einen injektiven Ringhomomorphismus $\iota_{\mathbb{R}} \colon \mathbb{R} \hookrightarrow \mathbb{H}$. Die Elemente von $\mathbb{H}$ lassen sich in eindeutiger Weise wie folgt zerlegen:[7]

$$\begin{pmatrix} a+b\mathrm{i} & c+d\mathrm{i} \\ -c+d\mathrm{i} & a-b\mathrm{i} \end{pmatrix} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k};$$

Hier ist

$$\mathbf{i} := \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad \mathbf{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} := \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

Es gilt

$$\det \begin{pmatrix} a+b\mathrm{i} & c+d\mathrm{i} \\ -c+d\mathrm{i} & a-b\mathrm{i} \end{pmatrix} = a^2 + b^2 + c^2 + d^2.$$

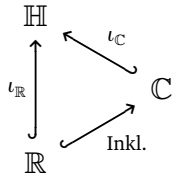
Das Quaternion $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ ist als Element von $\mathbb{C}^{2\times 2}$ daher invertierbar solange nur $z \neq 0_{\mathbb{H}}$ gilt. Eine kurze Rechnung (etwa mittels der Cramerschen Regel) zeigt, dass die zu $z \neq 0_{\mathbb{H}}$ inverse Matrix ebenfalls in $\mathbb{H}$ liegt. *Damnach ist jedes* $z \in \mathbb{H} \setminus \{0_{\mathbb{H}}\}$ *invertierbar!*
Man bestätigt leicht die Gleichungen $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1_{\mathbb{H}}$. Darüber hinaus bestätigt man leicht, dass es sich bei

$$\iota_{\mathbb{C}} \colon \mathbb{C} \longrightarrow \mathbb{H}, \quad z = a + b\mathrm{i} \longmapsto a + b\mathbf{i} = \begin{pmatrix} a+b\mathrm{i} & 0 \\ 0 & a-b\mathrm{i} \end{pmatrix} = \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix},$$

um einen injektiven Ringhomomorphismus handelt. Die Einbettungen $\iota_{\mathbb{R}}$ und $\iota_{\mathbb{C}}$ sind in dem Sinne miteinander verträglich, als dass es unerheblich ist, ob man eine reelle Zahl a erst als komplexe Zahl $a + \mathrm{i}b$ auffasst und dann mit $\iota_{\mathbb{C}}$ als Quaternion $a + \mathbf{i}b$ auffasst, oder die reelle Zahl a direkt mittels $\iota_{\mathbb{R}}$ als Quaternion auffasst: Das

[7] Hier ist „a“ gemäß der obigen Identifikation zu verstehen, also als „$a\mathbf{1}_2$“ zu lesen.

Diagramm



ist kommutativ.

6.2.6. Existenz maximaler Ideale. Korollar 6.10 liefert eine Methode zur Konstruktion von Körpern („besonders schönen Ringen“) aus einem bekannten Ring R: man wähle ein maximales Ideal $\mathfrak{m}$ von R und betrachte den Körper $R/\mathfrak{m}$. Von dieser Methode werden wir in der Vorlesung *Algebra* noch vielfachen Gebrauch machen (siehe [45, § 2.2 und § 2.3]). Für den Moment soll uns hier nur die Frage interessiert, ob es überhaupt stets maximale Ideale gibt.

Satz 6.12 (Existenzsatz für maximale Ideale)**.** *Es sei R ein Ring und $\mathfrak{a} \neq R$ ein beliebiges Ideal von R. Dann gibt es ein maximales Ideal $\mathfrak{m}$ von R mit $\mathfrak{m} \supseteq \mathfrak{a}$.*

Korollar 6.13. *In jedem Ring außer dem Nullring gibt es ein maximales Ideal.*

Beweis. In jedem Ring R ist $\mathfrak{a} = \{0_R\}$ ein Ideal und ist R nicht der Nullring, so gilt $\mathfrak{a} \neq R$. Satz 6.12 liefert nun schon die Behauptung. □

Für den Beweis von Satz 6.12 benötigen wir das ***Lemma von Zorn*** (für mehr hierzu, siehe etwa [37, Appendix 2]). Man beachte auch Abbildung 17.

Lemma 6.14 (Zorn)**.** *Sei $\mathscr{M}$ eine nichtleere Menge, die bezüglich einer binären Relation $\preceq$ **partiell geordnet** ist.*[8] *Ferner besitze jede **Kette**[9] eine obere Schranke in $\mathscr{M}$. Dann enthält $\mathscr{M}$ mindestens ein maximales Element.*

Beweis von Satz 6.12. Wir betrachten die Menge $\mathscr{M}$, der Ideale $\neq R$ von R, welche $\mathfrak{a}$ enthalten, zusammen mit der partiellen Ordnung, welche durch mengentheoretische Inklusion gegeben ist (ein Ideal $\mathfrak{a}_1 \in \mathscr{M}$ ist kleiner oder gleich $\mathfrak{a}_2$ genau dann wenn $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$). Wegen $\mathfrak{a} \in \mathscr{M}$ ist diese Menge jedenfalls nicht leer. Ferner besitzt jede Kette $(\mathfrak{a}_i)_i$ eine obere Schranke; hierfür kann man etwa $\mathfrak{A} := \bigcup_i \mathfrak{a}_i$ wählen und bestätigt unmittelbar, dass es sich hierbei um ein Ideal von R handelt, welches natürlich auch $\mathfrak{a}$ und jedes $\mathfrak{a}_i$ aus der Kette enthält. (Die Ideal-Eigenschaft braucht i.Allg. für eine beliebige Vereinigung von Idealen natürlich nicht mehr gelten, doch sichert die Ketten-Eigenschaft hier dennoch, dass $\mathfrak{A}$ ein Ideal ist.) Überdies ist $\mathfrak{A}$ auch $\neq R$, denn anderenfalls wäre ja $1_R \in \mathfrak{A}$ und also $1_R \in \mathfrak{a}_i$ für ein i, womit wir $\mathfrak{a}_i = R$, also einen Widerspruch zu $\mathfrak{a}_i \in \mathscr{M}$ erhielten. Das Lemma von Zorn (Lemma 6.14) liefert nun die Behauptung. □

[8] Zur Erinnerung: Das heißt, dass die Relation $\preceq$ reflexiv, antisymmetrisch und transitiv ist. Allerdings braucht $\preceq$ nicht notwendigerweise ***total*** zu sein, d.h. es kann durchaus Elemente $a, x \in \mathscr{M}$ geben, für die weder $a \preceq x$ noch $x \preceq a$ gilt. — Siehe auch Abbildung 17.

[9] Das ist eine bezüglich $\preceq$ total geordnete Teilmenge von $\mathscr{M}$.

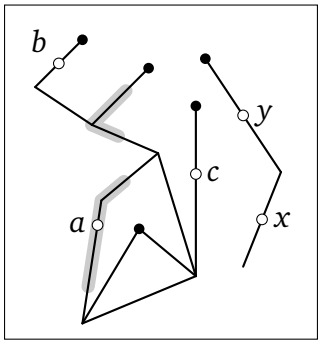


Abbildung 17. Veranschaulichung zum *Lemma von Zorn*: Die Menge $\mathscr{M}$ sei hier durch das schwarz gefärbte „Gebilde“ im $\mathbb{R}^2$ repräsentiert und ein Punkt darauf sei „kleiner“ als ein anderer Punkt, wenn man von dem Ausgangspunkt stetig und in der Vertikalen monoton steigend zum anderen Punkt „laufen“ kann. Beispielsweise ist a kleiner als b und x kleiner als y. Des Weiteren kann man keinen der Punkte a, b, oder x miteinander vergleichen. Alle maximalen Elemente sind als schwarze Punkte im Gebilde hervorgehoben. Grau hinterlegt sieht man eine Kette.

6.3. Chinesischer Restsatz

In diesem Abschnitt vergleichen wir die Struktur des Faktorrings $R/\bigcap_i \mathfrak{a}_i$ nach einem Durchschnitt $\bigcap_i \mathfrak{a}_i$ von Idealen $\mathfrak{a}_i$ mit der Struktur der einzelnen Faktorringe $R/\mathfrak{a}_i$. Das Hauptergebnis hierzu ist der sogenannte *Chinesische Restsatz* (Satz 6.16). Als Anwendung davon bestimmen wir in § 6.3.4 die Struktur der Einheitengruppen $(\mathbb{Z}/n\mathbb{Z})^\times$.

6.3.1. Kongruenzen. Ist R ein Ring, $\mathfrak{a}$ ein Ideal von R und $\pi\colon R \to R/\mathfrak{a}$ die kanonische Projektion. Dann schreiben wir auch oft „$r \bmod \mathfrak{a}$“ statt $\pi(r)$. Sind $r, r' \in R$, so schreiben wir

$$r \equiv r' \bmod \mathfrak{a} \quad :\Longleftrightarrow \quad \pi(r) = \pi(r') \quad \Longleftrightarrow \quad r - r' \in \mathfrak{a} = \ker \pi$$

und sagen r ist ***kongruent*** zu r' ***modulo*** $\mathfrak{a}$.

Lemma 6.15 (Rechenregeln für Kongruenzen)**.** *Es sei R ein Ring und $\mathfrak{a}$ ein Ideal von R. Für alle $a, a', b, b', c \in R$ gelten dann die folgenden Aussagen:*

(1) $a \equiv a \bmod \mathfrak{a}$; *(Reflexivität)*
(2) $a \equiv b \bmod \mathfrak{a} \Longleftrightarrow b \equiv a \bmod \mathfrak{a}$; *(Symmetrie)*
(3) $(a \equiv b \bmod \mathfrak{a}) \wedge (b \equiv c \bmod \mathfrak{a}) \implies a \equiv c \bmod \mathfrak{a}$; *(Transitivität)*
(4) $(a \equiv a' \bmod \mathfrak{a}) \wedge (b \equiv b' \bmod \mathfrak{a}) \implies a + b \equiv a' + b' \bmod \mathfrak{a}$;
(5) $(a \equiv a' \bmod \mathfrak{a}) \wedge (b \equiv b' \bmod \mathfrak{a}) \implies ab \equiv a'b' \bmod \mathfrak{a}$.

Beweis. Die gemachten Aussagen ergeben sich leicht aus der Definition. □

Speziell für $R = \mathbb{Z}$ ist jedes Ideal $\mathfrak{a}$ von R von der Form $a\mathbb{Z}$ mit einem $a \in \mathbb{Z}$ (und umgekehrt; siehe Proposition 1.11) und wir schreiben $r \bmod a$ statt $r \bmod \mathfrak{a}$.

Beispiel. $11 \equiv 1 \bmod 5$, denn $11 - 1 = 10 = 5 \cdot 2$ ist durch 5 teilbar und somit ein Element von $5\mathbb{Z} = \ker(\pi\colon \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z})$.

Mit Kongruenzrechnung lassen sich diverse Rechenhilfen begründen, die man sicher schon aus der Schule kennt. (Die praktische Bedeutung dieser Rechenhilfen sollte eher als gering eingeschätzt werden, aber dafür haben einige davon vielleicht eine gewisse intrinsische Ästhetik.)

Beispiele (Teilbarkeitsregeln)**.** Für $a_0, a_1, \ldots, a_n \in \{0, \ldots, 9\}$ schreiben wir

$$[\![a_n \ldots a_1 a_0]\!] = \sum_{m=0}^{n} a_m 10^m;$$

Das ist die Zahl, deren Ziffern im Dezimalsystem von links nach rechts gelesen genau $a_n, \ldots, a_1, a_0$ lauten. Zum Beispiel:

$$[\![837]\!] = 8 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0 = 800 + 30 + 7 = 837.$$

(1) (Teilbarkeit durch 2.) Ohne groß überlegen zu müssen, sehen wir sofort, dass 837 nicht durch 2 teilbar ist. Dies erkennen wir, indem wir auf die letzte Ziffer (= 7) schauen und feststellen, dass diese nicht durch 2 teilbar ist. Diese Rechenhilfe ist aus der Schule bekannt. Zu ihrer Begründung kann Kongruenzrechnung herangezogen werden. Wegen Lemma 6.15 ist nämlich $10^m \equiv 0^m \bmod 2$ und damit weiter

$$\begin{aligned}[\![a_n \ldots a_1 a_0]\!] &= a_n 10^n + \ldots + a_1 10^1 + a_0 10^0 \\ &\equiv a_n 0^n + \ldots + a_1 0^1 + a_0 0^0 \equiv a_0 \mod 2.\end{aligned}$$

Also ist $[\![a_n \ldots a_1 a_0]\!]$ genau dann kongruent 0 modulo 2 (d.h. durch 2 teilbar), wenn dies schon auf die Ziffer a_0 zutrifft.

(2) (Teilbarkeit durch 5.) Wegen $10 \equiv 0 \bmod 5$ liefert derselbe Beweis eine analoge Teilbarkeitsregel für Teilbarkeit durch 5: die Zahl $[\![a_n \ldots a_1 a_0]\!]$ ist genau dann durch 5 teilbar, wenn a_0 durch 5 teilbar ist, also wenn $a_0 \in \{0, 5\}$ gilt.

(3) (Teilbarkeit durch 10.) Wegen $10 \equiv 0 \bmod 10$ folgt auch, dass $[\![a_n \ldots a_1 a_0]\!]$ genau dann durch 10 teilbar ist, wenn dies auf a_0 zutrifft, also wenn $a_0 = 0$ gilt.

(4) (***Dreierprobe***.) Wir haben $10 \equiv 1 \bmod 3$ und darum

$$[\![a_n \ldots a_1 a_0]\!] = \sum_{m=0}^{n} a_m 10^m = \sum_{m=0}^{n} a_m \mod 3.$$

Also ist die Zahl $[\![a_n \ldots a_1 a_0]\!]$ genau dann durch 3 teilbar, wenn dies auf ihre Quersumme $a_n + \ldots + a_1 + a_0$ zutrifft. Beispielsweise ist die Zahl 837 durch 3 teilbar, denn wir haben $8 + 3 + 7 = 18 = 6 \cdot 3$. Tatsächlich hätten

wir dieses Argument auch iterieren können: 18 ist durch 3 teilbar, denn $1+8=9=3\cdot 3$ ist durch 3 teilbar.

(5) (***Neunerprobe***.) Wir haben $10\equiv 1 \bmod 9$ und dasselbe Argument wie oben liefert, dass die Quersumme einer Zahl auch über Teilbarkeit durch 9 entscheiden lässt. Beispielsweise ist die Zahl 837 (Quersumme: 18) nicht nur durch 3, sondern sogar durch 9 teilbar.

(6) (***Elferprobe***.) Wegen $10\equiv -1 \bmod 11$ erhält man eine analoge Teilbarkeitsregel für 11, jedoch mit der *alternierenden* Quersumme. Für 837 ist diese $8-3+7=12$, womit sich 837 als nicht durch 11 teilbar erweist.

(7) (Teilbarkeit durch M.) Wir behaupten, dass man analoge Teilbarkeitsregeln für Teilbarkeit durch beliebige Zahlen M auffinden kann. Die Details seien den interessierten Leserinnen und Lesern überlassen; Wir geben nur als Beispiel (ohne Beweis) die Aussage: „Die Zahl 44388 ist durch 27 teilbar, weil $4\cdot 19+4\cdot 1+3\cdot 10+8\cdot 19+8\cdot 1=270$ durch 27 teilbar ist“.

6.3.2. Chinesischer Restsatz. Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ eines Ringes R heißen ***teilerfremd***, falls ihre Summe $\mathfrak{a}+\mathfrak{b}=\{a+b : a\in\mathfrak{a}, b\in\mathfrak{b}\}$ mit R übereinstimmt. Diese Summe ist des Übrigen stets ein Ideal von R, wie man leicht nachrechnet; Gleiches gilt für den Schnitt $\mathfrak{a}\cap\mathfrak{b}$.

Satz 6.16 (Chinesischer Restsatz, allgemeine Form)**.** *Es sei R ein Ring und $(\mathfrak{a}_i)_i$ eine endliche Folge von paarweise teilerfremden Idealen von R (d.h. $\mathfrak{a}_i+\mathfrak{a}_j=R$ für $i\neq j$). $\pi_i\colon R\to R/\mathfrak{a}_i$, $r\mapsto r+\mathfrak{a}_i$, bezeichne die kanonische Projektion. Dann handelt es sich bei der Abbildung*

$$f\colon R\to\prod\nolimits_i (R/\mathfrak{a}_i),\quad r\mapsto(\pi_i(r))_i,$$

um einen Ringhomomorphismus mit Kern $\ker f=\bigcap_i \mathfrak{a}_i$ *und f induziert (gemäß Korollar 6.8) einen Isomorphismus*

$$R\Big/\bigcap\nolimits_i \mathfrak{a}_i\cong\prod\nolimits_i (R/\mathfrak{a}_i),$$

der $\pi(r)=r+\bigcap_i\mathfrak{a}_i$ auf $(\pi_i(r))_i=(r+\mathfrak{a}_i)_i$ abbildet:

$$\begin{array}{ccc} R & \xrightarrow{(\pi_i)_i} & \prod_i (R/\mathfrak{a}_i)\,. \\ {\scriptstyle\pi}\downarrow & \nearrow_{\sim} & \\ R\Big/\bigcap_i \mathfrak{a}_i & & \end{array}$$

Beweis. Es ist klar, dass es sich bei f um einen Ringhomomorphismus handelt. Mithin genügt es gemäß Korollar 6.8 also nachzuweisen, dass f surjektiv ist und $\ker f=\bigcap_i\mathfrak{a}_i$ gilt. Die Aussage über den Kern ist offensichtlich.

Zum Nachweis der *Surjektivität* von f genügt es, für jedes j aus der zugrundeliegenden Indexmenge ein Element $r_j \in R$ mit

$$r_j + \mathfrak{a}_i = \begin{cases} 1_{R/\mathfrak{a}_j} & \text{falls } i = j, \\ 0_{R/\mathfrak{a}_i} & \text{falls } i \neq j, \end{cases}$$

(für alle i) zu finden, denn jedes Element im Zielbereich von f lässt sich dann als Bild einer geeigneten „Linearkombination“ der Elemente r_j unter f schreiben.
Für $n = 1$ ist das natürlich trivial. Wir stellen die Idee für den allgemeinen Fall zunächst für $n = 2$ dar: Wegen $\mathfrak{a}_1 + \mathfrak{a}_2 = R$ gibt es Elemente $r_2 \in \mathfrak{a}_1$ und $r_1 \in \mathfrak{a}_2$ (man beachte die umgedrehte Nummerierung!) mit $r_2 + r_1 = 1_R$. Man sieht sofort, dass diese Elemente das Gewünschte leisten.
Nun sei $n \geq 2$ beliebig. Für $i, j \in \{1, \ldots, n\}$, $i \neq j$, lassen sich dank der Annahme $\mathfrak{a}_i + \mathfrak{a}_j = R$ Elemente $u_{ij} \in \mathfrak{a}_i$ $v_{ji} \in \mathfrak{a}_j$ mit $u_{ij} + v_{ji} = 1_R$ wählen. Mit jenen setzen wir

$$r_j := \prod_{i \neq j} u_{ij} = \prod_{i \neq j} (1_R - v_{ji}).$$

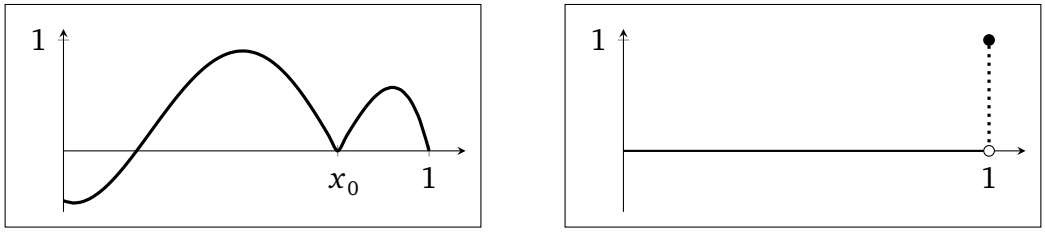
Die erste Produktdarstellung zeigt $r_j \in \mathfrak{a}_i$ für alle $i \neq j$. Aus der zweiten Produktdarstellung erhalten wir wegen $1_R - v_{ji} \equiv 1_R \bmod \mathfrak{a}_j$ zusätzlich $r_j \equiv 1_R \bmod \mathfrak{a}_j$. □

Bemerkung. Wir schreiben die Konstruktion der r_j $(1 \leq j \leq n)$ aus dem Beweis von Satz 6.16 noch für den Fall $n = 3$ explizit aus: Hierfür ist

$$1_R = u_{21} + v_{12} = u_{31} + v_{13} = u_{12} + v_{21} = u_{32} + v_{23} = u_{13} + v_{31} = u_{23} + v_{32}$$

mit $u_{ij} \in \mathfrak{a}_i$, $v_{ji} \in \mathfrak{a}_j$ und man konstruiert daraus

$$r_1 = u_{21}u_{31}, \quad r_2 = u_{12}u_{32} \quad \text{und} \quad r_3 = u_{13}u_{23}.$$



(a) Eine Funktion $g \in R$, die in dem maximalen Ideal $\mathfrak{m}_{x_0} = \{h \in R : h(x_0) = 0\}$ von R enthalten ist.

(b) Das Element $(g_x)_x \in \prod_{x \in [0,1]} \mathbb{R}$ ist *nicht* von der Form $(g(x))_x$ für ein $g \in R$, denn eine derartige Funktion g wäre bei 1 unstetig.

Abbildung 18. Zum Chinesischen Restsatz: Hier ist R der Ring der stetigen Funktionen von $[0, 1]$ nach $\mathbb{R}$.

Bemerkung. Der Chinesische Restsatz ist im Allgemeinen *falsch*, wenn es sich bei der Folge der Ideale $(\mathfrak{a}_i)_i$ um eine *unendliche* Folge handelt. Um dies zu sehen betrachten

wir etwa den Ring R der stetigen Funktionen $g\colon I \to \mathbb{R}$ mit $I = [0,1]$. Wie in Aufgabe 10.1 gesehen, handelt es sich für jedes $x \in I$ bei $\mathfrak{m}_x = \{\, g \in R : g(x) = 0 \,\}$ um ein maximales Ideal von R und die Auswertung $\mathrm{ev}_x\colon R \to \mathbb{R}$, $g \mapsto g(x)$, bei x induziert einen Isomorphismus $\overline{\mathrm{ev}}_x\colon R/\mathfrak{m}_x \cong \mathbb{R}$. Wegen Maximalität ist $\mathfrak{m}_x + \mathfrak{m}_y = R$ für alle $x, y \in I$ mit $x \neq y$. Ferner ist

$$\bigcap_{x\in[0,1]} \mathfrak{m}_x = \{\, g \in R : \forall x \in [0,1]\colon g(x) = 0 \,\} = \{\text{Nullfunktion}\} = \{0_R\}.$$

Der in Satz 6.16 konstruierte Homomorphismus $\bar{f}$ nimmt folgende Form an:

$$\begin{aligned} R \xrightarrow{\sim} R \Big/ \bigcap_{x\in I} \mathfrak{m}_x \xrightarrow{\bar{f}} \prod_{x\in I} (R/\mathfrak{m}_x) \xrightarrow[(\overline{\mathrm{ev}}_x)_x]{\sim} \prod_{x\in I} \mathbb{R}\,, \\ (h_x + \mathfrak{m}_x)_x \longmapsto (h_x(x))_x\,, \\ g \longmapsto g + \{0_R\} \longmapsto (g + \mathfrak{m}_x)_x \longmapsto (g(x))_x\,. \end{aligned}$$

Die Zusammensetzung dieser Homomorphismen ist injektiv (denn die äußeren beiden Homomorphismen sind als Isomorphismen insbesondere injektiv und $\bar{f}$ ist ebenfalls injektiv), jedoch *nicht* surjektiv (insbesondere ist $\bar{f}$ nicht surjektiv). In der Tat wird das Element von $\prod_{x\in I} \mathbb{R}$, welches in der Komponente mit Index 1 den Wert 1 hat und in allen anderen Komponenten der Wert 0, nicht als Bild erreicht, denn es gibt keine *stetige* Funktion $g\colon I \to \mathbb{R}$ mit diesem Abbildungsverhalten (siehe Abbildung 18).

6.3.3. Anwendung auf $\mathbb{Z}/n\mathbb{Z}$. Wir benutzen nun den Chinesischen Restsatz, um die Struktur von $\mathbb{Z}/n\mathbb{Z}$ zu untersuchen. Anschließend klären wir in § 6.3.4 auch noch die Struktur der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Jede natürliche Zahl n besitzt eine ***Primfaktorzerlegung*** $n = p_1 \cdots p_r$ mit Primzahlen $p_1, \ldots, p_r$, wie man leicht mittels Induktion beweist, denn für $n = 1$ ist dies klar (wähle $r = 0$; leeres Produkt) und (Induktion!) eine Zahl $n > 1$ ist entweder schon prim oder lässt sich als ein Produkt zweier kleiner natürlicher Zahlen schreiben, die gemäß Induktionsvoraussetzung schon eine Primfaktorzerlegung besitzen. Gruppiert man gleiche Primzahlen in der Primfaktorzerlegung von n zusammen, so erhält man (nach etwaiger Umbenennung der Variablen) $n = p_1^{\nu_1} \cdots p_t^{\nu_t}$ mit Exponenten $\nu_i \geq 1$ und *paarweise verschiedenen* Primzahlen p_i. Diese Darstellung ist bis auf Umnummerierung der Faktoren eindeutig, denn aus dem Lemma von Euklid (Lemma 3.2) folgt $\nu_i = \nu_p(n) := \max\{\, k \in \mathbb{N}_0 : p_i^k \mid n \,\}$.

Wir schreiben im Folgenden $p^\nu \parallel n$, falls p prim ist und p^ν die höchste Potenz von p ist, welche n teilt.

Beispiel. $2^2 \parallel 4$, $2^2 \parallel 12$, aber $6 \nparallel 30$, da 6 nicht prim ist.

Es sei $p^\nu \parallel n$. Schreiben wir $m = n/p^\nu$, so folgt $p \nmid m$ und somit sind p und m teilerfremd. Dann sind aber auch p^ν und m teilerfremd, denn jeder Primteiler eines gemeinsamen Teilers von p^ν und m müsste laut Lemma 3.2 ein Teiler von p sein, also

gleich p sein. Laut Lemma 1.6 ist also $p^\nu\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. Aus Aufgabe 4.4 ergibt sich $p^\nu\mathbb{Z} \cap m\mathbb{Z} = n\mathbb{Z}$. Eine Induktion zeigt nun

$$\bigcap_{p^\nu \| n} p^\nu = n\mathbb{Z}.$$

Satz 6.16 liefert dann das folgende Ergebnis:

Korollar 6.17 (Chinesischer Restsatz)**.** *Für $n \in \mathbb{N}$ ist*

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{p^\nu \| n} (\mathbb{Z}/p^\nu\mathbb{Z})$$

mittels der Abbildung $r + n\mathbb{Z} \mapsto (r + p^\nu\mathbb{Z})_{p^\nu \| n}$.

Beispiel. Wir betrachten den durch Korollar 6.17 erhaltenen Isomorphismus $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ näher. Dieser bildet wie folgt ab:

$$\begin{cases} 0 \bmod 6 \mapsto \binom{0 \bmod 2}{0 \bmod 3}, & 1 \bmod 6 \mapsto \binom{1 \bmod 2}{1 \bmod 3}, & 2 \bmod 6 \mapsto \binom{0 \bmod 2}{2 \bmod 3}, \\ 3 \bmod 6 \mapsto \binom{1 \bmod 2}{0 \bmod 3}, & 4 \bmod 6 \mapsto \binom{0 \bmod 2}{1 \bmod 3}, & 5 \bmod 6 \mapsto \binom{1 \bmod 2}{2 \bmod 3}. \end{cases}$$

Nun prüfen wir noch exemplarisch die Gleichung $f(a+b) = f(a) + f(b)$ für unseren Isomorphismus f und zwei Elemente a, b von $\mathbb{Z}/6\mathbb{Z}$. Wir haben

$$(2 \bmod 6) + (3 \bmod 6) = (2 + 3 \bmod 6) = (5 \bmod 6),$$

sowie

$$\binom{0 \bmod 2}{2 \bmod 3} + \binom{1 \bmod 2}{0 \bmod 3} = \binom{0 + 1 \bmod 2}{2 + 0 \bmod 3} = \binom{1 \bmod 2}{2 \bmod 3}.$$

Bemerkung. Die in Korollar 6.17 benutzte Zerlegung $n = \prod_{p^\nu \| n} p^\nu$ ist besonders fein. Man kann allerdings auch mit etwas gröberen Zerlegungen arbeiten. So liefern die bereits diskutierten Argumente auch für jede Zerlegung $n = ab$ von n in ein Produkt teilerfremder Zahlen a und b einen Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/ab\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}).$$

Mit der oben eingeführten Notation $\nu_p(n) := \max\{ k \in \mathbb{N}_0 : p_i^k \mid n \}$ gelten für $n, m \in \mathbb{N}$ auch die folgenden beiden Gleichungen:

$$\operatorname{ggT}(n,m) = \prod_{\substack{p \mid nm \\ p \text{ prim}}} p^{\min\{\nu_p(n), \nu_p(m)\}}, \quad \operatorname{kgV}(n,m) = \prod_{\substack{p \mid nm \\ p \text{ prim}}} p^{\max\{\nu_p(n), \nu_p(m)\}}.$$

Dabei folgt die zweite offenbar leicht aus der ersten zusammen mit

$$\prod_{\substack{p \mid nm \\ p \text{ prim}}} p^{\nu_p(n) + \nu_p(m)} = mn = \operatorname{ggT}(n,m) \operatorname{kgV}(n,m)$$

(siehe Aufgabe 4.4 für die letzte hier gelistete Gleichung). Zum Beweis der Gleichung für $\mathrm{ggT}(n,m)$ beachte man, dass

$$g := \prod_{\substack{p \mid nm \\ p \text{ prim}}} p^{\min\{\nu_p(n),\nu_p(m)\}}$$

offensichtlich ein gemeinsamer Teiler von n und m ist. Also gilt $g \leq \mathrm{ggT}(n,m)$. Um die umgekehrte Ungleichung zu sehen, beachte man, dass wegen $\mathrm{ggT}(n,m) \mid n$ sicher $\nu_p(\mathrm{ggT}(n,m)) \leq \nu_p(n)$ folgt. Eine analoge Betrachtung mit m statt n zeigt insgesamt $\nu_p(\mathrm{ggT}(n,m)) \leq \min\{\nu_p(n),\nu_p(m)\}$ und also $\mathrm{ggT}(n,m) \leq g$.

6.3.4. Anwendung auf die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$. Sind R und S zwei Ringe, so gilt $(R\times S)^\times = R^\times \times S^\times \subseteq R\times S$ und eine analoge Aussage gilt für beliebige direkte Produkte. Damit ergibt sich das nächste Ergebnis:

Korollar 6.18 (Struktur von $(\mathbb{Z}/n\mathbb{Z})^\times$)**.** *Für $n \in \mathbb{N}$ gilt* $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{p^\nu \| n} (\mathbb{Z}/p^\nu\mathbb{Z})^\times$.

Lemma 6.19. *Für $n \in \mathbb{N}$ gilt $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ mit der Eulerschen φ-Funktion aus § 1.4 und für Primzahlpotenzen p^ν gilt $\varphi(p^\nu) = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$.*

Beweis. Bekanntlich ist $\varphi(p^\nu)$ die Anzahl der Zahlen $1 \leq m \leq p^\nu$, die zu p^ν teilerfremd sind. Dies sind — wegen eindeutiger Primfaktorzerlegung, oder Lemma von Bézout, Lemma 1.6 — genau die zu p teilerfremden Zahlen. Wir haben dann

$$\begin{aligned}
\varphi(p^\nu) &= \#\{\,1 \leq m \leq p^\nu : \mathrm{ggT}(m,p^\nu) = 1\,\} \\
&= \#\{\,1 \leq m \leq p^\nu : p \nmid m\,\} \\
&= p^\nu - \#\{\,1 \leq m \leq p^\nu : p \mid m\,\} \\
&= p^\nu - \#\{\,x \in \mathbb{N} : px \leq p^\nu\,\} \\
&= p^\nu - p^{\nu-1}.
\end{aligned}$$

Nun beweisen wir noch $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ für $n \in \mathbb{N}$. Ist nämlich $a \in \mathbb{Z}$ teilerfremd zu n, so gibt es laut Lemma 1.6 Zahlen $x,y \in \mathbb{Z}$ mit $ax + ny = 1$. Dann ist $(a \bmod n)(x \bmod n) = (1 \bmod n)$ und somit $(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^\times$. Ist Umgekehrt $(a \bmod n)(x \bmod n) = (1 \bmod n)$, so ist n ein Teiler von $ax-1$, d.h. $ax - 1 = ny$ und somit $ax + ny = 1$. Daraus folgt auch die Teilerfremdheit von a und n. Wir haben also gesehen, dass $a \bmod n$ genau dann invertierbar ist, wenn a und n teilerfremd sind. Daraus folgt $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$. □

Beispiel. Die Zahl 17 ist prim und wir haben daher $\#(\mathbb{Z}/17\mathbb{Z})^\times = \varphi(17) = 16 = 2^4$.

Korollar 6.20. $\varphi(n) = \prod_{p^\nu \| n} p^{\nu-1}(p-1) = n \prod_{\substack{p \mid n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right)$.

Beweis. Man kombiniere Korollar 6.18 und Lemma 6.19. □

Bemerkung. Sind n und m teilerfremde natürliche Zahlen, so folgert man aus Korollar 6.20 leicht $\varphi(nm) = \varphi(n)\varphi(m)$. (Alternativ erhält diese Aussage aber schon deutlich direkter aus der Bemerkung unter Korollar 6.17.) Diese Eigenschaft nennt man in der Zahlentheorie auch ***Multiplikativität*** (von $\varphi\colon \mathbb{N} \to \mathbb{C}$). Man beachte hierbei allerdings, dass $\varphi(nm) = \varphi(n)\varphi(m)$ nicht zu gelten braucht, wenn n und m nicht teilerfremd sind, z.B. $\varphi(2 \cdot 2) = 2 \neq 1 \cdot 1 = \varphi(2)\varphi(2)$. Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ mit $f(nm) = f(n)f(m)$ für alle n und m nennt man in der Zahlentheorie auch ***vollständig multiplikativ***. Man sieht leicht, dass solche Funktionen bereits eindeutig durch ihre Werte $f(p)$ an den Primzahlen p bestimmt sind. Für lediglich multiplikative Funktionen kommt es zusätzlich auf die Werte an Primzahlpotenzen p^ν an.

Korollar 6.18 reduziert die Untersuchung der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ auf die Untersuchung von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ für Primzahlpotenzen p^ν. Dieses Problem wurde von C. F. Gauß gelöst.

Satz 6.21 (Gauß). *Es sei $p \neq 2$ eine Primzahl und $\nu \geq 1$. Dann gilt*
(1) $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ *ist zyklisch mit Ordnung* $\varphi(p^\nu) = p^{\nu-1}(p-1)$.
(2) $(\mathbb{Z}/2\mathbb{Z})^\times \cong C_1$,
(3) $(\mathbb{Z}/2^2\mathbb{Z})^\times \cong C_2$,
(4) $(\mathbb{Z}/2^{2+\nu}\mathbb{Z})^\times \cong C_2 \times C_{2^\nu}$.

Beweis. Die Aussagen (2) und (3) lassen sich ohne großen Aufwand händisch verifizieren. Der Beweis der übrigen Aussagen ist insgesamt recht aufwändig und wird teilweise in Übungsaufgaben ausgelagert. Die Anzahlformel aus (1) ist durch Lemma 6.19 bereits geklärt. Den Fall $\nu = 1$ in (1) stellen wir zurück, bis wir einige elementare Eigenschaften von Polynomen diskutiert haben (siehe Korollar 7.8). Darauf aufbauend, wird der Fall $\nu \geq 2$ in Aufgabe 10.2 behandelt. Die ungefähre Strategie besteht darin, induktiv für $\nu = 1, 2, \ldots$ einen Erzeuger $r + p^\nu\mathbb{Z}$ von $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ zu einem Erzeuger von $(\mathbb{Z}/p^{\nu+1}\mathbb{Z})^\times$ „hochzuheben“. Die Betrachtung von Zweierpotenzen in (4) wird in Aufgabe 9.3 erledigt. □

Zusammen mit Aufgabe 3.1 (a) und dem Eindeutigkeitsteil in Satz 5.3 kann man hieraus das folgende Ergebnis ableiten:

Korollar 6.22 (Gauß). *Für natürliche Zahlen n ist $(\mathbb{Z}/n\mathbb{Z})^\times$ genau dann zyklisch, wenn n aus der folgenden Liste von Zahlen stammt:* 1, 2, 4, p^ν, $2p^\nu$ *(mit p prim und $\nu \in \mathbb{N}$).*

Das nächste Beispiel mag als Illustration des hier nicht näher ausgeführten Beweises von Korollar 6.22 dienen.

Beispiele. (1) Die Gruppe

$$\begin{aligned}(\mathbb{Z}/36\mathbb{Z})^\times &\cong (\mathbb{Z}/2^2\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \\ &\cong C_2 \times C_{3(3-1)} \\ &= C_2 \times C_6 \\ &\cong C_2 \times C_2 \times C_3\end{aligned}$$

ist *nicht* zyklisch. Das sieht man einerseits direkt aus Satz 5.3, aber andererseits auch mittels Satz 1.12 und Korollar 2.8, da eine zyklische Gruppe ja für jeden Teiler d ihrer Ordnung genau eine Untergruppe mit Ordnung d besitzt. Die untere Gruppe, $C_2 \times C_2 \times C_3$, besitzt allerdings zwei verschiedene Untergruppen mit Ordnung 2, nämlich $\{0\} \times C_2 \times C_3$ und $C_2 \times \{0\} \times C_3$.

(2) $(\mathbb{Z}/18\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \cong C_1 \times C_{3(3-1)} \cong C_{3(3-1)}$ ist zyklisch.

6.3.5. Primitivwurzeln. Es sei n eine natürliche Zahl. Eine Zahl $g \in \mathbb{Z}$ derart, dass $g \bmod p\mathbb{Z}$ ein Erzeuger der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist, nennt man ***Primitivwurzel modulo n***. Primitivwurzeln gibt es nicht immer (z.B. $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2 \ncong C_4$ ist nicht zyklisch). Korollar 6.22 klassifiziert die n für welche es Primitivwurzeln gibt.

Gemäß Satz 6.21 (bzw. Korollar 7.8) ist $(\mathbb{Z}/p\mathbb{Z})^\times$ für jede Primzahl zyklisch. Wir beschränken uns im Folgenden der Einfachheit halber auf Primzahlen p. Da $g \bmod p\mathbb{Z}$ offenbar genau dann $(\mathbb{Z}/p\mathbb{Z})^\times$ erzeugt, wenn g nicht durch p teilbar ist und $g \bmod p\mathbb{Z}$ in keiner echten Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$ enthalten ist, kann man die Frage nach der Verteilung von Primitivwurzeln auch als eine Frage nach der Lage von Urbildern von echten Untergruppen von $(\mathbb{Z}/p\mathbb{Z})^\times$ unter der Projektion $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ deuten.

Eine berühmte ***Vermutung von Emil Artin***, auch als ***Primitivwurzelvermutung*** bekannt, besagt, dass jede ganze Zahl $g \in \mathbb{Z} \setminus (\{-1\} \cup \{n^2 : n \in \mathbb{Z}\})$ Primitivwurzel modulo unendlich vieler Primzahlen ist. (Eine schärfere Form dieser Vermutung besagt sogar, dass die Primzahlen, für welche g eine Primitivwurzel ist, in der Menge der Primzahlen eine asymptotische Dichte besitzen; g ist also mutmaßlich nicht zu selten eine Primitivwurzel modulo einer „zufällig“ gewählten Primzahl.) Im Jahr 1967 gelang es Christopher Hooley [27], die Primitivwurzelvermutung unter Annahme einer gewissen Verallgemeinerung der berühmten Riemannschen Vermutung (in einer quantitativen Form) zu beweisen. Dennoch ist bis heute noch für *keine einzige* Zahl g bekannt, dass diese Primitivwurzel modulo unendlich vieler Primzahlen ist. Im Jahr 1984 bewiesen Rajiv Gupta und Ram Murty [21], das folgende Ergebnis:

Satz (Gupta & Murty; 1984). *Für je drei verschiedene Primzahlen q, r, s gibt es unter den* 13 *Zahlen*

$$qs^2,\ q^3r^2,\ q^2r,\ r^3s^2,\ r^2s,\ q^2s^3,\ qr^3,\ q^3rs^2,\ rs^3,\ q^2r^3s,\ q^3s,\ qr^2s^3,\ qrs$$

mindestens eine, — nennen wir sie g, — sodass es für eine geeignet kleine Konstante $\delta_g > 0$ und alle $x \geq 3$ stets mindestens

$$\delta_g \frac{x}{(\log x)^2}$$

Primzahlen $p \leq x$ gibt, für welche g eine Primitivwurzel ist.

Die Anzahl der Primzahlen $p \leq x$ ist gemäß des berühmten ***Primzahlsatzes*** asymptotisch zu $x/\log x$. Demnach liefert das Ergebnis von Gupta und Murty zwar keine Beispiele für die Gültigkeit der Primitivwurzelvermutung in ihrer quantitativen Form, zeigt aber dennoch, dass die Primitivwurzelvermutung für unendlich viele

Zahlen in ihrer qualitativen Form zutrifft. Das Ergebnis von Gupta und Murty wurde von D. R. Heath-Brown verschärft [24].

Ein anderer sehr klassischer Forschungsgegenstand ist die Verteilung von Primitivwurzeln. Diesbezüglich spannende Fragen lauten beispielsweise: „*Wie groß ist die kleinste Primitivwurzel modulo einer Primzahl p?*“ Diese und verwandte Themen sind Untersuchungsgegenstand der (analytischen) Zahlentheorie. Interessierte Leserinnen und Leser seien an dieser Stelle an einschlägige Lehrveranstaltungen im Master-Studium verwiesen. (Als zusätzliche Lektüre sei das schöne Buch von Montgomery und Vaughan [38] empfohlen. Einen mehr algebraischen Blickwinkel findet man bei Ireland und Rosen [28].)

KAPITEL 7

Polynome

In diesem Kapitel beschäftigen wir uns damit, wie man zu einem kommutativen Ring R „möglichst allgemein“ ein Element X hinzunehmen kann, um somit einen größeren Ring $R[X]$ zu erhalten. Dies möglichst allgemein zu tun hat, wie wir noch sehen werden, wichtige Anwendungen und erlaubt in Kombination mit Faktorbildung die Konstruktion weiterer Ringe in denen es diverse Elemente mit gewünschten Eigenschaften gibt. In der *Algebra*-Vorlesung wird sich gerade dieser Blickwinkel noch als ubiquitär erweisen und so beispielsweise die Grundlage für die Konstruktion sogenannter algebraischer Abschlüsse bilden (das sind besonders große Körper in denen die algebraische Theorie erst richtig aufblühen kann). In § 7.3 geben wir einen Vorgeschmack auf die soeben geschilderte Methodik, indem wir sogenannte *Lokalisierungen* mittels Polynomringen konstruieren. (Diese Konstruktion verallgemeinert den Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$ und ist ein fundamentales Hilfsmittel in der kommutativen Algebra und algebraischen Geometrie.)

7.1. Konstruktion

Polynome sind bereits aus der Schule bekannt; X^5 ist ein Polynom, $33X^{12}-8X+\frac{11}{2}$ auch und für einen beliebigen Ring R kann man Polynome mit Koeffizienten aus R betrachten. Diese sind das, was man sich naiv unter diesen vorstellt, verhalten sich aber trotzdem (bedingt durch etwaig ungewohnte Arithmetik in R) ggf. etwas merkwürdig; so ist z.B. das Quadrat des Polynoms $(2+4\mathbb{Z})X$ in $(\mathbb{Z}/4\mathbb{Z})[X]$ das Nullpolynom.

7.1.1. Konstruktion im univariaten Fall. Es sei R ein beliebiger *kommutativer*[1] Ring. Die Menge

$$R[\mathbb{N}_0] := \{\text{Abbildungen } f\colon \mathbb{N}_0 \to R \text{ mit } f(i) = 0_R \text{ für fast alle } i\}$$

bildet mit punktweise definierter Addition eine abelsche Gruppe. Man definiert nun eine Multiplikation durch

$$f \cdot g := \left(i \mapsto \sum_{\substack{a,b\in\mathbb{N}_0\\ a+b=i}} \sum f(a)g(b)\right) = \left(i \mapsto \sum_{a=0}^{i} f(a)g(i-a)\right) \tag{7.1}$$

[1]Polynome kann man auch über nicht-kommutativen Ringen betrachten, dort spielen diese allerdings keine so essentielle Rolle, da die in § 7.2 definierte Auswertungsabbildung dann i.Allg. kein Homomorphismus zu sein braucht.

Dann bildet $R[\mathbb{N}_0]$ zusammen mit den eben definierten Verknüpfungen einen kommutativen Ring, wie man leicht (wenngleich mühsam) nachrechnet und die Abbildung

$$\iota\colon R \to R[\mathbb{N}_0], \quad r \mapsto \begin{cases} \mathbb{N}_0 \to R, \\ \quad i \mapsto \begin{cases} r & \text{falls } i = 0, \\ 0_R & \text{sonst,} \end{cases} \end{cases}$$

ist ein injektiver Ringhomomorphismus.

Es bezeichne $X \in R[\mathbb{N}_0]$ die Abbildung $X\colon \mathbb{N}_0 \to R$ mit

$$X(i) = \begin{cases} 0_R & \text{falls } i = 0, \\ 1_R & \text{falls } i = 1, \\ 0_R & \text{falls } i \geq 2. \end{cases}$$

Für $n \in \mathbb{N}_0$ ist $X^n = X \cdot \ldots \cdot X$ (n mal via (7.1)) die Abbildung $\mathbb{N}_0 \to R$ mit $X^n(n) = 1_R$ und $X^n(i) = 0_R$ für $i \neq n$. Dementsprechend schreibt sich jedes Element $f \in R[\mathbb{N}_0]$ in der Form

$$f = \sum_{i \in \mathbb{N}_0} \iota(f(i)) X^i, \tag{7.2}$$

wobei in der Summe rechter Hand nur höchstens endlich viele Terme von 0_R verschieden sind.

Wir identifizieren im Folgenden zumeist R mit $\iota(R) \subset R[\mathbb{N}_0]$ und bezeichnen ι als die ***kanonische Einbettung***. Kommt in Diagrammen ein unbeschrifteter Pfeil $R \to R[X]$ vor, so ist mit diesem stets ι gemeint. Falls wir für ein Element $r \in R$ speziell darauf hinweisen möchten, dass wir dieses als Element von $R[\mathbb{N}_0]$ auffassen, schreiben wir hingegen doch rX^0. Man beachte insbesondere

$$1_{R[X]} = X^0 = 1_R X^0 = \iota(1_R) = 1_R,$$

wobei die *letzte Gleichheit* unserer Konvention zur Identifikation von R mit $\iota(R)$ folgt. Der kleinste Teilring von $R[\mathbb{N}_0]$, der R (gemeint ist $\iota(R)$) und X enthält, ist wegen (7.2) gerade $R[\mathbb{N}_0]$ selbst. Wir schreiben darum $R[X]$ statt $R[\mathbb{N}_0]$ und nennen $R[X]$ den ***Polynomring über R in der Variablen X***.

Für diverse Anwendungen braucht man auch Polynomringe in mehreren (ja sogar potentiell überabzählbar vielen) Variablen. Die Konstruktion dieser Ringe verläuft quasi völlig analog zur Konstruktion des Polynomringes in nur einer Variablen, leidet aber darunter, auf den ersten Blick sehr kompliziert auszusehen. Die Details hierzu werden in Aufgabe T11.2 besprochen.

Bemerkung. Die hier benutzte Notation $R[X]$ für $R[\mathbb{N}_0]$ passt zur generell üblichen Notation, dass für einen Ringhomomorphismus $\alpha\colon R \to A$ und ein Element $a \in A$ der Ausdruck $R[a]$ den kleinsten Teilring von A bezeichnet, der $\alpha(R) \cup \{a\}$ enthält. Man beachte, dass der benutzte Ringhomomorphismus in dieser Notation nicht gesondert erwähnt wird und aus dem Kontext heraus verstanden werden muss. (Beispiel: $\mathbb{Z}[\mathrm{i}]$ via $\alpha = \mathrm{id}_{\mathbb{C}}|_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{C}$; $R[\mathbb{N}_0] = R[X]$ via α gewählt als die kanonische Einbettung

$\iota\colon R \to R[\mathbb{N}_0]$.) Generell benutzen wir Großbuchstaben für Variablen, etwa X, Y, Z, X_1, X_2 etc.

7.1.2. Exkurs: Monoidringe. Die oben benutzte Konstruktion von $R[\mathbb{N}_0]$ ist ein Spezialfall der Konstruktion des sogenannten ***Monoidrings*** $R[M]$ für ein Monoid M (salopp: eine Gruppe ohne die Forderung, dass inverse Elemente existieren müssen). Hierbei möchte man zu einem Ring $(R, +, \cdot)$ die Elemente eines Monoids $(M, \circ)$ hinzufügen und immer noch einen Ring $(R[M], \oplus, \odot)$ erhalten, wobei sich die von M kommenden Elemente von M so multiplizieren sollen, wie sie das schon in M tun: für $m, n \in R[M] \cap M$ sollte $m \odot n = m \circ n$ gelten. Es wirkt natürlich so, dass das neutrale Element 1_M von M auch neutral auf allen Elementen von $R[M]$ (bezüglich $\odot$) wirken sollte. Selbiges sollte für das multiplikativ neutrale Element 1_R von R gelten. Dann folgt natürlich schon formal $1_R = 1_M$ in $R[M]$.[2] Wenn man zusätzlich noch fordert, dass die Elemente von M in $R[M]$ mit den Elementen von R in $R[M]$ kommutieren, so erhält man für $r, r' \in R \cap R[M]$ und $m, m' \in R[M] \cap M$

$$(r \odot m) \odot (r' \odot m') = (r \odot r') \odot (m \odot m') = (r \cdot r') \odot (m \circ m').$$

Schreibt man nun die Elemente von $m \in \mathbb{N}_0$ formal als Potenzen X^m einer „Variablen“ X, so erhält man mit $X^m \cdot X^n = X^{m+n}$ genau die zuvor festgelegten Rechenregeln für Polynome.

7.1.2.1. *Laurentpolynome.* Das Monoid $(\mathbb{N}_0, +)$ wird von einem Element erzeugt, nämlich von 1. Die ganzen Zahlen $\mathbb{Z}$ mit Addition werden als Gruppe ebenfalls von einem Element erzeugt, als Monoid aufgefasst braucht man jedoch zwei Erzeuger, beispielsweise -1 und 1, da Inversion beim Erzeugen nicht mehr zur Verfügung steht. (Randbemerkung: -1 und 42 bilden beispielsweise auch ein Erzeugendensystem für das Monoid $(\mathbb{Z}, +)$.) Der Monoidring $R[\mathbb{Z}]$ heißt ***Ring der Laurentpolynome über R*** und besteht aus „Polynomen“ (sogenannten ***Laurentpolynomen***), bei denen auch negative Exponenten zulässig sind; z.B.

$$13X^8 - 4X + 12X^0 + X^{-17} - 42X^{-100} \in \mathbb{Z}[\mathbb{Z}] \quad \text{(Monoidring!)}.$$

Das Element $X \in R[\mathbb{Z}]$ sei analog wie bei $R[\mathbb{N}_0]$ definiert. Dieses ist dann invertierbar mit inversem Element X^{-1}, welches (gemäß der Konstruktion) aufgefasst als Funktion $X^{-1}\colon \mathbb{Z} \to R$ überall 0_R liefert, bis auf an der Stelle -1, wo 1_R geliefert wird. Als Pendant dazu, dass -1 und 1 die ganzen Zahlen als Monoid erzeugen, erzeugen X und X^{-1} den Monoidring $R[\mathbb{Z}]$; der kleinste Teilring von $R[\mathbb{Z}]$, welcher R (eingebettet bezüglich der kanonischen Einbettung), X und X^{-1} enthält, wird mit $R[X, X^{-1}]$ notiert. Wir haben dann also $R[X, X^{-1}] = R[\mathbb{Z}]$.

[2] Formal soll „$1_R = 1_M$ in $R[M]$“ natürlich bedeuten, dass die Bilder von 1_R und 1_M unter den Inklusionen $R \hookrightarrow R[M] \hookleftarrow M$ übereinstimmen.

7.1.2.2. *Dirichlet-Polynome.* Auch $(\mathbb{N}, \cdot)$ ist ein Monoid. Mittels eindeutigen Primfaktorzerlegung in $\mathbb{N}$ schließen wir, dass $\mathbb{N}$ als Monoid von den Primzahlen

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

erzeugt wird. Wir schreiben n^{-s} für das Element vom $R[\mathbb{N}]$ Monoidring, welches als Funktion von $\mathbb{N} \to R$ überall 0_R liefert, bis auf an der Stelle n, wo es 1_R liefert. Der Exponent „$-s$“ ist an dieser Stelle nur eine formale Schreibweise. Man beachte allerdings, dass sich zwei Elemente n^{-s} und m^{-s} genau wie bei den üblichen Potenzrechenregeln multiplizieren: $n^{-s}m^{-s} = (nm)^{-s}$. Die Elemente von $R[\mathbb{N}]$ sind sogenannte ***Dirichlet-Polynome***. Diese und ihre Erweiterungen zu ***Dirichlet-Reihen*** spielen eine fundamentale Rolle in der *analytischen Zahlentheorie*; dort wird das s im Exponent als Variable in der komplexen Zahlenebene aufgefasst. Dabei spielen Dirichlet-Reihen dann die Rolle einer Art „erzeugenden Funktion“ für Zahlenfolgen mit „multiplikativer Struktur“, genau wie Potenzreihen oft als erzeugenden Funktionen für Zahlenfolgen mit „additiver Struktur“ dienen:

- $(a_0, a_1, a_2, \ldots) \longmapsto \sum_{k=0}^{\infty} a_k X^k,$ (Potenzreihen,)
- $(b_1, b_2, b_3, \ldots) \longmapsto \sum_{n=1}^{\infty} b_n n^{-s},$ (Dirichlet-Reihen.)

Algebraische/arithmetische Eigenschaften der benutzten Folgen schlagen sich dann zumeist in gutartigen analytischen Eigenschaften der zugeordneten erzeugenden Funktionen nieder. Umgekehrt lassen sich dann in günstigen Fällen Rückschlüsse über algebraische oder arithmetische Eigenschaften der Folgen anhand von analytischen Untersuchungen der erzeugenden Funktionen ziehen. Beispielsweise gilt

$$(1, 1, 1, \ldots) \longmapsto \sum_{k=0}^{\infty} X^k = \frac{1}{1-X}, \quad \text{(geometrische Reihe!)}$$

und für die ***Fibonacci-Folge*** $(F_k)_k$ ist

$$(0, 1, 1, 2, 3, 5, 8, \ldots, \underbrace{F_{k-1}, F_k, \overbrace{F_{k-1} + F_k}^{\text{Index } k+1}}_{\text{(Rekursives Bildungsgesetz für } k \geq 1)}, \ldots) \longmapsto \sum_{k=0}^{\infty} F_k X^k = \frac{X}{1-X-X^2},$$

wobei man die letzte Gleichung durch Anwendung des rekursiven Bildungsgesetzes und einige algebraische Manipulationen gewinnen kann. Durch eine Partialbruchzerlegung von $X/(1-X-X^2)$, Expansion in geometrische Reihen und anschließenden Koeffizientenvergleich kann man dann beispielsweise die bekannte ***Faulhaber-Formel*** für Fibonacci-Zahlen herleiten. Im Bezug auf Dirichlet-Reihen hat man die Zuordnung

$$(1, 1, 1, \ldots) \longmapsto \sum_{n=1}^{\infty} n^{-s}$$

und dies liefert für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$ den Wert $\zeta(s)$ der ***Riemannschen Zetafunktion*** bei s. In ihr liegen die tiefsten Geheimnisse der Arithmetik vergraben. Für mehr Hintergrund konsultiere man [29].

7.1.3. Arithmetik in Polynomringen. Die Elemente f von $R[X]$ nennt man ***Polynome (über R)*** oder ***Polynome mit Koeffizienten aus R***. Die Werte $f(i) \in R$ heißen ***Koeffizienten von f***. Diese notieren wir oft auch in der Form a_i oder mit Varianten davon. Die Zahl

$$\deg f := \sup\{ i \in \mathbb{N}_0 : f(i) \neq 0_R \} \in \mathbb{N}_0 \cup \{-\infty\}$$

heißt ***Grad von f***. Das einzige Polynom mit Grad $-\infty$ ist das ***Nullpolynom*** $0_{R[X]} = 0_R X^0$. Die Menge der Polynome in $R[X]$ mit Grad 0 ist genau $\iota(R) \setminus \{0_{R[X]}\}$. Die Polynome $\iota(R)$ heißen ***konstante Polynome***. Der Koeffizient $f(\deg f)$ heißt ***Leitkoeffizient von f***.

Beispiel. Ein typisches Beispiel für ein Polynom aus $\mathbb{Z}[X]$ ist $123 + X - X^5 + 18X^{42}$. Dieses hat Grad 42 und der erste Term bezeichnet eigentlich das Polynom $123X^0 \in \mathbb{Z}[X]$.

Aus den Definitionen von Addition und Multiplikation in $R[X]$ (siehe (7.1)) entnimmt man unmittelbar das folgende Ergebnis:

Lemma 7.1 (Grad-Ungleichungen)**.** *Es sei R ein beliebiger kommutativer Ring und $f, g \in R[X]$ seien Polynome. Dann gilt:*

(1) $\deg(f+g) \leq \max\{\deg f, \deg g\}$*;*
(2) $\deg(f \cdot g) \leq \deg f + \deg g$*;*
(3) $\deg(f \cdot g) = \deg f + \deg g$ *falls der Leitkoeffizient von f oder g kein Nullteiler ist. (Siehe unten für die Definition von „Nullteiler“.)*

Es sei R ein kommutativer Ring. Ein Element $a \in R$ heißt ***Nullteiler***, wenn es ein $b \in R \setminus \{0_R\}$ mit $0_R = a \cdot b$ gibt. Für jeden kommutativen Ring R, ungleich dem Nullring, ist $a = 0_R$ ein Nullteiler, aber i.Allg. kann es in R weitere Nullteiler geben, z.B. 2 mod 4 in $\mathbb{Z}/4\mathbb{Z}$:

$$(2 \bmod 4)^2 = (4 \bmod 4) = (0 \bmod 4) = 0_{\mathbb{Z}/4\mathbb{Z}}. \tag{7.3}$$

Elemente $a \in R$ mit $a^k = 0_R$ für ein $k \in \mathbb{N}$ nennt man auch ***nilpotent***. Im Allgemeinen ist nicht jeder Nullteiler nilpotent (z.B. 2 mod 6 in $\mathbb{Z}/6\mathbb{Z}$). Ist R nicht der Nullring und hat außer 0_R keine weiteren Nullteiler, so nennt man R einen ***Integritätsbereich***.

Beispiel. Jeder Körper K ist ein Integritätsbereich, da für einen solchen $K \setminus \{0_K\}$ ja eine Gruppe mit der eingeschränkten Multiplikation bildet und insbesondere für kein $a \in K \setminus \{0_K\}$ das Produkt mit einem $b \in K \setminus \{0_K\}$ den Wert $0_K \notin K \setminus \{0_K\}$ annehmen kann. Jeder Teilring eines Integritätsbereichs ist auch ein Integritätsbereich. Insbesondere ist $\mathbb{Z} \subset \mathbb{Q}$ ein Integritätsbereich.

Liest man (7.3) als Gleichung von konstanten Polynomen, so sieht man, dass in Lemma 7.1 (2) i.Allg. keine Gleichheit zu gelten braucht. Über Integritätsbereichen sieht dies besser aus.

Proposition 7.2. *Es sei R ein Integritätsbereich und $f, g \in R[X]$ seien Polynome. Dann gelten die folgenden Aussagen:*

*(1) (**Gradformel**:)* $\deg(f \cdot g) = \deg f + \deg g$.[3]

(2) $R[X]$ ist ein Integritätsbereich und für die Einheitengruppe gilt $(R[X])^\times = R^\times$.[4]

*(3) (**Division mit Rest**:) Ist $g \neq 0_{R[X]}$ und der Leitkoeffizient von g eine Einheit, so gibt es Polynome $q, r \in R[X]$ mit $f = qg + r$ und $\deg r < \deg g$. Die Polynome q und r sind durch diese Eigenschaften eindeutig bestimmt.*

Beweis. Die erste Aussage folgt offensichtlich aus den Definitionen und Lemma 7.1. Die zweite Aussage folgt aus der ersten, da der Grad des Produktes zweier Polynome $f, g \neq 0_{R[X]}$ jedenfalls größer als $-\infty$ ist und somit $f \cdot g \neq 0_{R[X]}$ gilt. Die letzte Aussage beweist man mit Induktion über den Grad. Für $\deg f < \deg g$ kann man einfach $q = 0_{R[X]}$ und $r = f$ wählen. Für den Induktionsschritt sei nun $\deg f \geq \deg g$. Es sei a der Leitkoeffizient von f und b der Leitkoeffizient von g. Dann erkennt man durch einen Vergleich von Leitkoeffizienten, dass $f - ab^{-1}X^{\deg f - \deg g}g$ kleineren Grad als f hat. Mittels Induktionsvoraussetzung findet man also $q', r' \in R[X]$ mit

$$f - ab^{-1}X^{\deg f - \deg g}g = q'g + r'$$

und $\deg r' < \deg g$. Umstellen liefert die behauptete Gleichung. Zum Beweis der *Eindeutigkeit* von q und r gelte $f = qg + r$ und $f = \tilde{q}g + \tilde{r}$ mit $\deg r, \deg \tilde{r} < \deg g$. Subtraktion beider Gleichungen und anschließendes Umstellen liefert

$$\tilde{r} - r = (q - \tilde{q})g. \tag{7.4}$$

Das Polynom auf der rechten Seite hat Grad $\leq \max\{\deg \tilde{r}, \deg r\} < \deg g$ wegen Lemma 7.1 (1). Wegen (1) hat die rechte Seite allerdings Grad $\deg(q - \tilde{q}) + \deg g$. Das ist nur dann nicht widersprüchlich, wenn $\deg(q - \tilde{q}) = -\infty$ und also $q - \tilde{q} = 0_{R[X]}$ gilt. In jenem Fall folgt dann aber $q = \tilde{q}$ und anschließend (via (7.4)) $r = \tilde{r}$. □

Beispiel 7.3 (Polynomdivision)**.** Der Beweis von Proposition 7.2 (3) liefert einen Algorithmus zur Bestimmung von q und r. Wir betrachten dies für $R = \mathbb{Z}$ anhand der Polynome $f = 3X^4 + 4X^3 - 5X^2 - 2$ und $g = X^2 - 2$. Dann hat

$$f_1 := f - 3X^2 g = 4X^3 + X^2 - 2$$

einen kleineren Grad als f. Gleichsam hat

$$f_2 := f_1 - 4X g = X^2 + 8X - 2$$

[3] Wegen $0_{R[X]} \cdot g = 0_{R[X]} = g \cdot 0_{R[X]}$ gilt diese auch, wenn einer der Summanden $-\infty$ ist, wobei diese dann als „$(-\infty) + n := -\infty =: n + (-\infty)$“ zu lesen ist.

[4] Mit $R^\times$ ist an dieser Stelle streng genommen $\iota(R^\times)$ gemeint.

einen kleineren Grad als f_1 und

$$r := f_2 - 1X^0 g = 8X$$

hat einen kleineren Grad als f_2, ja sogar einen kleineren Grad als g. Wir haben

$$8X = r = f - 3X^2 g - 4Xg - 1X^0 g = f - (3X^2 - 4X - 1)g.$$

Man erinnere sich in diesem Kontext auch an die aus der Schule bekannte schriftliche Polynomdivision.

7.2. Universelle Eigenschaft und Einsetzungshomomorphismus

7.2.1. Universelle Eigenschaft. Die Bedeutung von Polynomringen für die Algebra gründet sich auf den folgenden fundamentalen Satz:

Satz 7.4 (Universelle Eigenschaft von $R \to R[X]$)**.** *Es sei R ein kommutativer Ring und $f\colon R \to S$ ein Ringhomomorphismus in einen beliebigen kommutativen Ring S. Ferner sei $x \in S$ gegeben. Dann gibt es genau einen Ringhomomorphismus $\varepsilon_x\colon R[X] \to S$ mit $\varepsilon_x(X) = x$, der das folgende Diagramm kommutativ macht:*

$$\begin{array}{ccc} R[X] & \overset{\exists!\,\varepsilon_x}{\underset{X\mapsto x}{\dashrightarrow}} & S\,. \\ \uparrow & \nearrow_{f} & \\ R & & \end{array}$$

Hierbei wird ein beliebiges Polynom $\sum_i a_i X^i$ von ε_x auf $\sum_i f(a_i)x^i$ abgebildet.

Beweis. Angenommen es gibt einen Ringhomomorphismus ε_x, der das obige Diagramm kommutativ macht und X auf x abbildet. Dann folgt $\varepsilon_x(\sum_i a_i X^i) = \sum_i f(a_i)x^i$ und somit ist ε_x bereits eindeutig bestimmt. Dies legt nahe, zum Beweis der Existenz von ε_x einfach $\varepsilon_x(\sum_i a_i X^i) := \sum_i f(a_i)x^i$ zu *definieren*. Dann gilt offensichtlich

- $\varepsilon_x(X) = \varepsilon_x(1_R X^1) = f(1_R)x = x$, sowie $(X \mapsto x)$
- $\varepsilon_x(1_{R[X]}) = \varepsilon_x(1_R X^0) = f(1_R) = 1_S$. $(1_{R[X]} \mapsto 1_S)$

Analog zeigt man

- $\varepsilon_x(g+h) = \varepsilon_x(g) + \varepsilon_x(h)$ und (Additivität)
- $\varepsilon_x(g \cdot h) = \varepsilon_x(g) \cdot \varepsilon_x(h)$ für alle $g, h \in R[X]$. (Multiplikativität)

Wir zeigen nur exemplarisch die letzte der beiden Eigenschaften. Für $g = \sum_i a_i X^i$ und $h = \sum_j b_i X^j$ ist nämlich

$$\varepsilon_x(gh) = \varepsilon_x\Big(\sum\nolimits_i \sum\nolimits_j a_i b_j X^{i+j}\Big) = \sum\nolimits_i \sum\nolimits_j f(a_i) f(b_j) x^{i+j}$$

Unter Ausnutzung der Kommutativität in S lassen sich x^i und $f(b_j)$ miteinander vertauschen. Damit kommt

$$\varepsilon_x(gh) = \sum\nolimits_i \sum\nolimits_j f(a_i)x^i f(b_j)x^j = \Big(\sum\nolimits_i f(a_i)x^i\Big)\Big(\sum\nolimits_j f(b_j)x^j\Big) = \varepsilon_x(g)\,\varepsilon_x(h). \quad \square$$

Satz 7.4 kann beispielsweise benutzt werden, um Oberringe S von R zu studieren (lässt sich aber auch allgemeiner anwenden):

Beispiel. Betrachtet man etwa den Ring

$$\mathbb{Z}[\mathrm{i}] = \{\, a + \mathrm{i}b \in \mathbb{C} : a, b \in \mathbb{Z} \,\} \subset \mathbb{C}$$

der ganzen Gaußschen Zahlen über $\mathbb{Z}$, so erhält man mit $f = \mathrm{id}_{\mathbb{Z}[\mathrm{i}]}|_{\mathbb{Z}}$ aus Satz 7.4 einen *surjektiven* Ringhomomorphismus $\varepsilon\colon \mathbb{Z}[X] \to \mathbb{Z}[\mathrm{i}]$, $X \mapsto \mathrm{i}$. Der erste Isomorphiesatz (Korollar 6.8) zeigt dann

$$\mathbb{Z}[\mathrm{i}] \cong \mathbb{Z}[X]/\ker\varepsilon.$$

Man kann $\ker\varepsilon = \langle X^2+1\rangle$ zeigen und erhält somit $\mathbb{Z}[\mathrm{i}] \cong \mathbb{Z}[X]/\langle X^2+1\rangle$. Dies erlaubt einem, das Studium von $\mathbb{Z}[\mathrm{i}]$ auf das Studium des Faktorrings $\mathbb{Z}[X]/\langle X^2+1\rangle$ zurückzuführen und dieser wiederum kann durch das Studium von $\mathbb{Z}[X]$ verstanden werden. Umgekehrt suggeriert dies auch eine Methode, wie man sich einen Oberring von $\mathbb{Z}$ mit einem Element i, welches $\mathrm{i}^2+1=0$ erfüllt, hätte *beschaffen* können, wenn man die komplexe Zahl i nicht schon zur Verfügung gehabt hätte: man betrachtet einfach $R = \mathbb{Z}[X]/\langle X^2+1\rangle$ und erkennt, dass $\ï := (X \bmod \langle X^2+1\rangle)$ die gewünschte Gleichung $\ï^2 + 1_R = 0_R$ erfüllt.

Bemerkung. Wir werden das im vorangegangenen Beispiel erläuterte Verfahren in der Vorlesung *Algebra* noch dafür benutzen, um zu einem gegebenem Polynom über einem Körper K einen Oberkörper von K zu konstruieren, in dem das gegebene Polynom eine Nullstelle besitzt.

7.2.2. Einsetzungshomomorphismus. Es sei $f\colon R \to S$ ein Homomorphismus zwischen kommutativen Ringen. Für jedes $x \in S$ bekommt man dann aus Satz 7.4 einen Ringhomomorphismus

$$\varepsilon_x\colon R[X] \xrightarrow{X\mapsto x} S, \quad \sum\nolimits_i a_i X^i \mapsto \sum\nolimits_i f(a_i)x^i, \tag{7.5}$$

den sogenannten ***Einsetzungshomomorphismus (bezügl. x)***. Die Abbildung

$$\varepsilon_\bullet\colon R[X] \to \mathrm{Abb}(S,S), \quad g \mapsto \begin{cases} S \to S, \\ x \mapsto g(x) := \varepsilon_x(g), \end{cases} \tag{7.6}$$

ordnet jedem Polynom $g \in R[X]$ die zugehörige ***Auswertungsabbildung*** (oder ***Polynomfunktion***) $g(\,\cdot\,)$ zu. Man beachte, dass der Bezug auf f hier nicht explizt in der Notation kenntlich gemacht wird und aus dem Kontext her erschlossen werden muss.

Bemerkung (Wichtige Notationsänderung)**.** Wir vergessen im Folgenden, dass Polynome $g \in R[X] = R[\mathbb{N}_0]$ formal als Abbildungen $g\colon \mathbb{N}_0 \to R$ konstruiert wurden und demnach die Auswertung $g(n)$ (mit $n \in \mathbb{N}_0$) die Koeffizienten von g liefert. Mit „$g(r)$“ ($r \in R$) verstehen wir (auch in Fällen wie $R = \mathbb{Z} \supset \mathbb{N}_0$) im Folgenden nur noch $\varepsilon_r(g)$. Für $g = 0X^0 + 7X^1 + 2X^2$ in $\mathbb{Z}[X]$ ist also

$$g(1) = 0\cdot 1^0 + 7\cdot 1 + 2\cdot 1^2 = 9 \neq 7 = \text{„Koeffizient von } g \text{ bei } X^1\text{“}.$$

Beispiele.

- Einsetzen von $4 \in \mathbb{Z}$ für X in $X^2 + 1 \in \mathbb{Z}[X]$ liefert $\varepsilon_4(X^2 + 1) = 4^2 + 1 = 17$. (Hier wurde implizit $f = \mathrm{id}_{\mathbb{Z}}$ in (7.5) angenommen.)
- Wählt man für f die kanonische Einbettung $\iota\colon R \to R[X]$, so kann man auch Polynome in Polynome einsetzen, z.B. $g(X^2)$. Man beachte: Einsetzen von X für X in g liefert wieder g. Bezüglich der eben eingeführten Notation ist also „$g(X) = g$“. Bei Ausdrücken wie $X(X + 1)$ ist hierbei Vorsicht geboten: ist X mal $X + 1$ gemeint, oder $X + 1$ im Polynom X eingesetzt (also $X + 1$)? Sofern nichts anderes gesagt wird, meinen wir in solchen Fällen stets das Produkt von Polynomen und nicht das Einsetzen.

Bemerkung. Für einen Ringhomomorphismus $f\colon R \to S$ zwischen kommutativen Ringen erhält man durch Verkettung mit der kanonischen Inklusion $S \to S[X]$ einen Ringhomomorphismus $R \to S[X]$. Den zugehörigen Einsetzungshomomorphismus der $X \in S[X]$ für $X \in R[X]$ einsetzt, nennen wir f^*; dieser macht das folgende Diagramm kommutativ:

$$\begin{array}{ccc} R[X] & \xrightarrow[X \mapsto X]{f^*} & S[X] \\ \uparrow & & \uparrow \\ R & \xrightarrow{f} & S\,. \end{array}$$

Für jedes $x \in S$ kommutiert das Diagramm

$$\begin{array}{ccccc} R[X] & \xrightarrow[X \mapsto X]{f^*} & S[X] & & \\ \uparrow & & \uparrow & \searrow^{X \mapsto x} & \\ R & \xrightarrow{f} & S & \xrightarrow{\mathrm{id}_S} & S\,. \end{array}$$

Demnach und zusammen mit der Eindeutigkeitsaussage in Satz 7.4 sieht man[5] $g(x) = (f^*g)(x)$, wobei die linke Seite das Auswerten eines Polynoms $g \in R[X]$ bezeichnet und die rechte Seite das Auswerten des Polynoms $f^*g \in S[X]$. Die Notation f^*g wird später in der Vorlesung „Algebra“ wichtig sein, um darüber Buch zu führen, wo gewisse Polynome „leben“, da dies Einfluss auf deren Eigenschaften hat. Für den Moment soll die Analogie reichen, dass $2 \in \mathbb{Z}$ keine Einheit ist, $2 \in \mathbb{Q}$ allerdings schon. Arbeitet man mit Einheiten, $\mathbb{Z}$ und $\mathbb{Q}$ gleichzeitig, so ist es daher nötig, genau zu spezifizieren, in welchem Ring die jeweiligen Elemente betrachtet werden.

Man sollte streng zwischen dem *Polynom* g und der *Polynomfunktion* $\varepsilon_\bullet(g)\colon R \to R$ unterscheiden:

Beispiel (Polynome $\neq$ Polynomfunktionen)**.** Über dem Körper $\mathbb{F}_2$ handelt es sich bei der dem Polynom $g = (X - 1_{\mathbb{F}_2})X \in \mathbb{F}_2[X]$ zugeordneten Polynomfunktion $\varepsilon_\bullet(g)$ um die Nullfunktion $\mathbb{F}_2 \to \mathbb{F}_2$, $x \mapsto 0_{\mathbb{F}_2}$. Selbstverständlich wird die Nullfunktion auch

[5] Benutze, dass die Verkettung von $f^*\colon R[X] \to S[X]$ mit $S[X] \to S$ (mit $S[X] \ni X \mapsto x \in S$) ein Ringhomomorphismus $R[X] \to S$ mit $X \to x$ ist, der ein entsprechendes Diagramm wie in Satz 7.4 kommutativ macht.

dem Nullpolynom $0_{\mathbb{F}_2[X]}$ zugeordnet. Die in (7.6) definierte Auswertungsabbildung $\varepsilon_\bullet\colon \mathbb{F}_2[X] \to \mathrm{Abb}(\mathbb{F}_2, \mathbb{F}_2)$ ist also nicht injektiv. Analoge Beispiele lassen sich für jeden endlichen (kommutativen) Ring $R \neq \mathbf{0}$ konstruieren. Hierfür ersetze man g schlichtweg durch das Polynom $\prod_{r\in R}(X-r) \in R[X]$. Dieses ist monisch und also nicht das Nullpolynom. Allerdings wertet es sich bei jedem $r \in R$ zu 0_R aus.

7.2.3. Nullstellen. Wir behalten die Notation aus § 7.2.2 bei. Sei $x \in S$ und $g(x) := \epsilon_x(g)$ die Auswertung des Polynoms $g \in R[X]$ bei x im Sinne von § 7.2.2 (siehe (7.5)). Das Element $x \in S$ nennt man ***Nullstelle von g (in S)***, wenn $g(x) = 0_S$ gilt.[6] Die ***Nullstellen von g*** sind die $x \in R$ mit $g(x) = 0_R$ (hierbei ist implizit $f = \mathrm{id}_R$ in (7.5) zu verstehen).

Lemma 7.5 (Abspalten von Linearfaktoren)**.** *Es sei R ein kommutativer Ring und $p \in R[X]$. Ist $x_0 \in R$ eine Nullstelle von p, so existiert ein $q \in R[X]$ mit $p = (X - x_0) \cdot q$.*

Beweis. Es sei $x_0 \in R$ eine Nullstelle von p. Proposition 7.2 (3) liefert $q, r \in R[X]$ mit $p = (X - x_0)q + r$ und $\deg(r) < \deg(X - x_0) = 1$. Einsetzen von x_0 zeigt dann aber

$$0_R = p(x_0) = (x_0 - x_0)q(x_0) + r(x_0) = 0_R q(x_0) + r(x_0) = r(x_0).$$

Also hat r eine Nullstelle bei x_0. Das ist wegen $\deg(r) < 1$ aber nur möglich, wenn r das Nullpolynom ist. Also ist $p = (X - x_0) \cdot q$, wie gewünscht. □

Proposition 7.6 (Nullstellenanzahlabschätzung)**.** *Ist R ein Integritätsbereich, so hat jedes Polynom $p \in R[X] \setminus \{0_{R[X]}\}$ höchstens* $\deg p$ *Nullstellen in R.*

Beweis. Man führt eine Induktion über $\deg p$. Für $\deg p = 0$ gilt die Behauptung trivialerweise. Ist nun $\deg p \geq 1$ und x_0 eine Nullstelle von p. Dann schreibt sich p gemäß Lemma 7.5 als $p = (X - x_0) \cdot q$ mit einem Polynom $q \in R[X]$ mit kleinerem Grad als der von p (genauer: sogar $\deg q = (\deg p) - 1$ wegen der Gradformel). Wegen Nullteilerfreiheit kann $x \in R$ nur dann eine Nullstelle von p sein, wenn $x - x_0 = 0_R$ oder $q(x) = 0_R$ gilt. Die erste Gleichung wird nur von x erfüllt und q hat nach Induktionsvoraussetzung höchstens $(\deg p) - 1$ Nullstellen. □

Bemerkungen.

(1) Ist R kein Integritätsbereich, so kann es Polynome $p \in R[X]$ mit mehr Nullstellen als $\deg p$ geben. Man betrachte etwa das Polynom $(2 + 4\mathbb{Z})X$ über $R = \mathbb{Z}/4\mathbb{Z}$. Dessen Nullstellen sind $0 + 4\mathbb{Z}$ und $2 + 4\mathbb{Z}$.
(2) Das Polynom $X^2 + 1 \in \mathbb{R}[X]$ besitzt keine Nullstellen in $\mathbb{R}$, denn für jede reelle Zahl x ist $x^2 \geq 0$ und also $x^2 + 1 > 0$. Ein Polynom *kann* also durchaus *weniger* Nullstellen besitzen, als sein Grad angibt.
(3) Das Polynom $X^2 + 1 = (X + \mathrm{i})(X - \mathrm{i}) \in \mathbb{C}[X]$ besitzt genau zwei Nullstellen in $\mathbb{C}$.

[6] Man beachte, dass das Auswerten eines Polynoms $f \in R[X]$ bei $s \in S$ erst durch das Vorhandensein eines Ringhomomorphismus $R \to S$ ermöglicht wird.

Korollar 7.7. *Es sei R ein Integritätsbereich. Dann ist jede endliche Untergruppe G von $R^\times$ zyklisch. Insbesondere ist die multiplikative Gruppe jedes endlichen Körpers zyklisch.*

Beweis. Da R kommutativ ist, ist $R^\times$ und damit auch jede endliche Untergruppe $G \leq R^\times$ abelsch. Wäre G *nicht* zyklisch, so wäre $G \cong C_{p^n} \times C_{p^m} \times \ldots$ gemäß Satz 5.3 mit Primzahlpotenzen p^n und p^m *derselben* Primzahl p. Sowohl C_{p^n} wie auch C_{p^m} besitzen eine zu C_p isomorphe Untergruppe. Demnach besitzt G eine zu $C_p \times C_p$ isomorphe Untergruppe U. Jedes Element u von U hat allerdings Ordnung 1 oder p; in jedem Fall ist $u^p = 1_G = 1_R$ und wir sehen, dass das Polynom $X^p - 1_R \in R[X]$ mindestens $\#U = p^2$ Nullstellen hat, im Widerspruch zu Proposition 7.6. (Dieses Argument ist auch schon aus Aufgabe 8.3 bekannt und tatsächlich hätten wir uns beim Beweis auch direkt auf jene Aufgabe berufen können.) □

Nun lässt sich auch der letzte noch fehlende Teil für den *Beweis des Satzes von Gauß*, Satz 6.21, nachholen:

Korollar 7.8. *Für jede Primzahl p ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch.*

Beweis. Bei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ handelt es sich gemäß Beispiel 6.11 um einen Körper und die Aussage folgt aus Korollar 7.7. □

7.3. Lokalisierung

Bei $\mathbb{Z}$ handelt es sich um einen Teilring von $\mathbb{Q}$. In $\mathbb{Z}$ ist 2 keine Einheit, denn es gibt kein $n \in \mathbb{Z}$ mit $2n = 1$, aber in $\mathbb{Q}$ gibt es doch so ein n, nämlich $n = 1/2 \in \mathbb{Q} \setminus \mathbb{Z}$. Wir können auch den kleinsten Teilring $\mathbb{Z}[1/2]$ von $\mathbb{Q}$ betrachten, der $\mathbb{Z}$ als Teilring enthält und das Element $1/2$ enthält. Man kann sich überlegen, dass dieser Ring genau die Brüche $a/2^j \in \mathbb{Q}$ mit $a \in \mathbb{Z}$ und $j \in \mathbb{N}_0$ enthält.

Wir widmen uns nun der Aufgabe, zu einem gegebenen *kommutativen* Ring R einen größeren Ring R' zu konstruieren, der R als Teilring enthält und in dem gewisse Elemente von R nun Einheiten sind. Tatsächlich ist es technisch günstig, einen Ring R' nebst Ringhomomorphismus $f : R \to R'$ zu konstruieren, sodass $f(s) \in R'$ für alle zu invertierenden Elemente $s \in R$ eine Einheit in R' ist. Anschließend kann man gewillt sein, R mit dem Bild $f(R) \subseteq R'$ zu identifizieren. Für den letzten Schritt ist es streng genommen wichtig, Injektivität von f zu gewährleisten, doch auch diese Problematik untersuchen wir getrennt.

7.3.1. Invertieren eines Elements. Zur Motivation der Konstruktion sei R ein beliebiger kommutativer Ring und $s \in R$ fixiert. Wir wollen nun „s invertieren“. Hierzu betrachten wir den Polynomring $R[T]$ und fassen die Variable T als Kandidat für „s^{-1}“ ins Auge. Natürlich gilt *nicht* wirklich $sT = 1_{R[T]}$, doch können wir diese Gleichung in einem geeigneten Faktorring „erzwingen“. Hierzu sei $\mathfrak{a} = \langle 1_R - sT \rangle$ das von $1_R - sT$ erzeugte Ideal. Im Faktorring $R/\mathfrak{a}$ gilt nun aber

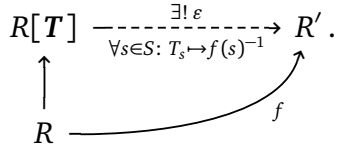
$$(s + \mathfrak{a}) \cdot (T + \mathfrak{a}) = sT + \mathfrak{a} = (1_R + (sT - 1_R)) + \mathfrak{a} = 1_R + \mathfrak{a} = 1_{R/\mathfrak{a}}.$$

In diesem Sinne ist also s (lies: $s+\mathfrak{a}$) in $R/\mathfrak{a}$ invertierbar. Man beachte insbesondere den folgenden degenerierten Fall: wählt man $s = 0_R$, so ist $\mathfrak{a} = \langle 1_R - 0_R T\rangle = \langle 1_R\rangle = R$ und $R/\mathfrak{a} = \mathbf{0}$ ist der Nullring. Die kanonische Projektion $R \to R/\mathfrak{a}$ braucht also nicht injektiv zu sein.

7.3.2. Der allgemeine Fall. Sind s und s' zwei invertierbare Elemente eines Rings, so auch gilt dies auch für ss'. Zudem ist das Einselement eines Ringes stets invertierbar. Es sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt ***multiplikatives System***, falls die folgenden beiden Eigenschaften erfüllt sind:

(1) $1_R \in S$,
(2) $s, s' \in S \implies ss' \in S$.

Ist nun $f\colon R \to R'$ ein beliebiger Ringhomomorphismus derart, dass $f(s)$ für jedes $s \in S$ eine Einheit in R' ist. Wir betrachten dann den Polynomring $R[\boldsymbol{T}]$ in einer durch S indizierten Menge $\boldsymbol{T} = \{\, T_s : s \in S \,\}$ paarweise verschiedener Variablen (siehe Aufgabe T11.2). Dann gibt es dank der in Aufgabe T11.2 bereitgestellten multivariaten Verallgemeinerung von Satz 7.4 genau einen Ringhomomorphismus $\varepsilon\colon R[\boldsymbol{T}] \to R'$, welcher das folgende Diagramm kommutativ macht und T_s auf $f(s)^{-1}$ abbildet:

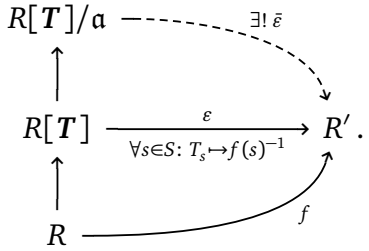


Insbesondere ist dann

$$\varepsilon(1_R - sT_s) = \varepsilon(1_R) - \varepsilon(s)\varepsilon(T_s) = 1_{R'} - f(s)f(s)^{-1} = 1_{R'} - 1_{R'} = 0_{R'}.$$

Das Ideal $\mathfrak{a} = \langle\, 1_R - sT_s : s \in S \,\rangle$ ist also im Kern von ε enthalten und Satz 6.7 liefert die Existenz von genau einer Abbildung $\bar{\varepsilon}$, welche das folgende Diagramm kommutativ macht:

(7.7)



Wir wollen nun $R[\boldsymbol{T}]/\mathfrak{a}$ näher in Abhängigkeit von R und S beschreiben. Hierfür ist es nötig, zu verstehen, was nach der Erweiterung von R zu dem deutlich größeren Ring $R[\boldsymbol{T}]$ und anschließender Faktorbildung nach $\mathfrak{a}$ zusammenfällt. Dies erfordert ein wenig Arbeit.

Lemma 7.9. *Es sei S ein multiplikatives System in einem kommutativen Ring R. $R[\boldsymbol{T}]$ und $\mathfrak{a} = \langle 1_R - sT_s : s \in S \rangle$ mögen wie oben definiert sein. Dann gilt:*

(1) $T_s T_u \equiv T_{su} \bmod \mathfrak{a}$.
(2) $T_u \equiv sT_{su} \bmod \mathfrak{a}$.
(3) $aT_s + bT_u \equiv (au + sb)T_{su} \bmod \mathfrak{a}$.
(4) $aT_u \equiv 0_R \bmod \mathfrak{a} \iff \exists s \in S\colon sa = 0_R$.

Beweis. Die ersten drei Behauptungen rechnet man leicht nach:

(1) $T_s T_u \equiv T_s T_u - T_s T_u(1_R - suT_{su}) = (sT_s)(uT_u)T_{su} \equiv T_{su} \mod \mathfrak{a}$,
(2) $T_u = 1_R T_u \equiv (sT_s)T_u = s(T_s T_u) = sT_{su} \mod \mathfrak{a}$,
(3) $aT_s + bT_u \equiv auT_{su} + bsT_{su} = (au + sb)T_{su} \mod \mathfrak{a}$.

Nun untersuchen wir die letzte Behauptung. Zunächst sei angenommen, dass es ein $s \in S$ mit $sa = 0_R$ gibt. Dann ist $a = a(1_R - sT_s) \equiv 0_R \bmod \mathfrak{a}$ und also $aT_u \equiv 0_R \bmod \mathfrak{a}$. Umgekehrt sei nun $aT_u \equiv 0_R \bmod \mathfrak{a}$. Wir müssen zeigen, dass es ein $s \in S$ mit $sa = 0_R$ gibt. Hierzu beachte man zunächst

$$0_R \equiv u(aT_u) = a(uT_u) \equiv a \mod \mathfrak{a}.$$

Demnach lässt sich a in der Form

$$a = \sum\nolimits_s (1_R - sT_s) f_s$$

schreiben, wobei die Laufvariable s über eine endliche Teilmenge von S zu erstrecken ist und die f_s Polynome aus $R[\boldsymbol{T}]$ sind. Für den Rest des Beweises seien die Laufvariablen in $\sum_s$, $\sum_u$ und $\prod_u$ alle auf die eben erwähnte endliche Teilmenge von S beschränkt. Wir arbeiten nun mit Multiindizes $\boldsymbol{j}$; das sind Abbildungen $S \to \mathbb{N}_0$ mit endlichem *Träger* $\boldsymbol{j}^{-1}(\mathbb{N}) \subseteq S$. Für einen solchen Multiindex $\boldsymbol{j}$ sei $\boldsymbol{T}^{\boldsymbol{j}} = \prod_{s \in S} T_s^{j(s)}$. Für $n \in \mathbb{N}_0$ und $s \in S$ schreiben wir $n\underline{s}$ für den Multiindex $S \to \mathbb{N}_0$, welcher bei s den Wert n annimmt und sonst überall Null ist. Wir schreiben ferner $\boldsymbol{0} := 0\underline{s}$ and $\underline{s} := 1\underline{s}$. Schreibt man nun $f_s = \sum_{\boldsymbol{j}} r_{s,\boldsymbol{j}} \boldsymbol{T}^{\boldsymbol{j}}$, wobei $\boldsymbol{j}$ über alle Abbildungen $S \to \mathbb{N}_0$ laufe, so erhalten wir

$$a = \sum\nolimits_s r_{s,\boldsymbol{0}} + \sum_{\boldsymbol{j} \neq \boldsymbol{0}} \Big(\sum\nolimits_s r_{s,\boldsymbol{j}} \Big) \boldsymbol{T}^{\boldsymbol{j}} - \sum\nolimits_{\boldsymbol{j}} \sum\nolimits_s s r_{s,\boldsymbol{j}} T_s \boldsymbol{T}^{\boldsymbol{j}}. \tag{7.8}$$

Ein Koeffizientenvergleich bei $\boldsymbol{T}^{\boldsymbol{0}}$ und $\boldsymbol{T}^{n\underline{s}}$, $n \in \mathbb{N}$, beider Seiten von (7.8) zeigt

$$a = \sum\nolimits_s r_{s,\boldsymbol{0}}, \tag{7.9}$$

$$s r_{s,(n-1)\underline{s}} = \sum\nolimits_u r_{u,n\underline{s}}. \tag{7.10}$$

Wegen $r_{u,n\underline{s}} = 0_R$ für alle hinreichend großen n, zeigt eine einfache Induktion mittels (7.10), dass Multiplikation mit einer geeignet großen Potenz s von $\prod_u u$ alle $r_{u,\boldsymbol{0}}$ annuliert. Wegen (7.9) ist dann allerdings $sa = 0_R$ und wir sind fertig. □

Wegen $r = r1_R \equiv rT_1 \bmod \mathfrak{a}$ zeigt Lemma 7.9, dass jedes Element von $R[\boldsymbol{T}]/\mathfrak{a}$ von der Form $aT_u \bmod \mathfrak{a}$ ist, z.B.

$$3T_sT_u^2 - T_t \equiv 3T_{su^2} - T_t \equiv (3t - su^2)T_{su^2t} \mod \mathfrak{a}.$$

Wir schreiben nun $\frac{a}{s}$ für $aT_s \bmod \mathfrak{a}$. Man nennt $R[\boldsymbol{T}]/\mathfrak{a}$ die ***Lokalisierung von R bei S*** und schreiben $S^{-1}R$ für $R[\boldsymbol{T}]/\mathfrak{a}$. Dann gilt:

Proposition 7.10 (Eigenschaften der Lokalisierung)**.** *Es ist*

$$S^{-1}R = \{\, \tfrac{a}{s} : a \in R, s \in S \,\} \tag{7.11}$$

und für die Elemente von $S^{-1}R$ gelten die folgenden Rechenregeln:

(1) $\frac{a}{s} + \frac{b}{u} = \frac{au+sb}{su}$,

(2) $\frac{a}{s} \cdot \frac{b}{u} = \frac{ab}{su}$,

(3) $\frac{a}{s} = \frac{b}{u} \iff \exists t \in S\colon t(au - sb) = 0_R$.

Darüber hinaus gelten auch die folgenden Aussagen:

(4) Die Abbildung $\tau\colon R \to S^{-1}R$, $r \mapsto \frac{r}{1_R}$, ist ein Ringhomomorphismus.

(5) $\ker\tau = \{\, r \in R : \exists t \in S\colon tr = 0_R \,\}$.

(6) $\tau(s)$ ist eine Einheit in $S^{-1}R$ für jedes $s \in S$.

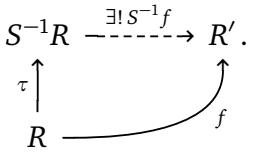
(7) $S^{-1}R$ ist genau dann der Nullring, wenn $0_R \in S$ gilt.

(8) τ ist bijektiv genau dann, wenn S nur aus Einheiten von R besteht.

Beweis. Die Darstellung (7.11) haben wir schon direkt oberhalb der Proposition begründet. Die drei Rechenregeln sind eine triviale Umformulierung von Lemma 7.9 und die übrigen Aussagen folgen leicht aus diesen bzw. aus der Konstruktion von $S^{-1}R$. (Beispielsweise die Aussage, dass es sich bei τ um einen Ringhomomorphismus handelt, ist klar, da es sich bei τ lediglich um die Verknüpfung der kanonischen Inklusion $R \to R[X]$ mit der kanonischen Projektion $R[X] \to R[X]/\mathfrak{a}$ handelt.) □

Die Abbildung τ aus Proposition 7.10 bezeichnen wir als ***kanonischen Homomorphismus in die Lokalisierung***. Sofern in einem Diagramm ein unbeschrifteter Pfeil $R \to S^{-1}R$ auftaucht und nichts Gegenteiliges behauptet wird, so ist mit diesem Pfeil stets τ gemeint.

Satz 7.11 (Universelle Eigenschaft von $S^{-1}R$)**.** *Es sei S ein multiplikatives System in einem kommutativen Ring R. Dann erfüllt die kanonische Abbildung $\tau\colon R \to S^{-1}R$ die folgende Eigenschaft: $\tau(S) \subseteq (S^{-1}R)^\times$ und für jeden Homomorphismen $f : R \to R'$ in einen kommutativen Ring R' mit $f(S) \subseteq (R')^\times$ gibt es genau einen Ringhomomorphismus $S^{-1}f$, der das folgende Diagramm kommutativ macht:*



Beweis. Man kann sich direkt mittels Proposition 7.10 überlegen, dass $S^{-1}f$ wie folgt abbilden muss:

$$(S^{-1}f)(\tfrac{a}{s}) = f(a)f(s)^{-1}.$$

Umgekehrt kann man diese Gleichung zur Definition von $S^{-1}f$ hernehmen und rechnet leicht nach, dass dies die gewünschten Eigenschaften hat.

Etwas konzeptioneller geht es allerdings, indem man auf das kommutative Diagramm (7.7) schaut. Dort hatten wir bereits die Existenz von $\bar{\varepsilon} = S^{-1}f$ geklärt. Umgekehrt folgt die Eindeutigkeit aber auch, indem man — gegeben die Kommutativität des äußeren Dreiecks in (7.7) die Abbildung ϵ durch Verkettung von $\bar{\epsilon}$ mit $R[\boldsymbol{T}] \to R[\boldsymbol{T}]/\mathfrak{a}$ rekonstruiert, sich darauf beruft, dass diese wegen Satz 7.4 eindeutig durch f bestimmt ist und dann bemerkt, dass diese wegen Satz 6.7 aber auch $\bar{\epsilon}$ eindeutig festlegt. □

7.3.3. Quotientenkörper. Ist R ein Integritätsbereich, so handelt es sich bei $S = R \setminus \{0_R\}$ um ein multiplikatives System. Der Ring $\mathrm{Quot}(R) := S^{-1}R$ ist dann ein Körper (vgl. (7.11)) und heißt ***Quotientenkörper von R***. Da R ein Integritätsbereich ist, ist der kanonische Homomorphismus

$$\tau\colon R \longrightarrow \mathrm{Quot}(R) \tag{7.12}$$

sogar *injektiv* (siehe Proposition 7.10 (5)) und heißt ***kanonische Einbettung*** von R in seinen Quotientenkörper.

Beispiele (Quotientenkörper)**.**

(1) $\mathrm{Quot}(\mathbb{Z}) \cong \mathbb{Q}$. Tatsächlich *gibt* es auch überhaupt *nur einen* Ringhomomorphismus $\mathrm{Quot}(\mathbb{Z}) \to \mathbb{Q}$ und dieser ist ein Ringisomorphismus. Darum schreiben wir auch ganz ohne Skrupel $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$, obwohl uns für $\mathbb{Q}$ womöglich eine andere Konstruktion bekannt ist, und $\mathrm{Quot}(\mathbb{Z})$ und $\mathbb{Q}$ rein mengentheoretisch gemäß der von uns benutzten Definitionen nicht identisch zu sein brauchen.

(2) Für den Polynomring $K[X]$ über einem Körper K nennt man $\mathrm{Quot}(K[X])$ den ***Körper der rationalen Funktionen über K***. Die Elemente von $\mathrm{Quot}(K[X])$ sind (formale) Quotienten aus Polynomen mit Koeffizienten aus K, wobei einzig das Nullpolynom als Nenner ausgeschlossen ist. Diese Quotienten sind den offensichtlichen Rechenregeln unterworfen (vgl. Proposition 7.10). Wir haben beispielsweise

$$\frac{(X^{12}+4X^3+3)(X+1)}{(X^2-42)(X+1)} = \frac{X^{12}+4X^3+3}{X^2-42} \in \mathrm{Quot}(\mathbb{Q}[X]).$$

Man beachte, dass der Begriff „Funktionen“ in der obigen Benennung nicht im eigentlichen Sinne verstanden werden soll: das Beispiel auf Seite 115 mahnt uns dazu, Polynome und die zugehörigen Polynomfunktionen zu unterscheiden.

Bemerkung. Für einen Homomorphismus $\iota\colon K \to L$ (eine sogenannte ***Körpererweiterung***; siehe etwa [45, Kapitel 1]) zwischen Körpern und $x \in L$ schreibt man auch $K(x)$ für den kleinsten Teil*körper* von L, welcher $\operatorname{im}\iota = \iota(K)$ und x enthält. (Man beachte die runden Klammern; Für $K[x]$ mit eckigen Klammern ist im obigen Text „Teilkörper“ durch „Teilring“ zu ersetzen.) Verkettet man die kanonischen Abbildungen $K \to K[X] \to \operatorname{Quot}(K[X])$, so erhält man eine Körpererweiterung und man kann sich überlegen, dass $K(X) = \operatorname{Quot}(K[X])$ gilt. In diesem Sinne schreibt man auch oft einfach $K(X)$ für $\operatorname{Quot}(K[X])$.

Man kann auch die Ideale von $S^{-1}R$ mit Bezug auf die Ideale von R präzise charakterisieren; siehe etwa [5, Ch. 1, Proposition 5]. Wir wollen diese Thematik hier allerdings nicht weiter verfolgen und behandeln lediglich ein Beispiel dafür in Form von Aufgabe 12.3.

7.3.4. Alternative Konstruktion. Wir merken noch an, dass in der Literatur oft eine alternative Konstruktion von Lokalisierungen gegeben wird. Hierzu betrachte man ein multiplikatives System S in einem kommutativen Ring R. Dann betrachte man das (mengentheoretische) kartesische Produkt $R \times S$ und führe auf diesem eine Äquivalenzrelation $\sim$ ein:

$$(a,s) \sim (a',s') \quad :\Longleftrightarrow \quad \exists t \in S\colon (as'-a's)t = 0_R. \tag{7.13}$$

Dass dies wirklich eine Äquivalenzrelation ist, rechnet man einfach nach; Symmetrie und Reflexivität sind hierbei sehr einfach einzusehen und sollen daher nicht ausgeführt werden. Für die Rechtfertigung der Transitivität seien

$$(a,s) \sim (a',s') \quad \text{und} \quad (a',s') \sim (a'',s'')$$

gegeben. Dann gibt es also $t, t' \in S$ mit

$$(as'-a's)t = 0_R \quad \text{und} \quad (a's''-a''s')t' = 0_R.$$

Wir haben dann

$$(as''-a''s)s's''tt' = (as'-a's)(s'')^2tt' + (a's''-a''s')ss''tt' = 0_R$$

und also $(a,s) \sim (a'',s'')$. Die Äquivalenzklasse $[(a,s)]_\sim$ von $(a,s) \in R \times S$ bezüglich $\sim$ bezeichnen wir auch suggestiv mit $\frac{a}{s}$. Dann definieren wir auf der Menge $(R\times S)/\!\sim$ der Äquivalenzklassen eine Addition und eine Multiplikation durch

$$\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{st} \quad \text{und} \quad \frac{a}{s}\cdot\frac{b}{t} := \frac{ab}{st}.$$

Hier gilt es nachzurechnen, dass diese Verknüpfungen wohl-definiert sind, da in etwa a durch die Angabe der Klasse $\frac{a}{s} = [(a,s)]_\sim$ nicht eindeutig bestimmt ist. Anhand von Proposition 7.10 kann man sehen, dass der eben konstruierte Ring $(R \times S)/\!\sim$ isomorph zu $S^{-1}R$ ist.

Man beachte, dass die in (7.13) definierte Relation in der Variante „$as' - a's = 0$“ vermutlich bereits aus einer Grundlagenvorlesung bekannt ist, in welcher $\mathbb{Q}$ aus

$\mathbb{Z}$ konstruiert wurde. Tatsächlich kann man bei Integritätsbereichen auf den Teil „$\exists t \in S\colon (\ldots)t = 0_R$“ (Multiplikation mit t) verzichten, braucht diesen bei allgemeinen Ringen R jedoch, um z.B. die Transitivität von $\sim$ gewährleisten zu können.

7.4. Universelle Identitäten

Neben unserer Konstruktion von Lokalisierungen, welche man als eine Anwendung von Polynomringen auffassen kann, skizzieren wir nun eine weitere Anwendung. Jene zeigt, dass man gewisse Identitäten bereits *für alle* kommutativen Ringe gewinnen kann, indem man selbige für einige wenige spezielle Ringe verifiziert. Der dabei gewonnene Vorteil ist, dass die auftretenden speziellen Ringe oft sehr gutartige ringtheoretische Eigenschaften aufweisen und man deshalb weitere Methoden zum Einsatz bringen kann, die uns für allgemeine (kommutative) Ringe nicht zur Verfügung stünden.

7.4.1. Ein triviales Beispiel. Im Polynomring $\mathbb{Z}[X,Y]$ gilt die Identität

$$(\dagger_{XY}) \qquad X^2 - Y^2 = (X+Y)(X-Y).$$

Gleichwohl gilt in jedem kommutativen Ring R die Identität

$$(\dagger_{ab}) \qquad a^2 - b^2 = (a+b)(a-b)$$

für alle $a, b \in R$ („***dritte binomische Formel***“). Selbstverständlich handelt es sich bei $(\dagger_{XY})$ um einen *Spezialfall* von $(\dagger_{ab})$ und beide Identitäten folgert man einfach aus den beiden Distributivgesetzen in Kombination mit den Rechenregeln aus Proposition 6.2.

Wir wollen nun die verblüffende Tatsache einsehen, dass wir *umgekehrt auch $(\dagger_{ab})$ als Spezialfall von $(\dagger_{XY})$ ansehen dürfen*! Die Identität $(\dagger_{ab})$ folgt nämlich aus $(\dagger_{XY})$ durch Einsetzen: Laut Proposition 6.3 gibt es (genau) einen Ringhomomorphismus $\mathbb{Z} \to R$ und Aufgabe T11.2 liefert die Existenz (genau) eines Ringhomomorphismus $f\colon \mathbb{Z}[X,Y] \to R$, der X auf a und Y auf b abbildet und das folgende Diagramm kommutativ macht:

$$\begin{array}{ccc} \mathbb{Z}[X,Y] & \xrightarrow[X\mapsto a,\, Y\mapsto b]{\exists!\, f} & R\,. \\ \uparrow & \nearrow & \\ \mathbb{Z} & & \end{array}$$

Dann folgt

$$a^2 - b^2 = f(X^2 - Y^2) = f((X+Y)(X-Y)) = (a+b)(a-b).$$

Man kann also sagen, dass $(\dagger_{ab})$ in jedem kommutativen Ring gilt, *weil* $(\dagger_{XY})$ in $\mathbb{Z}[X,Y]$ gilt. Hier gilt es zu beachten, dass $\mathbb{Z}[X,Y]$ ein Integritätsbereich ist und indes also in seinen Quotientenkörper $\mathrm{Quot}(\mathbb{Z}[X,Y])$ eingebettet werden kann. (Letzteres ist für allgemeine kommutative Ringe R nicht möglich!) Indes könnten zur Verifikation von $(\dagger_{XY})$ also auch Methoden aus der Körpertheorie benutzt werden. Das klingt in dem vorliegenden Fall natürlich nach einem schwachen Argument, da $(\dagger_{XY})$

unmittelbar durch eine Rechnung verifiziert werden kann und selbiges sogar auch für $(\dagger_{ab})$ gilt, doch lässt sich dies in anderen Situationen (siehe unten!) wirklich gewinnbringend einsetzen.

7.4.2. Ein Beispiel mit Determinaten. Die lineare Algebra befasst sich mit der Theorie der Vektorräume und viele ihrer Ergebnisse gelten über beliebigen K-Vektorräumen, wobei K ein völlig willkürlich gewählter *Körper* sein kann. Man zeigt etwa: ist K ein Körper und $n \in \mathbb{N}$, so gibt es genau eine alternierende Multilinearform $\det\colon K^{n\times n} \to K$, welche zusätzlich der Normierungsbedingung

$$\det \begin{pmatrix} 1_K & & \\ & \ddots & \\ & & 1_K \end{pmatrix} = 1_K$$

genügt, die sogenannte ***Determinante***. Die bekannte ***Leibniz-Formel*** besagt

$$\det \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}, \tag{7.14}$$

wobei $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ hier als $\in \{\pm 1_K\}$ zu verstehen ist. (Siehe auch § 4.2 und beachte $\{\pm 1\} \cong \{\pm 1_K\}$ als Gruppen.)

Für einen beliebigen kommutativen Ring R und eine Matrix $A \in R^{n\times n}$ *definieren* wir nun $\det(A)$ durch die rechte Seite von (7.14), da die entsprechenden Summen und Produkte ja in beliebigen Ringen gebildet werden können, wobei $\operatorname{sgn}(\sigma)$ darin dann als Element von $\{\pm 1_R\}$ zu verstehen ist. Man beachte, dass die Definition einer Determinantenfunktion $\det\colon R^{n\times n} \to R$ mittels der Charakterisierung als geeignet normierte alternierende Multilinearform nicht zur Verfügung steht, da R^n kein Vektorraum zu sein braucht und auch nicht klar ist, ob die genannten Eigenschaften die gesuchte Funktion eindeutig bestimmen. Definiert man das Produkt $A \cdot B$ zweier Matrizen $A, B \in R^{n\times n}$ mittels der aus der linearen Algebra bekannten Formel („Zeile mal Spalte“), so stellt sich die Frage, ob die bekannte Determinantenmultiplikationsformel

$$\det(A \cdot B) = \det(A)\det(B)$$

auch gültig bleibt? *Die Antwort ist „ja“!*

Proposition 7.12 (Determinantenmultiplikationsformel)**.** *Für Matrizen $A, B \in R^{n\times n}$ über einem kommutativen Ring gilt* $\det(A \cdot B) = \det(A)\det(B)$.

Beweis. Wir schreiben für den Moment des Beweises $\det_R$ für det und Varianten davon, um auf den Ring Bezug zu nehmen, in dem die fragliche Determinante zu berechnen ist. Wir betrachten den Polynomring $\mathbb{Z}[\boldsymbol{X}, \boldsymbol{Y}]$ in den $2n^2$ Variablen

$$\boldsymbol{X} = \{X_{ij} : 1 \le i, j \le n\} \quad \text{und} \quad \boldsymbol{Y} = \{Y_{ij} : 1 \le i, j \le n\}.$$

Wir benutzen nun die kanonische Einbettung

$$\tau\colon \mathbb{Z}[\boldsymbol{X}, \boldsymbol{Y}] \hookrightarrow K := \operatorname{Quot}(\mathbb{Z}[\boldsymbol{X}, \boldsymbol{Y}])$$

aus (7.12) und fassen $\boldsymbol{X}$ und $\boldsymbol{Y}$ in offensichtlicher Weise als $n\times n$-Matrizen über $\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]$ auf: $\boldsymbol{X} = (X_{ij})_{i,j=1}^n$ und $\boldsymbol{Y}$ analog. Wir setzen weiter $\tau\boldsymbol{X} := (\tau(X_{ij}))_{i,j=1}^n$ und $\tau\boldsymbol{Y} := (\tau(Y_{ij}))_{i,j=1}^n$ für die zugehörigen Matrizen über K. Für $n\times n$-Matrizen über dem Körper K gilt die Determinantenmultiplikationsformel, wie wir aus der *linearen Algebra* wissen. Also ist

$$\det_K(\tau\boldsymbol{X}\cdot\tau\boldsymbol{Y}) = \det_K(\tau\boldsymbol{X})\det_K(\tau Y).$$

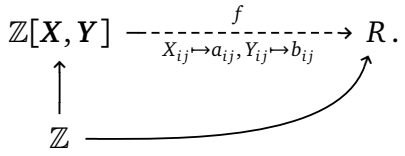
Unter Berufung auf die Darstellung (7.14) und die Homomorphismus-Eigenschaft von τ erhalten wir hieraus

$$\tau\big(\det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{X}\cdot\boldsymbol{Y})\big) = \tau\big(\det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{X})\det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{Y})\big).$$

Da τ injektiv ist, gilt diese Gleichung nun auch, wenn man τ weglässt und wir erhalten also

$$\det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{X}\cdot\boldsymbol{Y}) = \det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{X})\det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{Y}). \tag{7.15}$$

Offensichtlich handelt es sich bei (7.15) um einen Spezialfall der im Rahmen der Proposition behaupteten Aussage. Wir zeigen nun, wie man aus diesem den allgemeinen Fall gewinnen kann. Laut Proposition 6.3 gibt es (genau) einen Ringhomomorphismus $\mathbb{Z}\to R$ und Aufgabe T11.2 liefert die Existenz eines Ringhomomorphismus $f\colon \mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]\to R$, der X_{ij} auf a_{ij} (i,j-ter Eintrag von A) und Y_{ij} auf b_{ij} (i,j-ter Eintrag von B) abbildet und das folgende Diagramm kommutativ macht:



Anhand der Definition der Determinante sieht man

$$f\big(\det_{\mathbb{Z}[\boldsymbol{X},\boldsymbol{Y}]}(\boldsymbol{X})\big) = \det_R(A)$$

und analog für $\boldsymbol{Y}$ und B, sowie $\boldsymbol{X}\cdot\boldsymbol{Y}$ und $A\cdot B$. Demnach ergibt sich aus dann

$$\det_R(A\cdot B) = \det_R(A)\det_R(B)$$

mittels (7.15), wie gewünscht. □

Wir bemerken noch abschließend, dass die Leserinnen und Leser Proposition 7.12 bereits implizit oder explizit in der linearen Algebra benutzt haben dürften. Ein solches Ergebnis wird üblicher Weise verwendet, wenn man zeigen möchte, dass das charakteristische Polynom χ_A einer Matrix $A\in K^{n\times n}$ invariant unter Konjugation von

A mit invertierbaren Matrizen $T \in \mathrm{GL}_n K$ ist:

$$\begin{aligned}\chi_{TAT^{-1}} &= \det(X\mathbf{1}_n - TAT^{-1}) \\ &= \det(T(X\mathbf{1}_n - A)T^{-1}) \\ &= \det(T)\det(X\mathbf{1}_n - A)\det(T^{-1}) \\ &= \det(X\mathbf{1}_n - A) \\ &= \chi_A.\end{aligned}$$

(Man kann die Gleichheit von $\chi_{TAT^{-1}}$ und χ_A alternativ auch nach Einsetzen von Elementen $x \in K$ für X prüfen. Im Fall $\#K > n$ genügt das auch, um $\chi_{TAT^{-1}} = \chi_A$ zu folgern, aber Körper mit $\#K \leq n$ lassen sich so nicht behandeln.)

KAPITEL 8

Teilbarkeitslehre

Leitmotiv dieses Kapitels ist die eindeutige Primfaktorzerlegung in $\mathbb{Z}$. Welche uns bekannten (kommutativen!) Ringe gestatten eine derartige Primfaktorzerlegung? Diese Frage umfassend zu klären scheint zu kompliziert. Wir begnügen uns damit, diverse Klassen von Ringen zu untersuchen, in denen die Arithmetik besonders gutmütig ausfällt.

Wir wollen den Teilbarkeitsbegriff in allgemeinen kommutativen Ringen fassen. Sei R ein kommutativer Ring. Wir sagen $a \in R$ ***teilt*** $b \in R$ (in Zeichen: $a \mid b$, oder $a \mid_R b$, wenn wir auf R Bezug nehmen wollen), wenn b in $\langle a \rangle = aR$ enthalten ist, also wenn es ein $r \in R$ mit $ar = b$ gibt. Die Menge aller durch a teilbaren Elemente ist demnach das von a erzeugte (Haupt-)Ideal. Allgemein sagen wir, ein Ideal $\mathfrak{a}$ ***teilt*** ein Ideal $\mathfrak{b}$, wenn $\mathfrak{a} \supseteq \mathfrak{b}$ gilt. („***Teilen heißt Enthalten***“.) Im Allgemeinen braucht nicht jedes Ideal von R ein Hauptideal zu sein (z.B. $\langle 2, X \rangle$ in $\mathbb{Z}[X]$, siehe Beispiel 6.5). In günstigen Fällen ist dies jedoch trotzdem der Fall. Wir widmen uns nun der Untersuchung eben diesen Themenkreises. Abbildung 19 mag dabei als Orientierungshilfe dienen.

Bemerkung. Der Bezug auf den benutzten Ring ist durchaus wichtig, wenn mehrere Ringe und Oberringe im Spiel sind. Beispielsweise gilt $2 \nmid_{\mathbb{Z}} 3$ (2 teilt nicht 3 in $\mathbb{Z}$), aber sehr wohl $2 \mid_{\mathbb{Q}} 3$, denn es ist ja $3 = 2r$ mit $r = 3/2 \in \mathbb{Q}$.

8.1. Euklidische Ringe

R sei ein Integritätsbereich. R heißt ***Hauptidealbereich*** (oder ***Hauptidealring***), falls jedes Ideal von R ein Hauptideal ist. R heißt ***euklidisch***, falls eine ***Gradfunktion*** $\gamma\colon R \setminus \{0_R\} \to \mathbb{N}_0$ existiert, sodass für alle $a, b \in R$ mit $b \neq 0_R$ Elemente $q, r \in R$ mit $a = b \cdot q + r$ und $r = 0_R$ oder $\gamma(r) < \gamma(b)$ existieren.

Beispiele 8.1 (Beispiele für euklidische Ringe)**.**

(1) $\mathbb{Z}$ ist euklidisch mit Gradfunktion $\mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$, $n \mapsto |n|$.
(2) Der Polynomring $K[X]$ über einem beliebigen Körper K ist euklidisch mit Gradfunktion $K[X] \setminus \{0_{K[X]}\} \to \mathbb{N}_0$, $f \mapsto \deg(f)$ (siehe Proposition 7.2 (3)).
(3) Der Ring der ganzen Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}] = \{ a + \mathrm{i}b \in \mathbb{C} : a, b \in \mathbb{Z} \}$ ist euklidisch mit der Gradfunktion $\mathbb{Z}[\mathrm{i}] \setminus \{0\} \to \mathbb{N}_0$, $a + \mathrm{i}b \mapsto a^2 + b^2$ (siehe Aufgabe T9.2).
(4) Jeder Körper K ist euklidisch. Um dies zu sehen, wähle man $\gamma\colon K \setminus \{0_R\} \to \mathbb{N}_0$ einfach beliebig. Zu $a, b \in K$ mit $b \neq 0_K$ handelt es sich bei b ja um eine

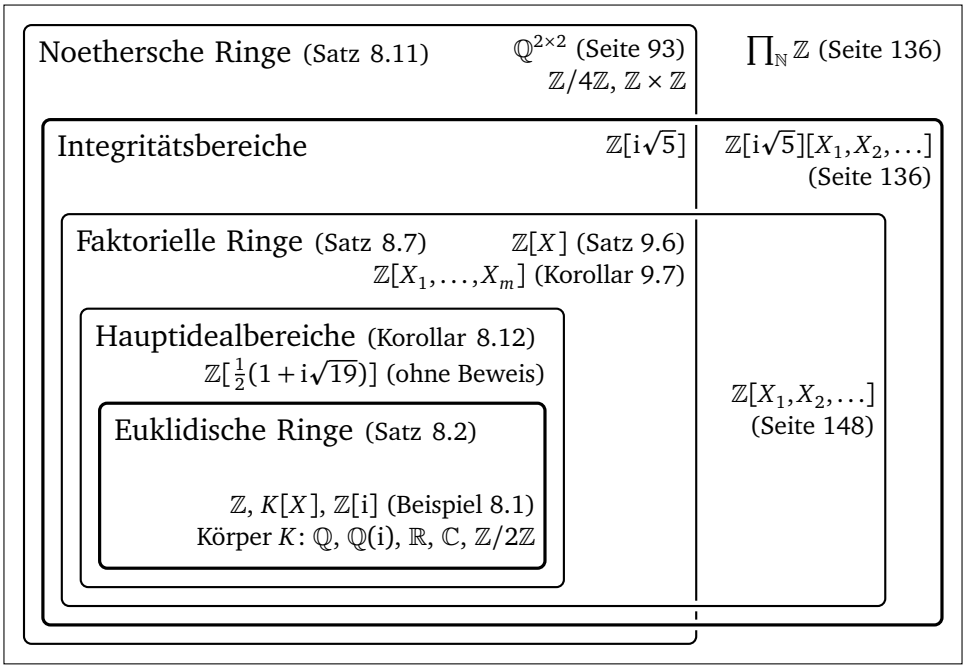


Abbildung 19. Verschiedene Klassen von Ringen mit entsprechenden Beispielen.

Einheit. Wählen wir $q = b^{-1}a$, so schreibt sich $a = b\cdot q + r$ mit $r = 0_K$. Der Fall, in welchem $\gamma(r) < \gamma(b)$ zu prüfen wäre, tritt daher also gar nicht auf.

8.1.1. Idealstruktur in euklidischen Ringen. Die Idealstruktur in euklidischen Ringen sieht besonders einfach aus:

Satz 8.2. *Jeder euklidische Ring ist ein Hauptidealbereich.*

Beweis. Der Beweis verläuft durch Adaption des Beweises von Proposition 1.11 (bzw. Aufgabe T2.3). Hierzu sei R ein euklidischer Ring mit Gradfunktion γ. Das Nullideal $\{0_R\} = \langle 0_R\rangle$ ist ein Hauptideal. Sei daher $\mathfrak{a}$ ein beliebiges Ideal von R, welches nicht das Nullideal ist. Dann ist $\mathfrak{a}\setminus\{0_R\}$ nicht leer. Darum gibt es unter den Elementen von $\mathfrak{a}\setminus\{0_R\}$ eines mit minimalem Grad. Wir nennen dieses b und wollen $\mathfrak{a} = \langle b\rangle$ beweisen. Ist nämlich $a\in\mathfrak{a}$ beliebig, so gibt es $q,r\in R$ mit $a = b\cdot q + r$ derart, dass $r = 0_R$ oder $\gamma(r) < \gamma(b)$ gilt. Der zweite Fall kann wegen $r = a - b\cdot q\in\mathfrak{a}$ und der minimalen Wahl von $\gamma(b)$ nicht eintreten. Also muss $r = 0_R$ gelten und wir haben $a = b\cdot q\in bR = \langle b\rangle$. Demnach gilt $\mathfrak{a}\subseteq\langle b\rangle$. Da die umgekehrte Inklusion aber ohnehin klar ist, folgt $\mathfrak{a} = \langle b\rangle$ und wir sind fertig. □

Bemerkung. Es gibt Hauptidealbereiche, die nicht euklidisch sind, z.B.

$$\mathbb{Z}[\tfrac{1}{2}(1+i\sqrt{19})] = \{\tfrac{1}{2}(a+i\sqrt{19}b) : a,b\in\mathbb{Z}\text{ mit }a\equiv b \bmod 2\}.$$

(Für einen Beweis hiervon sei auf einschlägige Vorlesungen über kommutative Algebra oder algebraische Zahlentheorie verwiesen.)

8.1.2. Euklidischer Algorithmus. Im Folgenden bezeichne R einen euklidischen Ring mit Gradfunktion $\gamma\colon R\setminus\{0_R\}\to\mathbb{N}_0$. Zu je zwei Elementen $r_0, r_1 \in R\setminus\{0_R\}$ mit $\gamma(r_0)\geq\gamma(r_1)$ finde man mittels Division mit Rest Elemente $q_1, r_2 \in R$ mit $r_0 = q_1 r_1 + r_2$ und wiederhole diesen Prozess, solange der Rest von Null verschieden ist, z.B. für $(r_0, r_1) = (246, 77)$ in $\mathbb{Z}$ mit $\gamma = |\cdot|$:

$$\begin{cases} 246 = 3\cdot 77 + 15, \\ 77 = 5\cdot 15 + 2, \\ 15 = 7\cdot 2 + 1, \\ 2 = 2\cdot 1 + \underline{0}. \end{cases} \tag{8.1}$$

Da die γ-Werte der Reste streng monoton fallen und durch 0 nach unten beschränkt sind, terminiert der oben beschriebene Prozess; d.h. es gibt ein $n\in\mathbb{N}$ derart, dass die beschriebene Division mit Rest die Form $r_{n-1} = q_n r_n + 0$ annimmt. Das hier beschriebene Verfahren heißt ***euklidischer Algorithmus***.

Wir zeigen nun, dass r_n ein größter gemeinsamer Teiler von r_0 und r_1 ist (siehe § 8.2 für die Definition). Dafür zeigen wir zwei Aussagen:

(1) r_n teilt r_i und r_{i-1} für $i = n-1, n-2, \ldots, 1, 0$,
(2) jeder gemeinsame Teiler d von r_0 und r_1 teilt r_i für $i = 2, 3\ldots, n$.

Daraus folgt dann jedenfalls die Behauptung, denn r_n teilt dann ja r_1 und r_0 und jeder gemeinsame Teiler von r_0 und r_1 teilt r_n. Zum Beweis von (1) und (2) schreiben wir

$$\begin{cases} r_0 = q_1 \cdot r_1 + r_2, \\ r_1 = q_2 \cdot r_2 + r_3, \\ \quad\vdots \\ r_i = q_{i+1}\cdot r_{i+1} + r_{i+2}, \\ \quad\vdots \\ r_{n-2} = q_{n-1}\cdot r_{n-1} + r_n, \\ r_{n-1} = q_n \cdot r_n + 0. \end{cases}$$

Der Beweis von (1) folgt nun induktiv im obigen Schema (8.2) von unten nach oben. In der Tat zeigt die letzte Gleichung $r_n \mid r_{n-1}$. Die vorletzte Gleichung zeigt dann $r_n \mid r_{n-2}$ (Induktionsanfang). Für den Induktionsschritt dürfen wir annehmen, dass r_n bereits als Teiler von r_{i+1} und r_{i+2} erkannt wurde und behaupten, müssen einsehen, dass r_n auch r_i teilt. Das ist mit Blick auf die mittlere Gleichung im obigen Schema aber offensichtlich.

Zum Beweis von (2) sei d ein Teiler von r_0 und r_1. Für führen abermals eine Induktion und dürfen annehmen, dass d bereits als Teiler von r_i und r_{i+1} erkannt wurde. (Der Induktionsanfang mit $i = 0$ ist nach Voraussetzung erfüllt.) Ein Blick auf die mittlere Gleichung in (8.2) zeigt dann, dass d auch r_{i+2} teilt.

Wenn man die Gleichungen in (8.2), von unten angefangen, der Reihe nach, nach r_n auflöst, kann man eine Darstellung der Form $xr_0 + yr_1 = r_n$ erhalten. Man

vergleiche dies etwa mit dem Lemma von Bézout (Lemma 1.6). Wir führen dies nur anhand des Beispiels in (8.1) durch und hoffen, dass das allgemeine Vorgehen daraus hinreichend ersichtlich ist:

$$\begin{aligned} 1 &= 15 - 7\cdot 2 = 15 - 7\cdot(77 - 5\cdot 15) = (1 + 7\cdot 5)\cdot 15 - 7\cdot 77 \\ &= 36\cdot(246 - 3\cdot 77) - 7\cdot 77 = 36\cdot 246 - (36\cdot 3 + 7)\cdot 77 = 36\cdot \underline{246} - 115\cdot \underline{77}. \end{aligned}$$

Dieser Zusatz zum euklidischen Algorithmus heißt auch ***erweiterter euklidischer Algorithmus***. Für eine Anwendung siehe etwa Beispiel 10.1.

8.2. Prime und irreduzible Elemente

In unserem Modellbeispiel $\mathbb{Z}$, wo wir die eindeutige Primfaktorzerlegung schon kennen, sind die Protagonisten die *Primzahlen*. In diesem Abschnitt lernen wir kennen, welche Akteure bei der Betrachtung von Faktorisierungstheorie in allgemeinen Integritätsbereichen auf die Bühne treten. Es stellt sich heraus, dass es zwei naheliegende Verallgemeinerungen des aus $\mathbb{Z}$ bekannten Primzahlbegriffs auf die vorliegende Situation gibt: *prime* und *irreduzible* Elemente. In besonders gutartigen Situationen fallen beide Begriffe zusammen, können im Allgemeinen aber verschieden sein. Wir machen allerdings zunächst noch einige Vorbemerkungen.

Es sei M eine beliebige Teilmenge eines Integritätsbereichs R. Ein Teiler g heißt ***größter gemeinsamer Teiler (ggT) von M***, falls für jeden Teiler $t \in R$ von M (d.h. $t \mid m$ für alle $m \in M$) schon t ein Teiler von g ist. Äquivalent: $\langle g\rangle$ ist das kleinste *Haupt*ideal, welches M enthält (vgl. Aufgabe 4.4).

Bemerkung. Für $R = \mathbb{Z}$ existieren größte gemeinsame Teiler von jeder Teilmenge $M \subseteq \mathbb{Z}$. Für allgemeine Integritätsbereiche R und $M \subseteq R$ ist die *Existenz eines größten gemeinsamen Teilers von M nicht garantiert*. (Man kann sich etwa überlegen, dass $M = \{a^2, ab\}$ für $R = \mathbb{Z}[\mathrm{i}\sqrt{3}] \subset \mathbb{C}$, $a = 2$ und $b = 1 + \mathrm{i}\sqrt{3}$ keinen größten gemeinsamen Teiler besitzt. Das wollen wir hier allerdings nicht näher ausführen.)

Ein größter gemeinsamer Teiler ist — obgleich der hier implizit benutzte bestimmte Artikel dies vielleicht suggeriert — i.Allg. nicht eindeutig: in $\mathbb{Z}$ sind etwa -2 und 2 beide größter gemeinsamer Teiler von 4 und 6 im Sinne der obigen Definition. Man beachte, dass wir jedoch (gemäß der üblichen Präferenz für positive natürliche Zahlen) 2 als „den“ größten gemeinsamen Teiler im Sinne der früher benutzten Definition ansehen (siehe Seite 19). Indes sei allerdings zu beachten, dass -2 und 2 sich bloß durch Multiplikation mit einer Einheit unterscheiden: $-2 = (-1)\cdot 2$. Überdies ist $\langle -2\rangle = \langle 2\rangle$; auf Ebene der erzeugten Hauptideale ist der ggT hier also eindeutig bestimmt.

Zwei Elemente $a, b \in R$ heißen ***assoziiert***, in Zeichen $a \sim b$, falls $a \mid b$ und $b \mid a$. Auf Ebene der erzeugten Hauptideale ist dies äquivalent zu $aR \supseteq bR$ und $bR \supseteq aR$, d.h. $aR = bR$.

Lemma 8.3. *Zwei Elemente a und b eines Integritätsbereichs R sind genau dann assoziiert, wenn $au = b$ mit einer Einheit u von R gilt.*

Beweis. Ist $ae = b$ mit einer Einheit e, so folgt sofort $aR = bR$ und damit $a \sim b$. Ist umgekehrt $a \sim b$, so gibt es also $u, t \in R$ mit $au = b$ und $bt = a$. Es gilt nun $u \in R^\times$ statt nur $u \in R$ einzusehen. Wir haben $aut = bt = a$. Durch Umstellen erhalten wir daraus die Gleichung $a(ut - 1_R) = 0_R$. Weil R ein Integritätsbereich ist, muss $a = 0_R$ oder $ut - 1_R = 0_R$ (also $tu = ut = 1_R$) gelten. Im ersten Fall ist $b \in bR = aR = 0_R R = \{0_R\}$, also $b = 0_R$ und also $b = a1_R$ mit der Einheit 1_R. Im zweiten Fall sind wir aber auch fertig, denn dann ist ja u eine Einheit (denn t ist invers zu u) mit $au = b$. □

Korollar 8.4. *Sei M eine beliebige Teilmenge eines Integritätsbereichs R. Dann erzeugen je zwei größte gemeinsame Teiler von M (falls diese existieren) dasselbe Hauptideal und jeder Erzeuger dieses Hauptideals ist ein größter gemeinsamer Teiler von M.*

Man nennt eine Teilmenge $M \subseteq R$ (bzw. die Elemente davon) eines Integritätsbereichs R ***teilerfremd***, falls ein (und dann jeder) größter gemeinsamer Teiler von M eine Einheit von R ist. (Äquivalent: $\langle M \rangle = R$.)

Ein Element $p \in R \setminus (R^\times \cup \{0_R\})$ heißt ***irreduzibel***, falls jede Zerlegung $p = ab$ mit $a, b \in R$ automatisch $a \in R^\times$ oder $b \in R^\times$ erfüllt. Nicht irreduzible Elemente von $R \setminus (R^\times \cup \{0_R\})$ nennt man ***reduzibel***. Ein Element $p \in R \setminus (R^\times \cup \{0_R\})$ heißt ***prim*** (oder ***Primelement***), falls für alle $a, b \in R$ aus $p \mid ab$ schon $p \mid a$ oder $p \mid b$ folgt. Äquivalent: $p \in R$ ist genau dann prim, wenn $\mathfrak{p} = \langle p \rangle$ ein Primideal ist (siehe Aufgabe 10.3); äquivalent: $R/\langle p \rangle$ ist ein Integritätsbereich.

In $\mathbb{Z}$ sind die irreduziblen Elemente genau $\pm p$ mit Primzahlen p; diese sind auch genau die Primelemente im Sinne der Ringtheorie, wie das Lemma von Euklid (Lemma 3.2) zeigt.

Lemma 8.5. *In einem Integritätsbereich sind alle Primelemente irreduzibel.*

Beweis. Sei p ein Primelement in einem Integritätsbereich R. Aus $p = ab$ mit $a, b \in R$ folgt dann $p \mid a$ oder $p \mid b$. Andererseits folgt aus $p = ab$ auch $a, b \mid p$ und insgesamt $p \sim a$ oder $p \sim b$. Dementsprechend gilt $b \in R^\times$ oder $a \in R^\times$ gemäß Lemma 8.3. □

Die Umkehrung von Lemma 8.5 braucht nicht zu gelten: man kann sich beispielsweise überlegen, dass im Ring

$$\mathbb{Z}[\mathrm{i}\sqrt{5}] = \{\, a + \mathrm{i}\sqrt{5}b : a, b \in \mathbb{Z} \,\}$$

die Zahl 2 irreduzibel aber nicht prim ist; man hat nämlich eine Zerlegung

$$2 \cdot 3 = 6 = (1 + \mathrm{i}\sqrt{5}) \cdot (1 - \mathrm{i}\sqrt{5}),$$

aber weder $1 + \mathrm{i}\sqrt{5}$ noch $1 - \mathrm{i}\sqrt{5}$ ist durch 2 teilbar (siehe Aufgabe T12.1 und beachte Aufgabe 9.4).

8.3. Faktorielle Ringe

Ein Integritätsbereich R heißt ***faktoriell*** oder ***ZPE-Ring*** (gedacht als Merkhilfe für „Zerlegung–Primzahlen–Existenz/Eindeutig“, im Englischen ***ufd*** für „***unique factorisation domain***“), falls jedes Element von $R \setminus (R^\times \cup \{0_R\})$ ein Produkt von endlich vielen irreduziblen Elementen ist und diese Darstellung „im Wesentlichen“ eindeutig ist, d.h. für je zwei Zerlegungen

$$a_1 \cdots a_n = b_1 \cdots b_m$$

mit *irreduziblen* Faktoren folgt stets $n = m$ (d.h. gleiche Länge) und $a_i \sim b_{\sigma(i)}$ für eine geeignete Permutation $\sigma \in \mathfrak{S}_n$ (d.h. Eindeutigkeit der Faktoren bis auf Umordnung).

Beispiel 8.6 ($\mathbb{Z}$ ist faktoriell)**.** Aus der bereits bewiesenen eindeutigen Primfaktorzerlegung in $\mathbb{N}$ (siehe Seite 101) ergibt sich leicht, dass $\mathbb{Z}$ ein faktorieller Ring ist, da ja jede negative ganze Zahl assoziiert zu ihrem Betrag ist. (Alternativ folgt dies aus Korollar 8.12, da $\mathbb{Z}$ gemäß Beispiel 8.1 (1) euklidisch ist.) Durch $2 \cdot 3 = (-3) \cdot (-2)$ sind zwei Zerlegungen von 6 in irreduzible Faktoren gegeben.

Satz 8.7 (Charakterisierung faktorieller Ringe)**.** *R sei ein Integritätsbereich. Dann sind die folgenden Aussagen äquivalent:*

(1) R ist faktoriell.

(2) Es gelten:

*(a) **Teilerkettenbedingung**: jede aufsteigende Folge $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots$ von Hauptidealen **wird stationär**, d.h. es existiert ein $k \in \mathbb{N}$ mit $\langle a_{k+j} \rangle = \langle a_k \rangle$ für alle $j \in \mathbb{N}_0$.*

*(b) **Primbedingung**: jedes irreduzible Element von R ist prim.*

(3) Jedes Element von $R \setminus (R^\times \cup \{0_R\})$ ist ein Produkt von Primelementen.

Beweis. „(1)⇒(2)“: R sei faktoriell. Sei $a \in R \setminus \{0_R\}$. Wir zeigen zunächst, dass $\langle a \rangle$ überhaupt nur von endlich vielen Hauptidealen von R enthalten wird. Dies impliziert dann insbesondere die *Teilerkettenbedingung*. Offenbar dürfen wir $a \notin R^\times$ annehmen, da sonst $\langle a \rangle = R$ überhaupt nur von dem Ideal $\langle 1 \rangle = R$ enthalten wird. Sei $a = \prod_i p_i$ eine Zerlegung von a in irreduzible Elemente p_i. Ist $\langle b \rangle$ ein Hauptideal, welches $\langle a \rangle$ enthält, so ist $a = bc$ für ein $c \in R$. O.B.d.A. sei $\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$. Dann folgt $b, c \notin R^\times \cup \{0_R\}$ und durch Zerlegung von b und c in irreduzible Faktoren, $b = \prod_j q_j$, $c = \prod_k q'_k$, folgt dann $a = \left(\prod_j q_j\right) \prod_k q'_k$. Da R faktoriell ist, müssen die q_j also assoziiert zu geeignet ausgewählten p_i aus der eingangs gewählten Zerlegung von a sein. Es folgt, dass sich b als Produkt einer Einheit und einer geeigneten Auswahl der p_i schreiben lässt. Die Anzahl der so generierbaren Hauptideale ist allerdings offensichtlich endlich. (Achtung: die Menge der bs muss allerdings i.Allg. nicht endlich sein, was mit der möglichen Existenz unendlich vieler Einheiten zusammenhängt.)
Nun zur *Primbedingung*: $p \in R$ sei irreduzibel und es gelte $p \mid ab$ mit geeigneten $a, b \in R$, also $ab = cp$ für ein $c \in R$. Ist $a \in R^\times$ oder $b \in R^\times$, so folgt $p \mid b$ bzw. $p \mid a$. Ist $c \in R^\times$, so folgt $p \mid a$ oder $p \mid b$ wegen der Irreduzibilität von p. Anderenfalls folgt

(mit der Notation für Zerlegungen von oben)

$$\left(\prod_i p_i\right)\prod_j q_j = ab = pc = p\prod_k q'_k.$$

Insbesondere ist $p \sim p_i$ oder $p \sim q_j$ für ein p_i oder ein q_j und es folgt $p \mid a$ bzw. $p \mid b$.

„(2)⇒(3)“: Dank der Primbedingung genügt es zu zeigen, dass sich jedes Element r von $R \setminus (R^\times \cup \{0_R\})$ als Produkt von irreduziblen Elementen schreiben lässt. Angenommen, letzteres wäre nicht erfüllt und $a_1 \in R \setminus (R^\times \cup \{0_R\})$ nicht Produkt von irreduziblen Elementen. Dann muss a_1 reduzibel sein. Wir können also $a_1 = ab$ mit Nicht-Einheiten a und b schreiben. Von diesen können nicht beide ein Produkt von irreduziblen Elementen sein, da sich dies sonst auf a_1 übertrüge. Sei nun $a_2 \in \{a, b\}$ kein Produkt von irreduziblen Elementen. Wir haben $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$, ja sogar $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$, denn anderenfalls wären a_1 und a_2 assoziiert, was aber $a, b \notin R^\times$ widerspricht. Man verfährt nun mit a_2 analog wie mit a_1 und gewinnt so ein Element a_3 mit $\mathfrak{a}_2 \subsetneq \mathfrak{a}_3$. Induktiv erhält man so eine Kette $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \ldots$, welche nie stationär wird. Dies widerspricht jedoch der Teilerkettenbedingung. Also muss a_1 doch ein Produkt von irreduziblen Elementen sein.

„(3)⇒(1)“: Dank Lemma 8.5 sind die Primelemente von R irreduzibel. Aus (3) erhalten wir also schon mal die Zerlegbarkeit jedes Elements r von $R \setminus (R^\times \cup \{0_R\})$ in irreduzible Elemente. Es verbleibt lediglich die Eindeutigkeit einer solchen Zerlegung zu zeigen. Seien daher $p_1 \cdots p_n = q_1 \cdots q_m$ zwei Zerlegungen in irreduzible Elemente, wobei die p_i zusätzlich noch als prim angenommen seien. Wir führen eine Induktion über n. Für $n = 1$ folgt $p_1 = q_1(q_2 \cdots q_m)$. Wegen der Irreduzibilität von p_1 folgt $q_1 \in R^\times$ oder $q_2 \cdots q_m \in R^\times$. Da q_1 irreduzibel ist, ist der erste Fall ausgeschlossen und wir haben $q_2 \cdots q_m \in R^\times$. Dann müssten aber auch alle hier beteiligten Faktoren Einheiten sein; das liefert nur dann keinen Widerspruch zur Irreduzibilität von q_2, wenn überhaupt schon $m = 1$ ist und das Produkt $q_2 \cdots q_m$ leer ist. Dann ist also $p_1 = q_1$. Nun zum Induktionsschritt. Es sei wieder $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ für ein $n \geq 2$. Da p_1 prim ist, folgt $p_1 \mid q_j$ für ein j. O.B.d.A. sei $j = 1$. Aus der Irreduzibilität von q_1 folgt dann $p_1 \sim q_1$. Da der eben geführte Induktionsanfang auch für $m = 1$ funktioniert (die Primalität der p_i wurde dort nicht benutzt), dürfen wir $m \geq 2$ annehmen und dürfen nach etwaigem „Umschaufeln“ einer Einheit von q_1 auf q_2 von $p_1 = q_1$ ausgehen. Dann folgt

$$p_1(p_2 \cdots p_n - q_2 \cdots q_m) = 0_R$$

und also $p_2 \cdots p_n = q_2 \cdots q_m$, da R ein Integritätsbereich ist, aber $p_1 \neq 0_R$ gilt. Die Induktionsvoraussetzung liefert nun die Behauptung. □

Bemerkung. Die Implikation „(2)⇒(1)“ in Satz 8.7 benutzen wir für den Beweis von Korollar 8.12 (siehe unten). Die Implikation „(3)⇒(1)“ in Satz 8.7 benutzen wir später beim Beweis eines Satzes von Gauß über die Faktorialität vom Polynomringen $R[X]$ über einem faktoriellen Ring R (Satz 9.6).

Unser nächstes Ziel ist es einzusehen, dass Hauptidealbereiche faktoriell sind. Das ist die Aussage von Korollar 8.12 (siehe unten). Als Vorarbeit dazu beweisen wir

im Rest dieses Abschnittes noch, dass Hauptidealbereiche der Primbedingung aus Satz 8.7 (2b) genügen (siehe Korollar 8.9). Dies folgt aus dem nächsten Ergebnis, welches auch für sich genommen von Interesse ist:

Proposition 8.8. *R sei ein Hauptidealbereich. Für jedes irreduzible Element $p \in R$ ist pR ein maximales Ideal von R.*

Beweis. Es sei $p \in R$ irreduzibel und $\mathfrak{a}$ ein Ideal, welches pR enthält. Da R ein Hauptidealbereich ist, gibt es $a \in R$ mit $aR = \mathfrak{a} \ni p$ und es folgt weiter $p = ab$ für ein $b \in R$. Da p irreduzibel ist, gilt $a \in R^\times$ oder $b \in R^\times$, also $\mathfrak{a} = R$ bzw. $\mathfrak{a} = pR$. Also ist pR maximal. □

Korollar 8.9. *In einem Hauptidealbereich sind die irreduziblen Elemente genau die Primelemente.*

Beweis. R sei ein Hauptidealbereich. Laut Lemma 8.5 sind alle Primelemente von R auch irreduzibel. Umgekehrt erzeugt laut Proposition 8.8 jedes irreduzible Element $p \in R$ ein maximales Ideal in R und Aufgabe 10.3 (b) zeigt, dass $\langle p \rangle$ ein Primideal ist. Also ist p prim. □

8.4. Noethersche Ringe

Unter Hauptziel ist es, nachzuweisen, dass gewisse Ringe faktoriell sind. Die Teilerkettenbedingung aus Satz 8.7 (2a) motiviert die folgende Definition: eine Menge S mit partieller Ordnung $\leq$ heißt ***noethersch***, falls jede nichtleere Teilmenge X von S ein maximales Element $m \in X$ besitzt (d.h. aus $m \leq x \in X$ folgt $m = x$, wobei nicht gefordert ist, dass m mit jedem Element aus X vergleichbar sein muss).

Ein kommutativer Ring heißt ***noethersch***, falls die Menge seiner Ideale zusammen mit der durch die Inklusion $\subseteq$ gestiftete partielle Ordnung noethersch ist.

Bemerkung (Warnung: „$m \in X$“ vs. „$m \in S$“)**.** In der Definition von „noethersch“ ist die leicht zu überlesende Forderung „$m \in X$“ für das[1] maximale Element m von $X \subseteq S$ dessen Existenz behauptet wird, ist wichtig. Hätte man etwa nur „$m \in S$“ gefordert, so wäre der Begriff eines noetherschen Rings trivial(!): Jedes Ideal $\mathfrak{a}$ eines Rings R wird durch das triviale Ideal $\langle 1_R \rangle = R$ nach oben beschränkt: $\mathfrak{a} \subseteq \langle 1_R \rangle$. Insbesondere hat also jede Menge S von Idealen von R ein maximales Element in der Menge *aller* Ideale von R. Wir sehen aber später noch Beispiele für nicht-noethersche Ringe.

Lemma 8.10. *Eine Menge S mit partieller Ordnung $\leq$ ist genau dann noethersch, wenn jede Kette $s_1 \leq s_2 \leq s_3 \leq \ldots$ von Elementen aus S stationär wird, also $s_n = s_m$ für einen Index $n \in \mathbb{N}$ und alle $m \geq n$ erfüllt.*

Beweis. Ist $(S, \leq)$ noethersch, so besitzt jede Kette $s_1 \leq s_2 \leq s_3 \leq \ldots$ ein maximales Element s_n und ab diesem gilt dann notwendigerweise Gleichheit.

[1] Achtung: Maximale Elemente brauchen nicht eindeutig zu sein, aber der unbestimmte Artikel wirkt sprachlich leider auch unpassend.

Nun gelte die obige Kettenbedingung und $X \subseteq S$ sei nicht leer. Wir wählen $x_1 \in X$ und konstruieren induktiv eine Kette $x_1 \leq x_2 \leq \ldots$; ist x_k schon konstruiert, so wähle ein beliebiges Element $x_{k+1} \in X$ mit $x_k \lneq x_{k+1}$, falls dies möglich ist und $x_{k+1} := x_k$ sonst. Da die soeben konstruierte Kette nach Voraussetzung schließlich konstant ist, muss x_n für ein geeignetes n maximal in X sein. Also ist $(S, \leq)$ noethersch. □

Das nächste Beispiel zeigt, dass der Begriff der noetherschen partiell geordneten Mengen in gewisser Weise die Dimensionstheorie von Vektorräumen verallgemeinert. Man mag die Eigenschaft eines Rings noethersch zu sein also gewissermaßen mit Endlichdimensionalität bei Vektorräumen vergleichen. (Tatsächlich gibt es beispielsweise einen auf Krull zurückgehenden Dimensionsbegriff für Ringe, der über Längen von aufsteigenden Ketten von Primidealen definiert wird, aber derartige Betrachtungen würden uns zu weit führen.)

Beispiel (Dimension von Vektorräumen)**.** Sei S die Menge der Unterräume eines Vektorraums V. Diese Menge ist bezüglich der mengentheoretischen Inklusion partiell geordnet. Man kann sehen, dass S genau dann noethersch ist, wenn V endlichdimensional ist. In der Tat, ist V unendlich-dimensional, so gibt es linear unabhängige Vektoren $b_1, b_2, b_3, \ldots \in V$ und durch

$$\operatorname{span}\{b_1\} \subsetneq \operatorname{span}\{b_1, b_2\} \subsetneq \operatorname{span}\{b_1, b_2, b_3\} \subsetneq \ldots$$

erhält man eine nicht-stationär-werdende Kette, wodurch sich S als nicht noethersch erweist (Lemma 8.10). Ist umgekehrt V endlich-dimensional, so muss jede Kette $U_1 \subseteq U_2 \subseteq \ldots$ in S schlussendlich stationär werden, denn bei jedem Schritt $U_n \subsetneq U_{n+1}$ gilt $\dim U_{n+1} \geq (\dim U_n) + 1$, aber alle auftretenden Dimensionen sind durch die Vektorraumdimension $\dim V < \infty$ von V beschränkt. In der fraglichen Kette kann es also höchstens $\dim V$ viele „$\subsetneq$“-Schritte geben und danach ist die Kette stationär. Tatsächlich ist

$$\dim V = \sup\{\, n \in \mathbb{N}_0 : \exists \text{Kette } U_0 \subsetneq U_1 \subsetneq \ldots \subsetneq U_n \text{ in } S \,\}.$$

Bemerkung. Auf Seite 88 hatten wir bereits den Begriff eines „R-Moduls“ (über einem Ring R) angerissen und erwähnt, dass diese einerseits den aus § 2.3 bekannten „Operationsbegriff“ aus der Gruppentheorie verallgemeinern und falls der Ring R ein Körper ist, mit dem aus der *linearen Algebra* bekannten Vektorraumbegriff übereinstimmen. Genau so, wie jeder Körper K ein (eindimensionaler) Vektorraum über sich selbst darstellt, kann man auch jeden Ring R als Modul über sich selbst auffassen. Zwar hat der eindimensionale K-Vektorraum K lediglich die beiden trivialen Unterräume ($\{0_K\}$ und K selbst), doch kann ein Ring R als R-Modul aufgefasst durchaus sehr viele „Untermoduln“ enthalten. (Den Begriff des „Untermoduls“ wollen wir hier nicht definieren.) Es stellt sich heraus, dass die *Untermoduln von R* genau die *Ideale von R* sind.

Satz 8.11. *Ein kommutativer Ring ist genau dann noethersch, wenn jedes seiner Ideale endlich erzeugt ist.*

Beweis. Sei R noethersch und $\mathfrak{a}$ ein Ideal. Man wähle nun ein maximales Element $\mathfrak{b}$ in der Menge der in $\mathfrak{a}$ enthaltenen, endlich erzeugten Ideale. Für jedes $a \in \mathfrak{a}$ ist dann $\langle \mathfrak{b} \cup \{a\} \rangle \subseteq \mathfrak{b} \subseteq \mathfrak{a}$ und darum $\mathfrak{b} = \mathfrak{a}$. Das zeigt, dass $\mathfrak{a}$ endlich erzeugt ist.

Sei nun umgekehrt jedes Ideal von R endlich erzeugt und $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ eine Kette von Idealen. Dann ist auch $\bigcup_i \mathfrak{a}_i$ endlich erzeugt, etwa von $x_1, \ldots, x_n$. Da es ein $n \in \mathbb{N}$ mit $x_1, \ldots, x_n \in \mathfrak{a}_n$ gibt, sieht man, dass die betrachtete Kette ab dem Index n stationär ist. Lemma 8.10 zeigt nun, dass R noethersch ist. □

Korollar 8.12. *Hauptidealbereiche sind faktoriell. Insbesondere sind euklidische Ringe faktoriell.*

Beweis. Da laut Satz 8.2 alle euklidischen Ringe auch Hauptidealbereiche sind, folgt die zweite Aussage des Korollars aus der ersten. Andererseits ist in einem Hauptidealbereich natürlich jedes Ideal endlich erzeugt, nämlich sogar von *einem* Element. Satz 8.11 liefert, dass Hauptidealbereiche noethersch sind. Dies garantiert die Teilerkettenbedingung in Satz 8.7 (2). Korollar 8.9 garantiert aber auch die Primbedingung. Also liefert Satz 8.7, dass Hauptidealbereiche faktoriell sind. □

Der Hilbertsche Basissatz (Satz 8.13 in § 8.5) liefert eine Vielzahl von noetherschen Ringen. Wir geben hier zwei Beispiele für nicht-noethersche Ringe:

Beispiel. Der Ring $R = \prod_{\mathbb{N}} \mathbb{Z}$, welcher auch als Ring der Funktionen $\mathbb{N} \to \mathbb{Z}$ betrachtet werden kann, ist *nicht noethersch*: Wir definieren Ideale durch

$$\mathfrak{a}_i = \{ (c_n)_n \in R : c_i = 0 \text{ für alle } n \geq i \}.$$

Im Hinblick auf

$$(0, \ldots, 0, \underbrace{1}_{(i\text{-te Stelle})}, 0, \ldots) \in \mathfrak{a}_{i+1} \setminus \mathfrak{a}_i$$

erkennen wir $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \ldots$ als eine aufsteigende Folge von Idealen, die nicht stationär wird. Man beachte auch, dass R *kein Integritätsbereich* ist:

$$(1, 0, 0, \ldots) \cdot (0, 1, 0, \ldots) = (0, 0, 0, \ldots) = 0_R.$$

Integritätsbereiche brauchen im Allgemeinen auch nicht noethersch zu sein, wie das folgende Beispiel belegt:

Beispiel. Auf Seite 131 haben wir den Ring $R = \mathbb{Z}[\sqrt{-5}]$ erwähnt, in welchem 2 irreduzibel, aber nicht prim ist (siehe Aufgabe T12.1). Insbesondere ist R nicht faktoriell (siehe Satz 8.7). Sei nun $\boldsymbol{X} = \{X_n : n \in \mathbb{N}\}$ eine abzählbare Menge von Variablen. Der Polynomring $R[\boldsymbol{X}]$ ist demnach nicht faktoriell, aber auch nicht noethersch, denn

$$\langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \langle X_1, X_2, X_3 \rangle \subsetneq \ldots$$

ist eine aufsteigende, nie stationär werdende, Kette von Idealen von $R[\boldsymbol{X}]$. Da R ein Integritätsbereich ist, handelt es sich bei $R[\boldsymbol{X}]$ auch um einen Integritätsbereich.

8.5. Hilbertscher Basissatz

Wir zeigen später, dass der Polynomring $R[X_1,\dots,X_n]$ in endlich vielen Variablen über einem faktoriellen Ring R auch wieder faktoriell ist (Korollar 9.7). Man beachte, dass dieser ab zwei Variablen kein Hauptidealring ist: $\langle X,Y\rangle \subseteq R[X,Y]$ ist kein Hauptideal. Man kann also nicht mittels Korollar 8.12 schließen.

Als faktorieller Ring $R[X_1,\dots,X_n]$ erfüllt $R[X_1,\dots,X_n]$ natürlich auch die Teilerkettenbedingung aus Satz 8.7 (2). Wir zeigen hier eine verwandte Aussage.

Satz 8.13 (Hilbertscher Basissatz, I). *Der Polynomring $R[X]$ über einem noetherschen Ring ist selbst noethersch.*

Beweis. Gemäß Satz 8.11 genügt es zu zeigen, dess jedes Ideal $\mathfrak{A}$ von $R[X]$ endlich erzeugt ist. Wir gehen zwecks der Erzeugung eines Widerspruchs davon aus, dass es doch ein Ideal $\mathfrak{A}$ von $R[X]$ gibt, welches *nicht* endlich erzeugt ist. Dann ist natürlich $\mathfrak{A} \neq \{0_{R[X]}\}$ und überdies können wir für $i = 1,2,\dots$ induktiv ein Element f_i mit minimalem Grad in $\mathfrak{A} \setminus \langle f_j : j < i\rangle$ wählen.[2] Da $\mathfrak{A}$ laut Annahme nicht endlich erzeugt ist, ist stets $\mathfrak{A} \setminus \langle f_j : j < i\rangle \neq \emptyset$, weswegen die Wahl von f_i immer möglich ist. Es bezeichne a_i den Leitkoeffizienten von f_i. Da R noethersch ist, ist das Ideal $\mathfrak{a} = \langle a_i : i \in \mathbb{N}\rangle$ endlich erzeugt; wir haben also $\mathfrak{a} = \langle a_i : i \neq n\rangle$ für ein $n \in \mathbb{N}$. Nun ist

$$a_{n+1} \in \langle a_i : i \in \mathbb{N}\rangle = \mathfrak{a} = \langle a_i : i \neq n\rangle,$$

weswegen es Elemente $r_1,\dots,r_n \in R$ mit $a_{n+1} = r_1a_1 + \dots + r_na_n$ gibt. Dann handelt es sich bei dem Polynom

$$g = f_{n+1} - \sum_{i\leq n} r_i X^{\deg f_{n+1} - \deg f_i} f_i$$

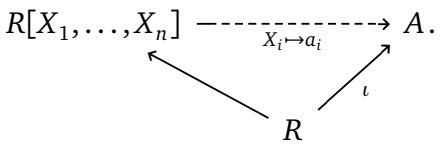
aber um ein Element von $\mathfrak{A}$ mit kleinerem Grad als f_{n+1}, welches nicht in $\langle f_1,\dots,f_n\rangle$ liegen kann (da sonst auch f_{n+1} in diesem Ideal läge, entgegen der Wahl von f_{n+1}). Dies widerspricht der Wahl von f_{n+1}. □

Bemerkung. Das Wort „Basis“ im Namen des Hilbertschen Basissatz rührt von einem älteren Gebrauch dieses Begriffes her und soll hier so viel wie „Erzeugendensystem“ heißen; der Basissatz besagt ja gemäß Satz 8.11 genau, dass alle Ideale des Polynomrings $R[X]$ über einem noetherschen Ring R endlich erzeugt sind. Für eine konzise Beschreibung der historischen Umstände, aus welchen der Hilbertsche Basissatz erwuchs, sei das schöne Buch von Eisenbud [17, insbes. I.1] empfohlen.

Ist $\iota\colon R \to A$ ein Homomorphismus zwischen kommutativen Ringen und $M \subseteq A$ eine beliebige Teilmenge, so schreibt man $R[M]$ für den kleinsten Teilring von A, der $\iota(R) \cup M$ enthält. Man nennt $\iota\colon R \to A$ eine ***R-Algebra***. Falls ι aus dem Kontext klar ist, bezeichnet man auch A selbst salopp als eine R-Algebra. Eine R-Algebra A heißt ***endlich erzeugt*** (oder von ***endlichem Typ***), falls $A = R[M]$ für eine *endliche*

[2] Wichtiger Spezialfall für die Wahl von f_1: $\langle f_j : j < 1\rangle = \langle\emptyset\rangle = \{0_{R[X]}\}$.

Teilmenge $M \subseteq A$ gilt. Schreibt man $M = \{a_1, \ldots, a_n\}$, so erhält man einen surjektiven Ringhomomorphismus vom Polynomring $R[X_1, \ldots, X_n]$ auf A, der das folgende Diagramm kommutativ macht (siehe Aufgabe T11.2):



Der erste Isomorphiesatz (Korollar 6.8) zeigt nun $A \cong R[X_1, \ldots, X_n]/\mathfrak{a}$ für ein geeignetes Ideal $\mathfrak{a}$ von $R[X_1, \ldots, X_n]$. Der Korrespondenzsatz (Satz 6.9) liefert dann, dass die Ideale von A in inklusionserhaltender Weise zu den $\mathfrak{a}$-enthaltenden Idealen von $R[X_1, \ldots, X_n]$ korrespondieren. Da wir

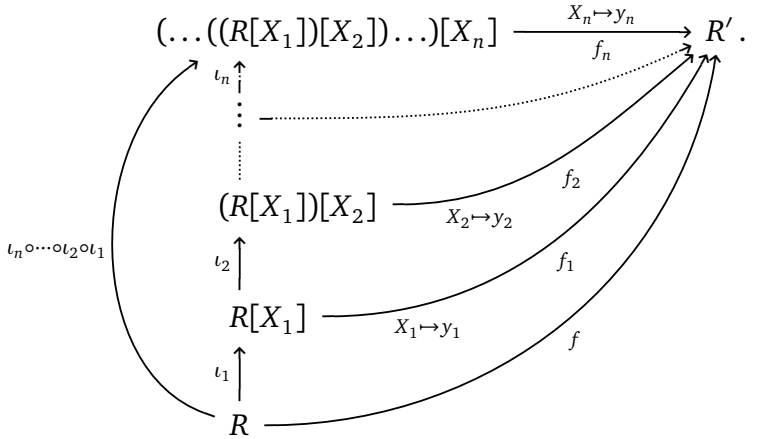
$$R[X_1, X_2, \ldots, X_n] \cong (\ldots((R[X_1])[X_2])\ldots)[X_n] \tag{8.2}$$

mittels induktiver Anwendung von Satz 8.13 als noethersch erkennen, sehen wir auch, dass A noethersch ist. (Den Beweis von (8.2) holen wir gleich im Anschluss nach.) Damit ergibt sich die folgende Verallgemeinerung von Satz 8.13:

Satz 8.14 (Hilbertscher Basissatz, II). *Sei R ein noetherscher Ring. Dann sind auch alle endlich erzeugten R-Algebren noethersch.*

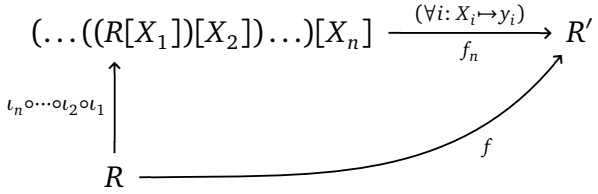
Zum Beweis von (8.2) beachte man, dass die rechte Seite von (8.2) die universelle Eigenschaft des Polynomrings in n Variablen erfüllt. (Siehe Satz 7.4 für den univariaten Fall, Aufgabe T11.2 für den multivariaten Fall.) Die offensichtliche Verallgemeinerung von Aufgabe 12.1 auf den multivariaten Fall liefert dann (8.2). (Beachte, dass der in den Übungen besprochene Beweis von Aufgabe 12.1 problemlos auch den multivariaten Fall abdeckt.) Nun zum Nachweis der universellen Eigenschaft. Gegeben einen Ringhomomorphismus $f : R \to R'$ und Elemente $y_1, \ldots, y_n \in R$, erhält man durch sukzessive Anwendung von Satz 7.4 Ringhomomorphismen $f_1, f_2, \ldots, f_n$, die das folgende Diagramm kommutativ machen:

(8.3)



Nun gilt aber $f_n(X_i) = y_i$ für $i = 1, 2, \ldots, n$. Umgekehrt ist aber f_n auch der einzige Ringhomomorphismus, der diese Abbildungseigenschaft besitzt und das Diagramm

(8.4)



kommutativ macht, denn aus f_n erhält man induktiv

$$f_{n-1} = f_n \circ \iota_n, \quad \ldots, \quad f_2 = f_3 \circ \iota_3, \quad f_1 = f_2 \circ \iota_2, \quad f = f_1 \circ \iota_1.$$

Der Eindeutigkeitsteil in Satz 7.4 und $f_1(X_1) = (f_n \circ \iota_n \circ \cdots \circ \iota_2)(X_1) = y_1$ zeigen, dass f_1 schon wie in (8.3) aus f entstanden ist und induktiv folgt, dass f_n in (8.4) mit f_n aus (8.3) übereinstimmt.

KAPITEL 9

Teilbarkeit in Polynomringen

In diesem Kapitel untersuchen wir die Teilbarkeitslehre in Polynomringen $R[X]$ über einem *faktoriellen* Ring R. (Insbesondere ist R ein Integritätsbereich.) Bezeichnet $K = \mathrm{Quot}(R)$ den Quotientenkörper von R, wobei wir die kanonische Einbettung $R \to K$ zur Inklusion $R \subseteq K$ erheben wollen, so zeigt sich, dass die Teilbarkeitslehre in $K[X]$ viel mit der Teilbarkeitslehre in $R[X]$ zu tun hat:

$$\begin{array}{ccccc} \text{(Faktoriell? — Ja! Satz 9.6.)}\ R[X] & & \xhookrightarrow{\text{Inkl.}} & & K[X]\ \text{(Faktoriell, da euklidisch.)} \\ \Big\uparrow{\scriptstyle \text{Inkl.}} & & & & \Big\uparrow{\scriptstyle \text{Inkl.}} \\ \text{(Faktoriell, laut Annahme.)}\ R & \xhookrightarrow{\text{Inkl.}} & \mathrm{Quot}(R) & = & K\,. \quad \text{(Faktoriell, da Körper.)} \end{array} \tag{9.1}$$

Vermöge der zusätzlichen Reichhaltigkeit an Einheiten in K (ggf. sehr konträr zur Situation in R) erweist sich $K[X]$ als *euklidisch* (Beispiel 8.1), somit als Hauptidealbereich (Satz 8.2), und folglich als faktoriell (Korollar 8.12). Daraus erwächst die Hoffnung, dass man die Faktorialität von $K[X]$ benutzen kann, um etwas über die Teilbarkeit in $R[X]$ zu lernen. Diese Hoffnung wird durch den weiter unten besprochenen ***Satz von Gauß*** (Satz 9.6) bestätigt.

Im darauf folgenden Abschnitt zeigen wir, dass sich obiges Kredo auch umdrehen lässt: man kann die Teilbarkeit in R benutzen, um etwas über die Teilbarkeit in $K[X]$ zu lernen! So wie K sich durch Reichhaltigkeit an Einheiten auszeichnet, liegt in R dafür ggf. eine gewisse Reichhaltigkeit an Idealen $\mathfrak{a}$ vor. (Man beachte, dass der Körper K natürlich ein einfacher Ring ist und als solcher nur die beiden trivialen Ideale $\{0_K\}, K \trianglelefteq K$ besitzt.) Wegen $R[X]/\mathfrak{a}R[X] \cong (R/\mathfrak{a})[X]$, lässt sich Teilbarkeit in $R[X]$ zu Teilbarkeit in $(R/\mathfrak{a})[X]$ transportieren. Ist der Ring $R/\mathfrak{a}$ deutlich verständlicher als R, so liefert dies unter Umständen nützliche Information, die man auch zurücktransportieren kann. Die Hauptergebnisse dieser Überlegungen sind das ***Reduktionskriterium*** (Proposition 9.11) und das ***Irreduzibilitätskriterium von Schönemann–Eisenstein*** (Korollar 9.12). Anwendungen der Irreduzibilitätskriterien folgen in Kapitel 11 und sind fundamental für das vertiefende Studium der Körpertheorie in der Vorlesung *Algebra*.

Unsere Darstellung folgt dem exzellenten Buch von Bosch [6, §§ 2.8–2.9], worin den Primidealen von R eine zentrale Rolle eingeräumt wird. Für andere Darstellungen konsultiere man etwa Lang [37, Chapter IV, §§ 2–3] oder Aluffi [2, Chapter V, §§ 4–5]; dort wird mittels des Begriffs des „Inhalts“ eines Polynoms der Effekt von den

lokalen Bewertungen $v_p(\cdot)$, die wir weiter unten studieren, gebündelt. Das macht die Argumente etwas kürzer, aber vielleicht vergleichsweise mysteriöser.

9.1. Produktdarstellung in Quotientenkörpern

Das folgende Beispiel steht im Mittelpunkt unserer Untersuchungen (siehe den Zusatz in Satz 9.6):

Beispiel. Das Polynom $f = 2X \in \mathbb{Q}[X]$ ist irreduzibel, aber nicht irreduzibel, wenn man es als Polynom in $\mathbb{Z}[X]$ auffasst: dort sind nämlich 2 und X jeweils irreduzibel und deren Produkt $2 \cdot X = f$ daher nicht.

Im Folgenden sei R stets ein faktorieller Ring und K sein Quotientenkörper. Die kanonische Einbettung $R \to K$ betrachten wir als Teilmengeninklusion, d.h. wir schreiben statt $\frac{r}{1_R} \in K$ nur r. Für $r \in R \setminus \{0_R\}$ ist dann $r^{-1} = \frac{1_R}{r}$ in K wohl-definiert. Mit $\mathscr{P} \subseteq R \subseteq K$ bezeichnen wir ein ***vollständiges System von paarweise nicht-assoziierten Primelementen***; „vollständig“ bedeutet hier, dass jedes Primelement von R assoziiert zu einem Element von $\mathscr{P}$ ist.

Beispiel. Für $R = \mathbb{Z}$ sind die Primelemente genau $\pm p$ mit Primzahlen p. Kanonischer Weise wählt man als $\mathscr{P}$ hier die Menge der Primzahlen.

Proposition 9.1 (Produktdarstellung von Elementen in Quotientenkörpern)**.** *Es seien $R \subseteq K$ wie in (9.1) und Dann hat jedes Element $x \in K \setminus \{0_K\}$ eine eindeutige Darstellung als Produkt*

$$x = \epsilon(x) \prod_{p \in \mathscr{P}} p^{v_p(x)}$$

mit einer Einheit $\epsilon(x) \in R^\times$, welche von der Wahl von $\mathscr{P}$ abhängen kann, und Exponenten $v_p(x) \in \mathbb{Z}$, wobei $v_p(x) = 0$ für fast alle $p \in \mathscr{P}$ gilt. Ferner ist x genau dann ein Element von R wenn alle $v_p(x) \geq 0$ sind und überdies genau dann eine Einheit von R, wenn stets $v_p(x) = 0$ gilt.

Beweis. Zunächst zeigen wir, dass jede Darstellung der obigen Form *eindeutig* ist. In der Tat, sind durch

$$\epsilon \cdot \prod_{p \in \mathscr{P}} p^{v_p} = \varepsilon \cdot \prod_{p \in \mathscr{P}} p^{\upsilon_p},$$

zwei derartige Darstellungen derselben Zahl gegeben, so gilt es $v_p = \upsilon_p$ für alle $p \in \mathscr{P}$ und $\epsilon = \varepsilon$ einzusehen. Hierfür bringen wir alle Faktoren mit negativen Exponenten auf die jeweils andere Seite, und erhalten somit eine Gleichung in R:

$$\epsilon \cdot \Big(\prod_{\substack{p \in \mathscr{P} \\ v_p \geq 0}} p^{v_p} \Big) \cdot \prod_{\substack{p \in \mathscr{P} \\ \upsilon_p < 0}} p^{-\upsilon_p} = \varepsilon \cdot \Big(\prod_{\substack{p \in \mathscr{P} \\ \upsilon_p \geq 0}} p^{\upsilon_p} \Big) \cdot \prod_{\substack{p \in \mathscr{P} \\ v_p < 0}} p^{-v_p}.$$

Man beachte, dass in dieser Gleichung alle auftretenden Exponenten nicht-negativ sind. Die Faktorialität von R liefert

$$\max\{0, v_p\} + \max\{0, -\upsilon_p\} = \max\{0, \upsilon_p\} + \max\{0, -v_p\}.$$

Durch eine Fallunterscheidung lösen wir nun die auftretenden Maxima auf und erhalten so:

$$\begin{cases} \nu_p + 0 = \upsilon_p + 0, & \text{falls } \nu_p \geq 0 \text{ und } \upsilon_p \geq 0, \\ 0 + 0 = \upsilon_p - \nu_p, & \text{falls } \nu_p < 0 \text{ und } \upsilon_p \geq 0, \\ \nu_p - \upsilon_p = 0 + 0, & \text{falls } \nu_p \geq 0 \text{ und } \upsilon_p < 0, \\ 0 - \upsilon_p = 0 - \nu_p, & \text{falls } \nu_p < 0 \text{ und } \upsilon_p < 0. \end{cases}$$

Die mittleren beiden Fälle erweisen sich als widersprüchlich, während die äußeren beiden Fälle $\nu_p = \upsilon_p$ implizieren. Dies zeigt $\nu_p = \upsilon_p$ und somit auch $\epsilon = \varepsilon$.

Nun zur *Existenz*: ist $x \in R^\times$, so kann man $\epsilon(x) = x$ und $\nu_p(x) = 0$ für alle p wählen. Nach Satz 8.7 (3) hat jedes $x \in R \setminus (R^\times \cup \{0_R\})$ eine Produktdarstellung als Produkt von Primelementen. Zu jedem Primelement p' gibt es ein assoziiertes Primelement $p \in \mathscr{P}$, also $p' = up$ mit einer Einheit $u \in R^\times$. Das Produkt über die us liefert $\epsilon(x)$, während Sammeln gleicher p-Faktoren $p^{\nu_p(x)}$ liefert. Insbesondere sind alle $\nu_p(x) \geq 0$ und umgekehrt liefert ein Produkt mit nicht-negativen $\nu_p(x)$ auch stets[1] ein Element von R, da hierbei ja alle Faktoren in R sind.

Ein beliebiges Element x von K schreibt sich nun als $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} = a \cdot s^{-1}$ mit $a, s \in R$. Durch Zerlegung von a und s kommt man an die gewünschte Produktzerlegung von x mit $\nu_p(x) = \nu_p(a) - \nu_p(s)$. □

Beispiel. In $R = \mathbb{Z} \subseteq \mathbb{Q} = K$ haben wir $\dfrac{12}{32} = \dfrac{2^2 \cdot 3}{2^5} = \dfrac{1}{2^3} \cdot \dfrac{3}{1} = 2^{-3} \cdot 3^1$.

Bemerkung. Auf die Einheit $\epsilon(x) \in R^\times$ in Proposition 9.1 kann im Allgemeinen nicht verzichtet werden. Das sieht man etwa, wenn man x selbst als Einheit von R wählt, aber auch für $x \notin R^\times$ können Probleme auftreten. In $\mathbb{Z}$ hat man beispielsweise $-9 = (-1)3^2 = (-1)(-3)^2$, aber -9 lässt sich nicht als $\prod_{p \in \mathscr{P}} p^{\nu_p(9)}$ (ohne vorangestellte Einheit) schreiben, denn dort müssten alle Exponenten bis auf den für $p \sim 3$ gleich 0 sein und der Exponent für das zu 3 assoziierte Primelement $p \in \mathscr{P}$ wäre gleich 2. Das geht aber nicht, da p^2 stets positiv ist und somit nicht gleich -9 sein kann. Man beachte auch, dass $\epsilon(x)$ sehr wohl von der Wahl von $\mathscr{P}$ abhängen kann. Wählt man $\mathscr{P} = \{2, 3, 5, \ldots\}$, so ist $-2 = (-1)2^1$ und also $\epsilon(-2) = -1$. Wählt man hingegen $\mathscr{P} = \{-2, \ldots\}$, so ist $-2 = (-2)^1$ und also $\epsilon(-2) = 1$.

9.2. Primitive Polynome

In Vorbereitung auf die zu Beginn des Kapitels angekündigten Resultate, ist unser Ziel in diesem Abschnitt, gewissermaßen Polynome in $K[X]$ in Polynomen in $R[X]$ zu verwandeln.

Sei $p \in \mathscr{P}$ ein Primelement von R. Wir setzen formal $\nu_p(0) := \infty$. Ferner folgt aus der Eindeutigkeitsaussage in Proposition 9.1 unmittelbar

$$\nu_p(xy) = \nu_p(x) + \nu_p(y) \quad \text{für alle } x, y \in K. \tag{9.2}$$

[1] Nach wie vor sei $\nu_p(x) = 0$ für fast alle p angenommen.

(Man sieht sofort, dass diese Formel auch noch gilt, wenn x oder y gleich 0_K sind; hier ist dann $\infty = \infty + k = k + \infty = \infty + \infty$ für alle $k \in \mathbb{Z}$.) Für Polynome $f = \sum_n a_n X^n \in K[X]$ schreiben wir

$$\nu_p(f) := \inf_n \nu_p(a_n).$$

Insbesondere ist $\nu_p(0_{K[X]}) = \infty$. Ferner definiert man auch $\nu_p(\cdot)$ für Primelemente $p \notin \mathscr{P}$ als $\nu_{p'}(\cdot)$ mit dem zu p assoziierten Primelement $p' \in \mathscr{P}$. Wir erwähnen noch, dass keine Verwechslungsgefahr zwischen dem eben definierten $\nu_p =: \nu_{p,R[X]}$ und dem in Proposition 9.1 definierten $\nu_p =: \nu_{p,R}$ besteht, denn offensichtlicher Weise gilt $\nu_{p,R[X]}(rX^0) = \nu_{p,R}(r)$ für alle $r \in R$.

Beispiel. Die folgenden Beispiele beziehen sich auf den Ring $\mathbb{Z}[X]$.

(1) $\nu_2(6X^2 + 20) = \min\{\nu_2(6), \nu_2(20)\} = \min\{1, 2\} = 1$,
(2) $\nu_3(6X^2 + 20) = \min\{\nu_3(6), \nu_3(20)\} = \min\{1, 0\} = 0$,
(3) $\nu_7(6X^2 + 20) = \ldots = 0$,
(4) $\nu_2(\frac{7}{8}X^9 + 4X) = \min\{\nu_2(\frac{7}{8}), \nu_2(4)\} = \min\{-3, 2\} = -3$.

Wir nennen ein Polynom $f \in R[X]$ ***normiert***, falls sein Leitkoeffizient gleich 1_R ist. Ein Polynom $f \in R[X]$ heißt ***primitiv***, falls $\nu_p(f) = 0$ für alle Primelemente p von R gilt. (Äquivalent: 1_R ist größter gemeinsamer Teiler der Koeffizienten von f.) Tritt 1_R als Koeffizient von f auf, so ist f natürlich primitiv. Insbesondere sind alle normierten Polynome primitiv.

Beispiele. Die folgenden Beispiele beziehen sich auf den Ring $\mathbb{Z}[X]$.

(1) $6X^2 + 20 = 2(3X^2 + 10)$ ist nicht primitiv.
(2) $X^4 + 3X$ ist normiert und primitiv.
(3) $3X^4 + X$ ist nicht normiert, aber primitiv.
(4) $2X + 3$ ist primitiv.

Lemma 9.2 (Übergang zu primitiven Polynomen)**.** *Es seien $R \subseteq K$ wie in (9.1). Jedes Polynom $f \in K[X]$ lässt sich in der Form $f = c\tilde{f}$ mit einem $c \in K^\times$ und primitivem $\tilde{f} \in R[X]$ schreiben. Ist f in $R[X]$, so lässt sich $c \in R \setminus \{0_R\}$ wählen.*

Beweis. Wähle $c = \prod_{p \in \mathscr{P}} p^{\nu_p(f)}$. Für $f \in R[X]$ ist dies offensichtlich auch in $R \setminus \{0_R\}$. □

Beispiele. Sei $R = \mathbb{Z} \subseteq \mathbb{Q} = K$.

- $2X^2 + 4X + 2 = 2(X^2 + 2X + 1)$.
- $\frac{6}{8}X^5 + \frac{9}{4}X + 3 = \frac{3}{4}(X^5 + 3X + 4)$.

9.3. Lemma von Gauß

Das nächste Lemma (vgl. [19, Art. 42]) ist das Schlüsselergebnis, welches Faktorisierungen in $K[X]$ mit der Faktorisierung in R und schließlich mit der in $R[X]$ verknüpft.

Lemma 9.3 (Lemma von Gauß). *Es seien $R \subseteq K$ wie in (9.1) und p in $\mathscr{P}$. Für alle Polynome $f, g \in K[X]$ gilt dann*

$$\nu_p(fg) = \nu_p(f) + \nu_p(g). \tag{9.3}$$

Beweis. Wegen (9.2) gilt die behauptete Formel für Polynome vom Grad ≤ 0 und sogar, wenn lediglich eines der beiden Polynome Grad ≤ 0 hat (†). Wir schreiben nun $f = c_f \tilde{f}$ und $g = c_g \tilde{g}$ im Sinne von Lemma 9.2 mit primitiven Polynomen $\tilde{f}, \tilde{g} \in R[X]$ und $c_f, c_g \in K^\times$. Die folgende Rechnung zeigt, dass es für den Beweis von (9.3) genügt, die entsprechende Gleichung für $\tilde{f}$ und $\tilde{g}$ zu haben (‡):

$$\begin{aligned} \nu_p(fg) = \nu_p(c_f \tilde{f} c_g \tilde{g}) &\overset{(\dagger)}{=} \nu_p(c_f) + \nu_p(c_g) + \nu_p(\tilde{f}\tilde{g}) \\ &\overset{(\ddagger)}{=} \nu_p(c_f) + \nu_p(\tilde{f}) + \nu_p(c_g) + \nu_p(\tilde{g}) \\ &= \nu_p(f) + \nu_p(g). \end{aligned}$$

Um einzusehen, dass (9.3) für $\tilde{f}$ und $\tilde{g}$ gilt, betrachten wir den sogenannten ***Reduktionshomomorphismus (modulo p)*** $\Phi\colon R[X] \to (R/pR)[X]$, den man aus Satz 7.4 als denjenigen Homomorphismus gewinnt, der das folgende Diagramm kommutativ macht und $X \in R[X]$ auf $X \in (R/pR)[X]$ abbildet (siehe auch die Bemerkung auf Seite 115):

$$\begin{array}{ccc} R[X] & \xrightarrow[X \mapsto X]{\Phi} & (R/pR)[X] \\ \uparrow & & \uparrow \\ R & \xrightarrow{r \mapsto r+pR} & R/pR\,. \end{array} \tag{9.4}$$

Offensichtlich bildet Φ ab, indem die Koeffizienten des abzubildenden Polynoms modulo p reduziert werden. Der Kern von Φ ist folglich

$$\ker \Phi = \{ h \in R[X] : \nu_p(h) > 0 \} = pR[X]. \tag{9.5}$$

Insbesondere ist $\Phi(\tilde{f}), \Phi(\tilde{g}) \neq 0_{(R/pR)[X]}$. Da R/pR und somit auch $(R/pR)[X]$ ein Integritätsbereich ist, gilt somit auch $\Phi(\tilde{f}\tilde{g}) = \Phi(\tilde{f})\Phi(\tilde{g}) \neq 0_{(R/pR)[X]}$. Es folgt $\nu_p(\tilde{f}\tilde{g}) = 0 = \nu_p(\tilde{f}) + \nu_p(\tilde{g})$, wie gewünscht. □

Der erste Isomorphiesatz (Korollar 6.8) angewandt auf Φ aus dem Beweis von Lemma 9.3 zeigt unter Beachtung von (9.5)

$$R[X]/pR[X] \cong (R/pR)[X] \tag{9.6}$$

für jedes Primelement p von R. Auf dieses Ergebnis werden wir später im Beweis von Satz 9.6 zurückgreifen.

Beispiel. Die Nullteilerfreiheit von $(R/pR)[X]$ im Beweis von Lemma 9.3 stammt aus Gradbetrachtungen (vgl. Proposition 7.2). Nähere Inspektion des hier geführten

Beweises zeigt, dass der Wert von $\nu_p(fg)$ von den Leitkoeffizienten von $\Phi(f)$ und $\Phi(g)$ stammt. Wir illustrieren dies an einem Beispiel:

$$f = 2X^5 + 4X^4 + \underline{7X^3} + 3, \quad g = 6X^2 + \underline{5X} + 10.$$

Offensichtlich gilt $\nu_2(f) = 0 = \nu_2(g)$ und wir haben die Monome mit nicht durch 2 teilbarem Koeffizient und höchstem Exponent unterstrichen. Man beachte $\Phi(f) = X^3 + 1_{(\mathbb{Z}/2\mathbb{Z})[X]}$ und $\Phi(g) = X$. Ferner ist

$$\begin{aligned} fg = (2\cdot 6)X^7 + (2\cdot \underline{5} + 4\cdot 6)X^6 + (2\cdot 10 + 4\cdot \underline{5} + \underline{7}\cdot 6)X^5 + \\ + \underline{(4\cdot 10 + \underline{7}\cdot \underline{5})}X^4 + (\underline{7}\cdot 10)X^3 + (3\cdot 6)X^2 + (3\cdot \underline{5})X + 3\cdot 10. \end{aligned}$$

Man betrachte nun den Koeffizienten vor X^4 (beachte $4 = 3 + 1$ mit den „unterstrichenen Exponenten“ 3 und 1 bei f und g). Dieser ist nicht durch 2 teilbar, denn

$$4\cdot 10 + \underline{7}\cdot \underline{5} \equiv 0 + \underline{1}\cdot \underline{1} \not\equiv 0 \bmod 2.$$

Man könnte diese Beobachtung auch für einen direkten Beweis von Lemma 9.3 nutzen, doch verliert die Situation etwas an Transparenz, wenn man allgemein mit Brüchen arbeitet und aus der obigen Rechnung direkt die in Lemma 9.3 behauptete Gleichung folgern möchte.

Die nächsten beiden aus dem Lemma von Gauß (Lemma 9.3) abgeleiteten Korollare bauen eine wichtige Brücke zwischen der (vermöge Faktorialität, dank Euklidizität, gewährleisteten) Faktorisierungstheorie in $K[X]$ und der noch näher zu studierenden Faktorisierungstheorie in $R[X]$.

Korollar 9.4 (Faktorisierung mit normierten Faktoren)**.** *Es seien $R \subseteq K$ wie in (9.1). Ferner sei $h \in R[X]$ ein normiertes Polynom und $h = f \cdot g$ eine Faktorisierung von h in zwei normierte Polynome $f, g \in K[X]$. Dann folgt $f, g \in R[X]$.*

Beweis. Es sei p ein beliebiges Primelement. Ein Blick auf die jeweiligen Leitkoeffizienten zeigt $\nu_p(h), \nu_p(f), \nu_p(g) \leq 0$. Wegen $h \in R[X]$ ist aber dann $\nu_p(h) = 0$ und $h = f \cdot g$ zusammen mit Lemma 9.3 liefert $\nu_p(f) = 0 = \nu_p(g)$. Damit folgt $f, g \in R[X]$, wie gewünscht. □

Korollar 9.5 (Faktorisierung mit einem primitiven Faktor)**.** *Es seien $R \subseteq K$ wie in (9.1). Ferner sei $h \in R[X]$ ein Polynom und $h = f \cdot g$ eine Faktorisierung von h in zwei Polynome $f \in R[X]$ und $g \in K[X]$. Ist f primitiv, so folgt $g \in R[X]$.*

Beweis. Es sei p ein beliebiges Primelement. Wegen $h \in R[X]$ ist $\nu_p(h) \geq 0$. Da f primitiv ist, folgt $\nu_p(f) = 0$. Lemma 9.3 liefert dann $\nu_p(g) = \nu_p(f) + \nu_p(g) = \nu_p(h) \geq 0$. Also ist $g \in R[X]$. □

Bemerkung. Man kann Korollar 9.5 auch wie folgt formulieren: ist $f \in R[X]$ ein Teiler von $h \in R[X]$ bezüglich der Teilbarkeitsrelation auf $K[X]$, in Zeichen $f \mid_{K[X]} h$, und ist f zusätzlich primitiv, so folgt bereits $f \mid_{R[X]} h$, d.h. f teilt h bezüglich der Teilbarkeitsrelation auf $R[X]$. Man beachte, dass dies für nicht-primitive Polynome scheitert. Beispielsweise gilt $2 \mid_{\mathbb{Q}[X]} 1$, jedoch $2 \nmid_{\mathbb{Z}[X]} 1$.

9.4. Satz von Gauß über Polynomringe

Wir kommen nun zu dem bereits zu Beginn des Kapitels angekündigten Hauptergebnis über Polynomringe $R[X]$ über einem faktoriellen Ring R:

Satz 9.6 (Gauß). *Es seien $R \subseteq K$ wie in (9.1). Dann ist der Polynomring $R[X]$ faktoriell. Ein Polynom $q \in R[X]$ ist genau dann prim wenn eine der folgenden beiden Bedingungen erfüllt ist:*

(1) q ist ein konstantes Polynom und (aufgefasst als Element von R) prim in R.
(2) q ist primitiv in $R[X]$ und prim in $K[X]$.

Insbesondere ist ein primitives Polynom $q \in R[X]$ genau dann prim in $R[X]$ wenn es prim in $K[X]$ ist.

Beweis. Wir zeigen zunächst, dass die in (1) und (2) genannten Polynome tatsächlich prim sind.

(1) Ist q ein Primelement von R, so ist R/qR ein Integritätsbereich (vgl. Aufgabe 10.3 (a)). Wegen $R[X]/qR[X] \cong (R/qR)[X]$ (siehe (9.6)) ist dann aber auch $R[X]/qR[X]$ ein Integritätsbereich und also q prim in $R[X]$.
(2) Nun betrachte ein primitives Polynom $q \in R[X]$, welches prim in $K[X]$ ist. Wir wollen nun zeigen, dass q sogar prim in $R[X]$ ist. Hierzu teile q ein Produkt fg von Polynomen $f, g \in R[X]$ mit der Teilbarkeitsrelation in $R[X]$. Dann teilt q natürlich auch fg mit der Teilbarkeitsrelation in $K[X]$. Da q nach Voraussetzung prim in $K[X]$ ist, teilt q einen der beiden Faktoren in $K[X]$; ohne Einschränkung sei dies f. Wir haben also $f = qh$ mit einem $h \in K[X]$. Aus Korollar 9.5 folgt aber sogar $h \in R[X]$. Also teilt q das Polynom f schon bezüglich der Teilbarkeitsrelation in $R[X]$.

Für den Rest des Beweises genügt es zu zeigen, dass $R[X]$ faktoriell ist und jedes Primelement von $R[X]$ die im Satz angegebenen Form (1) oder (2) hat. Gemäß Satz 8.7 (3) genügt es hierzu zu zeigen, dass jedes $f \in R[X] \setminus (R[X]^\times \cup \{0_{R[X]}\})$ eine Faktorisierung in Primelemente der obigen beiden Typen hat. Wir dürfen im Folgenden $\deg f \geq 1$ annehmen, da f sich im Fall $\deg f = 0$ durch die Primzerlegung in R bereits als Produkt von Primelementen alleinig vom Typ (1) schreiben lässt. Man schreibe nun $f = c\tilde{f}$, wie in Lemma 9.2. Wegen $f \in R[X]$ ist $c \in R$ und c ist ein Produkt von Primelementen von R. Es genügt zu zeigen, dass $\tilde{f}$ sich als Produkt primitiver Polynome in $R[X]$ schreiben lässt, welche prim in $K[X]$ sind. Hierzu sei $\tilde{f} = \tilde{c}\tilde{f}_1 \cdots \tilde{f}_r$ eine Faktorisierung in Primelemente $\tilde{f}_1, \ldots, \tilde{f}_r$ von $K[X]$ mit einer Einheit $\tilde{c} \in K^\times$. Durch r-fache Anwendung von Lemma 9.2 und Absorption etwaiger Konstanten in $\tilde{c}$ dürfen wir davon ausgehen, dass alle $\tilde{f}_i$ in $R[X]$ liegen und primitiv sind. Mit dem Lemma von Gauß (Lemma 9.3) folgt dann für jedes Primelement p von R

$$0 = \nu_p(\tilde{f}) = \nu_p(\tilde{c}) + \underbrace{\nu_p(\tilde{f}_1) + \ldots + \nu_p(\tilde{f}_r)}_{\substack{\text{alle Summanden} = 0,\\ \text{da Polynome primitiv}}} = \nu_p(\tilde{c}).$$

Also ist $v_p(\tilde{c}) = 0$ für alle p und $\tilde{c} \in K^\times$ damit sogar eine Einheit in R. Ersetzt man $\tilde{f}_1$ durch $\tilde{c}\tilde{f}_1$, so sieht man, dass $\tilde{f}$ sich in der gewünschten Produktform schreiben lässt. □

Beispiel. Wir wollen $6X^3 + 12X \in \mathbb{Z}[X]$ in Primfaktoren zerlegen. Wir behaupten, dass

$$2 \cdot 3 \cdot X \cdot (X^2 + 2)$$

diese Aufgabe löst. In der Tat sieht man sofort durch Ausmultiplizieren, dass es sich um dasselbe Polynom handelt. Wir wollen noch begründen, dass die hier auftretenden Faktoren wirklich prim über $\mathbb{Z}$ sind. Die Zahlen 2 und 3 sind als Polynome in $\mathbb{Z}[X]$ prim, da sie schon als Elemente von $\mathbb{Z}$ prim sind; hier geht also schon Satz 9.6 ein. Die Faktoren X und $X^2 + 2$ sind jedenfalls prim als Polynome über $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$, wie man leicht mit Proposition 9.8 (siehe unten!) einsehen kann. Da sowohl X, wie auch $X^2 + 2$ aber auch primitiv sind, liefert Satz 9.6, dass diese sogar prim über $\mathbb{Z}$ sind.

Korollar 9.7. *Für einen faktoriellen Ring R ist auch der Polynomring $R[X_1, \ldots, X_n]$ in $n \in \mathbb{N}$ Variablen faktoriell. Insbesondere sind $\mathbb{Z}[X_1, \ldots, X_n]$ faktoriell und auch $L[X_1, \ldots, X_n]$ für einen beliebigen Körper L.*

Beweis. Man wende Satz 9.6 wiederholt an. (Siehe auch das Argument auf Seiten 138 und 139, welches Polynomringe in mehreren Variablen schrittweise aufbaut.) □

Bemerkung. Zu einem faktoriellen Ring R betrachten wir den Polynomring $R[\boldsymbol{X}]$ in abzählbar vielen Variablen $\boldsymbol{X} = \{X_n : n \in \mathbb{N}\}$. Dieser ist nicht noethersch, denn bei

$$\langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \langle X_1, X_2, X_3 \rangle \subsetneq \ldots \tag{9.7}$$

handelt es sich um eine aufsteigende, nirgends stationäre Folge von Idealen von $R[\boldsymbol{X}]$. Andererseits kann man zeigen, dass $R[\boldsymbol{X}]$ faktoriell ist. Gemäß Satz 8.7 genügt es dafür zu zeigen, dass sich jedes Element von $R[\boldsymbol{X}] \setminus (R[\boldsymbol{X}]^\times \cup \{0_{R[X]}\})$ als ein Produkt von Primelementen schreiben lässt. Jedes solche Element f ist aber ein Polynom in endlich vielen Variablen und damit für hinreichend großes n enthalten im Ring $R[X_1, \ldots, X_n]$, den wir (in offensichtlicher Weise) als Teilring von $R[\boldsymbol{X}]$ auffassen wollen. Im faktoriellen Ring $R[X_1, \ldots, X_n]$ (Korollar 9.7) ist f aber ein Produkt von primen Elementen und es verbleibt einzusehen, dass diese Elemente auch als Elemente von $R[\boldsymbol{X}]$ prim sind. Das ist allerdings nicht schwierig. Wäre nämlich p ein Primelement von $R[X_1, \ldots, X_n]$, welches aufgefasst als Element von $R[\boldsymbol{X}]$ nicht prim ist, so gibt es $a, b \in R[\boldsymbol{X}]$ derart, dass p zwar das Produkt ab, aber weder a noch b teilt. Da die Polynome p, a und b, sowie der Komplementärfaktor r mit $pr = ab$ nur endlich viele Variablen enthalten, dürfen wir $p, r, a, b \in R[X_1, \ldots, X_m]$ für ein $m \geq n$ annehmen und wir sehen, dass p bereits in $R[X_1, \ldots, X_m]$ nicht prim ist. Dann ist p dort aber auch nicht irreduzibel (denn im laut Korollar 9.7 faktoriellen Ring $R[X_1, \ldots, X_m]$ stimmen die Begriffe „irreduzibel“ und „prim“ überein; Satz 8.7). Man sieht nun aber leicht mit der Gradformel (Proposition 7.2), dass irreduzible Elemente eines Integritätsbereichs R' auch im Polynomring $R'[X]$ irreduzibel bleiben. Mit Induktion

folgt daraus, dass p, welches ja laut Annahme irreduzibel in $R[X_1,\dots,X_n]$ ist, auch irreduzibel in $R[X_1,\dots,X_m]$ ist. Das ist der gewünschte Widerspruch und es folgt, dass $R[\boldsymbol{X}]$ faktoriell ist.

Man beachte, dass $R[\boldsymbol{X}]$ als faktorieller Ring natürlich die Teilerkettenbedingung aus Satz 8.7 erfüllt. Jede aufsteigende Kette von *Hauptidealen* in $R[\boldsymbol{X}]$ wird also ab irgendeinem Punkt stationär. Dies steht im Kontrast zu (9.7), wobei es sich bei den Idealen dort (mit Ausnahme von $\langle X_1\rangle$) natürlich nicht um Hauptideale handelt. In diesem Sinne könnte man versucht sein, zu sagen, dass $R[\boldsymbol{X}]$ zwar „viele“ Ideale, aber „wenige“ Hauptideale besitzt.

9.5. Irreduzibilitätskriterien

Da die Verhältnisse zwischen den Faktorisierungstheorien in $R[X]$ und $K[X]$ nunmehr durch Satz 9.6 vollständig geklärt sind, wenden wir uns der Aufgabe zu, dieses Wissen geeignet auszuspielen. Der natürliche Wunsch wäre eine Lösung des folgenden Problems:

> *Gegeben ein Polynom in $R[X]$ oder $K[X]$. Gesucht ist die Faktorisierung selbigen Polynoms im entsprechenden Ring.*

Tatsächlich ist uns diese Problemstellung hier zu komplex; Bemerkung 9.10 (siehe unten) kann in manchen Fällen (z.B. für $R=\mathbb{Z}$) zu einer Lösung davon benutzt werden, liefert aber kein wirklich effizientes Verfahren. Hier begnügen wir uns damit, Kriterien zu entwickeln, mit deren Hilfe man die Irreduzibilität von einigen Polynomen erkennen kann.

9.5.1. Polynome mit kleinem Grad. Irreduzibilität von Polynomen mit *sehr kleinem Grad* ist oft nicht zu schwierig zu prüfen. Das folgende Ergebnis ist Aufgabe 13.2:

Proposition 9.8 (Irreduzibilität von Polynomen mit kleinem Grad)**.** *K sei ein beliebiger Körper und $f\in K[X]$ ein Polynom mit Grad n.*

(1) Ist $n=1$, so ist f irreduzibel.
(2) Ist $n\in\{2,3\}$, so ist f genau dann irreduzibel, wenn f keine Nullstelle in K besitzt.

Bemerkung. Bei der Suche von Nullstellen (und auch dem Ausschluss derer Existenz) kann manchmal das Ergebnis aus Aufgabe T13.3 nützlich sein.

Man beachte, dass die in Proposition 9.8 genannte Beziehung zwischen Irreduzibilität und Nullstellen ab Grad 4 zusammenbricht. So hat beispielsweise das Polynom $(X^2+1)^2$ keine reellen Nullstellen (denn $x^2+1>0$ für alle $x\in\mathbb{R}$), ist aber offensichtlich reduzibel.

Ferner sei zu beachten, dass sich Proposition 9.8 auf Irreduzibilität in $K[X]$ bezieht. Beispielsweise $2X$ hat Grad 1, ist aber nicht irreduzibel als Polynom über $\mathbb{Z}$, jedoch sehr wohl irreduzibel als Polynom über $\mathbb{Q}$.

Beispiele 9.9.

(1) Das quadratische Polynom $X^2+1 \in \mathbb{R}[X]$ ist irreduzibel, denn es hat keine reellen Nullstellen: in der Tat wäre jede reelle Nullstelle von X^2+1 ja auch eine komplexe Nullstelle desselben Polynoms aufgefasst als Polynom in $\mathbb{C}[X]$. Dort hat es allerdings nur die beiden Nullstellen $\pm i$, von denen keine reell ist.
(2) Mit einem ähnlichen Argument sieht man, dass $X^2-2 \in \mathbb{Q}[X]$ irreduzibel ist, denn in $\mathbb{R} \supset \mathbb{Q}$ hat es die beiden Nullstellen $\pm\sqrt{2}$, die aber nicht rational sind, wie man sicher aus der Analysis weiß. (Alternativ vgl. Aufgabe 9.4 oder siehe Beispiel 9.13.)
(3) $X^2-2 \in \mathbb{R}[X]$ ist reduzibel, denn es hat die Nullstellen $\pm\sqrt{2}$; in der Tat haben wir die Faktorisierung $X^2-2 = (X+\sqrt{2})(X-\sqrt{2})$.

Bemerkung 9.10 (Faktorisierungsmethode von Kronecker)**.** In Aufgabe 14.4 wird ein auf Kronecker zurückgehendes Verfahren entwickelt, mit dem man — jedenfalls theoretisch — beliebige Polynome über $\mathbb{Z}[X]$ in irreduzible Faktoren zerlegen kann. In der Praxis ist dieses Verfahren allerdings viel zu aufwändig, um nützlich zu sein und wird umso nutzloser, wenn man Irreduzibilität von einer Familie von Polynomen nachweisen möchte. Moderne Faktorisierungsverfahren gehen auf Ideen von Zassenhaus zurück; für eine Einführung, siehe [12]. Die Grundidee ist hier, dass die Koeffizienten von etwaigen Faktoren eines Polynoms $f \in \mathbb{Z}[X]$ nicht zu groß (in Abhängigkeit von f) sein können. Man faktorisiert f dann modulo einer geeignet gewählten Primzahl p und hebt diese Faktorisierung zu einer Faktorisierung modulo p^n $(n = 2, 3, \ldots)$ hoch. Ist der Exponent n hinreichend groß, so kann man aus dieser Faktorisierung dann geeignete Rückschlüsse auf Faktorisierungen von f über $\mathbb{Z}$ treffen.

9.5.2. Irreduzibilität via Übergang zu Faktorringen. Der Bezug zwischen Irreduzibilität in $R[X]$ und Irreduzibilität in $K[X]$, der durch den Satz von Gauß (Satz 9.6) hergestellt wird, lässt sich benutzen, um Irreduzibilität von manchen Polynomen in $K[X]$ nachzuweisen. Der wichtige Punkt hierbei ist, dass man stets zu einem primitiven Polynom in $R[X]$ übergehen kann (siehe Lemma 9.2) und Irreduzibilität in $R[X]$ ggf. leichter nachzuweisen ist als in $K[X]$. Der Grund hierfür ist, dass der Ring R — ganz im Gegensatz zum Körper K — i.Allg. nicht-triviale Ideale $\mathfrak{a}$ besitzt und Faktorisierungen in $R[X]$ zu Faktorisierungen in $R[X]/\mathfrak{a}R[X]$ „absteigen“. Wenn man sicherstellt, dass bei diesem Abstieg nichts Triviales[2] passiert, kann man hieraus Einiges über $R[X]$ lernen.

Proposition 9.11 (Reduktionskriterium)**.** *Es seien $R \subseteq K$ wie in (9.1), p ein Primelement von R und $f \in R[X]$ ein Polynom mit Grad > 1, dessen Leitkoeffizient nicht durch p teilbar ist. $\Phi\colon R[X] \to (R/pR)[X]$ sei wie in (9.4). Dann gilt:*

(1) Falls $\Phi(f)$ in $(R/pR)[X]$ irreduzibel ist, so ist auch f irreduzibel in $K[X]$.
(2) Falls $\Phi(f)$ in $(R/pR)[X]$ irreduzibel und f primitiv ist, so ist f irreduzibel in $R[X]$.

[2]Beispielsweise liefert die Faktorisierung $4 = 2 \cdot 2$ in modulo 2 nur die triviale Information $0_{\mathbb{F}_2} = 0_{\mathbb{F}_2} \cdot 0_{\mathbb{F}_2}$. Ähnliches kann auch in der Situation von Polynomen passieren.

Beweis. Wir beginnen mit Teil (2). Sei zunächst f als primitiv und reduzibel in $R[X]$, also $f = gh$ mit nicht-konstanten Polynomen $g, h \in R[X]$. Da der Leitkoeffizient von f das Produkt der Leitkoeffizienten von g und h ist, sind jene ebenfalls nicht durch p teilbar. Anwenden von Φ liefert also eine *nicht-triviale* Faktorisierung $\Phi(f) = \Phi(g)\Phi(h)$ in $(R/pR)[X]$. Also ist $\Phi(f)$ reduzibel in $(R/pR)[X]$. Das zeigt (2).

Für (1) schreibe $f = c\tilde{f}$ mit einem $c \in R$ (siehe Lemma 9.2). Dann ist p weder ein Teiler von c noch vom Leitkoeffizienten. Insbesondere ist $\Phi(c)$ eine Einheit in $(R/pR)[X]$ und $\Phi(f)$ somit assoziiert zu $\Phi(\tilde{f})$. Ist nun $\Phi(f)$ irreduzibel, so auch $\Phi(\tilde{f})$ und wegen (2) folgt, dass $\tilde{f}$ irreduzibel in $R[X]$ ist. Laut Satz 9.6 ist f dann aber irreduzibel in $K[X]$. □

Das nächste Ergebnis fußt auf dem Reduktionskriterium (Proposition 9.11). Es ist häufig nur nach G. Eisenstein benannt, wurde allerdings schon zuvor von Th. Schönemann publiziert.

Korollar 9.12 (Irreduzibilitätskriterium von Schönemann–Eisenstein)**.** *Es seien $R \subseteq K$ wie in (9.1) und $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in R[X]$ sei primitiv mit Grad $n > 0$. Ferner sei p ein Primelement von R mit*

$$p \mid a_0, a_1, \ldots, a_{n-1}, \quad p \nmid a_n, \quad \textit{und} \quad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $R[X]$ und auch in $K[X]$.

Beweis. Mit Φ wie im Reduktionskriterium (Proposition 9.11) bzw. wie in (9.4) folgt $\Phi(f) = \overline{a_n}X^n$ mit $\overline{a_n} = (a_n \bmod pR) \in (R/p)^\times$. Angenommen $f = gh$ sei eine nicht-triviale Faktorisierung von f in $R[X]$. Da f primitiv ist, gilt[3] $0 < \deg g, \deg h < \deg f$ und mit Blick auf die Leitkoeffizienten folgt, dass $\overline{a_n}X^n = \Phi(g)\Phi(h)$ eine nicht-triviale Faktorisierung ist ($\deg(\Phi(g)) = \deg g$ und $\deg(\Phi(h)) = \deg h$). Betrachtet man diese Faktorisierung nicht in $(R/pR)[X]$, sondern in $(\mathrm{Quot}(R/pR))[X]$ (ein faktorieller Ring!), so folgt, dass $\Phi(g)$ und $\Phi(h)$ selbst Monome sind. Wegen $\deg g, \deg h > 0$ sind die konstanten Koeffizienten (vor X^0) von g und h also durch p teilbar. Dann folgt aber $p^2 \mid a_0$, im Widerspruch zu unseren Voraussetzungen. Also ist f irreduzibel in $R[X]$. Laut Satz 9.6 ist f dann aber auch irreduzibel in $K[X]$. □

Beispiele.
(1) $X^4 + 2X^2 + 2 \in \mathbb{Z}[X]$ ist irreduzibel (Korollar 9.12 mit $p = 2$).
(2) $X^4 + 4X^2 + 2 \in \mathbb{Z}[X]$ ist irreduzibel (analog zu (1)).
(3) $X^4 + 4X^2 + 4 = (X^2 + 2)^2 \in \mathbb{Z}[X]$ ist offensichtlich *nicht* irreduzibel. Das Kriterium von Schönemann–Eisenstein (Korollar 9.12) lässt sich auf dieses Polynom auch nicht anwenden, da $p = 2$ die einzige hierfür in Frage kommende Primzahl ist, diese jedoch quadratisch im konstanten Koeffizienten 4 des Polynoms aufgeht. (Man beachte die Voraussetzung „$p^2 \nmid a_0$“ in Korollar 9.12.)

[3] Hätte g oder h Grad $\deg f$, so hätte h bzw. g Grad 0. O.B.d.A. $\deg g = 0$, also $g \in R \setminus \{0_R\}$. Aus Lemma 9.3 folgt $\nu_p(g) + \nu_p(h) = \nu_p(f) = 0$, also $\nu_p(g) = 0$, für alle Primelemente p von R und darum ist g sogar eine Einheit von R.

9.5.3. Anwendung 1: n-te Wurzeln aus Primzahlen. Als erste Anwendung geben wir ein arithmetisches Resultat, welches manche Leserin und manchen Leser bestimmt schon seit der Analysis 1 begleitet.

Beispiel 9.13 (n-te Wurzeln aus Primzahlen)**.** Die Polynome $f = X^2 - 2$ und $g = X^3 - 2$ sind irreduzibel in $\mathbb{Z}[X]$ und auch $\mathbb{Q}[X]$ gemäß Korollar 9.12 mit $p = 2$. Insbesondere haben diese keine Nullstellen in $\mathbb{Q}$, da man durch Abspalten eines geeigneten Linearfaktors (Lemma 7.5) zu einer nicht-trivialen Faktorisierung gelangen könnte. Wegen $f(\sqrt{2}) = 0$ und $g(\sqrt[3]{2}) = 0$ sind die Zahlen $\sqrt{2}, \sqrt[3]{2} \in \mathbb{R}$ also nicht rational. (Allgemeiner: $X^n - p \in \mathbb{Q}[X]$ ist irreduzibel für $n \geq 1$ und p prim; insbesondere ist $\sqrt[n]{p} \notin \mathbb{Q}$ für $n \geq 2$.) Man beachte allerdings, dass $X^2 - 4 = (X-2)(X+2)$ nicht irreduzibel in $\mathbb{Q}[X]$ ist.

9.5.4. Anwendung 2: Kreisteilungspolynome. Das Schönemann–Eisenstein-Kriterium lässt sich nicht auf alle Polynome anwenden, z.B. nicht auf[4] X oder $X + 1$. Manchmal lässt sich dies aber beheben. Es sei $\psi\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ der (eindeutige) Ringhomomorphismus, der X auf $X+2$ abbildet und das folgende Diagramm kommutativ[5] macht (siehe Satz 7.4):

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow[X \mapsto X+2]{\psi} & \mathbb{Z}[X]. \\ & \nwarrow \quad \nearrow & \\ & \mathbb{Z} & \end{array}$$

Dann ist ψ ein Isomorphismus. (Die Umkehrabbildung ist wie ψ zu definieren, nur sollte diese X auf $X-2$ abbilden. Deren Verkettung mit ψ ist dann ein Epimorphismus von $\mathbb{Z}[X]$, welcher X auf X abbildet und ein entsprechendes Diagramm kommutativ macht; Satz 7.4 garantiert, dass es sich dabei um die identische Abbildung handelt.)

Es ist demnach klar, dass sich ψ zu einer *Permutation* der irreduziblen Elemente von $\mathbb{Z}[X]$ einschränkt; insbesondere ist $\psi(f)$ genau dann irreduzibel, wenn f irreduzibel ist. Wir haben aber

$$\psi(X) = X + 2, \quad \psi(X+1) = (X+2) + 1 = X + 3.$$

Auf beide Polynome rechter Hand lässt sich aber nun Korollar 9.12 anwenden!

Diese Beobachtung mag im vorliegenden Fall recht trivial wirken, kann aber in günstigen Fällen dennoch nicht-triviale Ergebnisse liefern. Wir geben das folgende Beispiel:

Beispiel 9.14. Für jede Primzahl p ist das ***p-te Kreisteilungspolynom***

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Q}[X]$$

[4]Selbstverständlich sieht man sofort, dass diese Polynome irreduzibel sind, doch die hiesige Betrachtung ist als Vorbereitung auf Beispiel 9.14 gedacht.

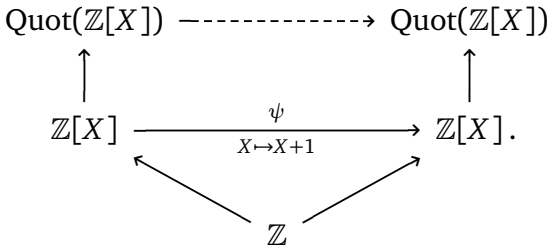
[5]Wegen Proposition 6.3 ist dies hier sogar trivial, wir erwähnen es aber trotzdem, da dies wichtig würde, wenn man $\mathbb{Z}$ durch einen beliebigen kommutativen Ring ersetzt.

irreduzibel in $\mathbb{Q}[X]$.[6] Zum Beweis davon ersetzen wir X durch $X+1$ (vgl. die vorangegangenen Ausführungen) Dann ist

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = \sum_{n=1}^{p} \binom{p}{n} X^{n-1} = X^{p-1} + \sum_{n=2}^{p-1} \underbrace{\binom{p}{n}}_{\text{wird von } p \text{ geteilt}} X^{n-1} + p.$$

Korollar 9.12 liefert nun die Irreduzibilität von $\Phi_p(X+1)$ und diese impliziert die Irreduzibilität von Φ_p.

Bemerkung. Die obige Rechnung mit Brüchen von Polynomen kann man rigoros machen, wenn man den Ringisomorphismus $\psi\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ mit $X \mapsto X+1$ mittels Satz 7.11 zu einem Ringhomomorphismus $\mathrm{Quot}(\mathbb{Z}[X]) \to \mathrm{Quot}(\mathbb{Z}[X])$ fortsetzt:



Alternativ kann man auch ψ auf $(X-1)\Phi_p$ anwenden und dann mit Nullteilerfreiheit von $\mathbb{Z}[X]$ schließen:

$$\begin{aligned} X\Phi_p(X+1) = X\psi(\Phi_p) = \psi((X-1)\Phi_p) = \psi((X+1)^p - 1) \\ = \ldots = \sum_{n=1}^{p} \binom{p}{n} X^n = X \sum_{n=1}^{p} \binom{p}{n} X^{n-1}, \end{aligned}$$

also

$$\Phi_p(X+1) = \sum_{n=1}^{p} \binom{p}{n} X^{n-1}.$$

Für weitere Beispiele siehe Aufgabe 14.3.

Ganz allgemein kann man auch das ***n-te Kreisteilungspolynom*** Φ_n für beliebige natürliche Zahlen n definieren. Dies macht man etwa so, dass $\Phi_1 = X - 1$ gilt und Φ_p für prime p wie oben gegeben ist. Dann definiert man Φ_n induktiv über die Anzahl der Faktoren von n mittels der Formel

$$X^n - 1 = \prod_{d|n} \Phi_d, \quad \text{oder äquivalent} \quad \Phi_n = (X^n - 1) \Big/ \prod_{\substack{d|n \\ d \neq n}} \Phi_d.$$

Dass Φ_n hierbei wirklich ein Polynom ist, also die Polynomdivision bei der letzten Gleichung keinen Rest lässt, wäre hier freilich noch zu begründen, aber wir vertrösten

[6] Für eine Anwendung hiervon siehe Satz 11.8.

die Leserinnen und Leser an dieser Stelle auf die *Algebra*-Vorlesung (siehe [45, § 5.5]). Wir berechnen nur beispielhaft

$$\Phi_1 = X-1, \quad \Phi_2 = \frac{X^2-1}{\Phi_1} = X+1, \quad \Phi_4 = \frac{X^4-1}{\Phi_1\Phi_2} = \frac{X^4-1}{X^2-1} = X^2+1, \quad \dots$$

Insbesondere fällt auf, dass auch Φ_4 irreduzibel ist. In Beispiel 9.14 haben wir die Irreduzibilität von Φ_p für primes p gezeigt. Ganz allgemein gilt jedoch laut einem Satz von Kronecker, dass Φ_n für jedes $n \in \mathbb{N}$ irreduzibel über $\mathbb{Q}$ ist; Für einen Beweis, siehe [45, Satz 5.20].

Kreisteilungspolynome und ihre Nullstellen (sogenannte ***Einheitswurzeln***) spielen eine wichtige Rolle in der Algebra und Zahlentheorie. Als eine Anwendung von Beispiel 9.14 zeigen wir in Kapitel 11, dass sich kein regelmäßiges 7-Eck mit Zirkel und Lineal konstruieren lässt. (Für Details dazu, was „Konstruierbarkeit“ hier genau heißt, siehe Kapitel 11; Der versprochene Satz ist Satz 11.8.) Speziell für die Anwendung auf das regelmäßige 7-Eck benötigen wir, dass

$$\Phi_7 = X^6+X^5+X^4+X^3+X^2+X+1$$

irreduzibel ist (und dessen Grad $6 = 2 \cdot 3$ keine Zweierpotenz ist). Kreisteilungspolynome begegnen uns auch später in der „Algebra“ wieder, wenn wir die Frage nach der Auflösbarkeit von Polynomgleichungen durch sogenannte Wurzelausdrücke untersuchen (siehe [45]).

Bemerkung. Es gibt irreduzible Polynome, deren Irreduzibilität auch nach Verschiebung nicht mit dem Kriterium von Schönemann–Eisenstein (Korollar 9.12) erkannt werden kann. Man betrachte etwa das Polynom $f = X^2+4 \in \mathbb{Z}[X]$. Dieses ist hat keine Nullstellen in $\mathbb{Q}$, hat Grad 2 und ist daher als Polynom in $\mathbb{Q}[X]$ irreduzibel gemäß Proposition 9.8. Da f zusätzlich primitiv ist, ist f laut Satz 9.6 auch irreduzibel als Polynom über $\mathbb{Z}$. Betrachtet man nun eine Verschiebung[7] $X \mapsto aX+b$ mit $a, b \in \mathbb{Z}$, so wird f zu $f(aX+b) = a^2X^2 + 2abX + (b^2+4)$. Angenommen, das Kriterium von Schönemann–Eisenstein ließe sich mit einer Primzahl p auf $f(aX+b)$ anwenden. Dann haben wir

(1) $p \nmid a^2$, also $p \nmid a$;
(2) $p \mid 2ab$, also $p \mid 2$ (d.h. $p = 2$), $p \mid a$, oder $p \mid b$ gemäß Lemma 3.2;
(3) $p \mid (b^2+4)$, aber $p^2 \nmid (b^2+4)$.

Wir diskutieren nun die drei Fälle in (2). Wäre $p = 2$, so hätten wir $p \mid b^2$ wegen (3) und also $p \mid b$ wegen Lemma 3.2, woraus sich $p^2 \mid (b^2+4)$, im Widerspruch zu (3) ergibt. Der Fall $p \mid a$ in (2) ist wegen (1) ausgeschlossen. Sei daher nun $p \mid b$ angenommen. Aus (3) folgt dann $p \mid 4$ und also $p = 2$. Diesen Fall haben wir aber bereits als widersprüchlich erkannt.

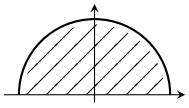
[7] Für $a \neq \pm 1$ ist der gestiftete Ringhomomorphismus $\psi\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ kein Automorphismus mehr und erhält tatsächlich Irreduzibilität nicht mehr (z.B. $\psi(X-b) = aX$), kann aber dennoch für Irreduzibilitätsnachweise genutzt werden, denn ist $\psi(f)$ irreduzibel, so gilt dies auch für f, obwohl die Umkehrung falsch sein kann.

KAPITEL 10

Diophantische Gleichungen

Zum Abschluss unserer Betrachtungen der Teilbarkeitstheorie soll hier ein Vorgeschmack auf etwaige vertiefende Vorlesungen zur *algebraischen Zahlentheorie* gegeben werden. Die Grundphilosophie sieht hier wie folgt aus: die Analysis schafft in der Bestrebung „kontinuierliche“ Phänomene zu beschreiben die reellen und (je nach Sichtweise) auch die komplexen Zahlen. Erst nach diesem Übergang erlangt die Differential- und Integralrechnung ihre Schlagkraft. Fragt man etwa nach der Fläche, welche der Graph von $[-1,1] \to \mathbb{R}$, $x \mapsto \sqrt{1-x^2}$, zusammen mit $[-1,1] \times \{0\}$ einschließt, so erhält man

$$\int_{-1}^{1} \sqrt{1-x^2}\,\mathrm{d}x = \frac{\pi}{2}.$$



(Fläche unter einem Halbkreis zum Radius 1.) Lindemann zeigte 1882, dass π (und damit auch $\pi/2$) ***transzendent über*** $\mathbb{Q}$ ist, d.h. keine Nullstelle eines Polynoms aus $\mathbb{Q}[X] \setminus \{0_{\mathbb{Q}[X]}\}$ ist.

Zahlentheoretikerinnen und Zahlentheoretiker hingegen beschäftigen sich mit den ganzen Zahlen und deren Arithmetik. Großes Interesse gilt hierbei den Primzahlen — den multiplikativen „Atomen“ der natürlichen Zahlen — und deren Verteilung. Ein anderer Schwerpunkt gilt dem Lösen von Gleichungen (etwa in den ganzen Zahlen). Genau damit wollen wir uns hier anhand einiger Beispiele(!) beschäftigen. Oft besteht dabei eine recht unstetige Gradwanderung zwischen trivialen und deutlich komplizierteren Problemen. Wir besprechen nur wenig und hoffen Interesse an tieferen Untersuchungen im Rahmen einer Spezialvorlesung zur Algebraischen Zahlentheorie zu wecken. Interessierte Leserinnen und Leser seien auch auf [28, 13, 40] verwiesen.

10.1. Lineare Gleichungen

Wir sprechen hier sehr knapp über lineare Gleichungen. Die lineare Gleichung $aX = b$ mit Koeffizienten $a, b \in \mathbb{Z}$ ist offensichtlich genau dann lösbar, wenn b ein Vielfaches von a ist. Nun zu zwei Variablen. Wir betrachten die lineare Gleichung

$$aX + bY = c. \tag{10.1}$$

Idealtheoretisch wissen wir $a\mathbb{Z} + b\mathbb{Z} = \mathrm{ggT}(a,b)\mathbb{Z}$ und demnach ist diese Gleichung genau dann lösbar, wenn c vom größten gemeinsamen Teiler von a und b geteilt wird; vgl. Lemma 1.6 für eine frühe (aber äquivalente) Version dieser Beobachtung.

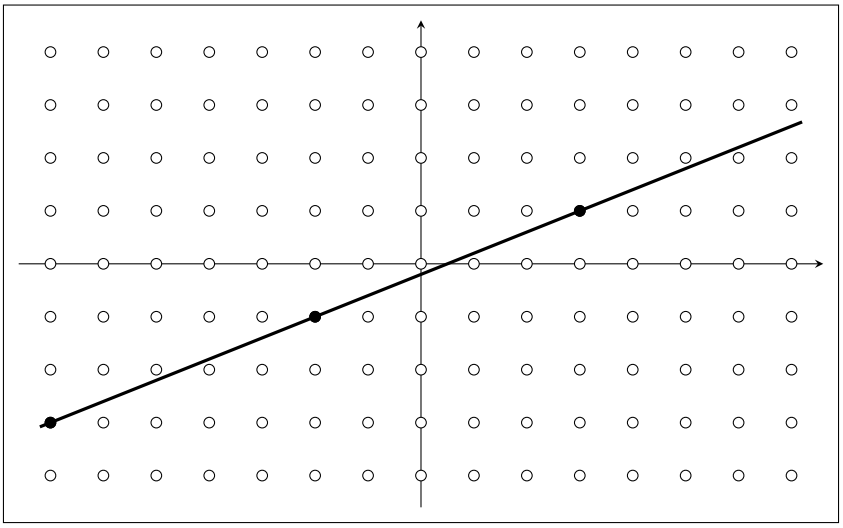


Abbildung 20. Die Lösungen $(x, y) \in \mathbb{R}^2$ von $aX + bY = c$ bilden eine Gerade (hier: $(a, b, c) = (2, -5, 1)$). Das gezeichnete Gitter entspricht $\mathbb{Z}^2$ und die Gitterpunkte auf der Geraden entsprechen ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$.

Entsprechende Lösungen $(x, y) \in \mathbb{Z}^2$ von (10.1) kann man tatsächlich auch algorithmisch bestimmen, wenn man den euklidischen Algorithmus zur Bestimmung von $\mathrm{ggT}(a, b)$ anwendet und rückwärts auflöst (siehe auch § 8.1.2). Rigorose Details hierzu besprechen wir nicht, sondern behandeln nur ein Beispiel:

Beispiel 10.1. Man löse die Gleichung

$$575X + 139Y = 2 \tag{10.2}$$

in den ganzen Zahlen. (Man spricht von „ganzzahligen Lösungen“.) Zur Lösung der Gleichung beachte man (wiederholte Division mit Rest!)

$$\begin{cases} 575 = 4 \cdot 139 + 19, \\ 139 = 7 \cdot 19 + 6, \\ \ 19 = 3 \cdot 6 + 1. \end{cases}$$

Das zeigt $\mathrm{ggT}(575, 139) = 1$. (Man überlege sich weshalb!) Durch Umstellen und Einsetzen der obigen Gleichungen von unten nach oben erhält man sukzessive

$$\begin{aligned} 1 &= 19 - 3 \cdot 6 \\ &= 19 - 3 \cdot (139 - 7 \cdot 19) \\ &= 22 \cdot 19 - 3 \cdot 139 \\ &= 22 \cdot (575 - 4 \cdot 139) - 3 \cdot 139 \\ &= 22 \cdot 575 - 91 \cdot 139. \end{aligned}$$

(Spätestens jetzt sieht man $\operatorname{ggT}(575,139) = 1$ mittels Lemma 1.6.) Dann ist aber $(x,y) = 2\cdot(22,-91)$ eine Lösung von (10.2). Für jede weitere Lösung $(x',y') \in \mathbb{Z}^2$ ist $(x'-x, y'-y) \in \mathbb{Z}^2$ eine Lösung der homogenen Gleichung $575X + 139Y = 0$ und also von der Form $(t,(-575/139)t)$ mit $t \in (139/\operatorname{ggT}(575,139))\mathbb{Z} = 139\mathbb{Z}$. Die Menge aller *ganzzahligen* Lösungen von (10.2) ist also

$$\left\{ \begin{pmatrix} 2\cdot 22 + 139r \\ -2\cdot 91 - 575r \end{pmatrix} \in \mathbb{Z}^2 : r \in \mathbb{Z} \right\}.$$

Prinzipiell kann man mit ähnlichen Methoden auch lineare Gleichungen mit ganzzahligen Koeffizienten in beliebig vielen Variablen lösen und sogar Systeme von Gleichungen betrachten. Wir verzichten auf nähere Ausführungen.

10.2. Pythagoreische Tripel

Bevor wir uns dem eigentlichen Thema dieses Abschnittes widmen, studieren wir ein (recht konstruiertes) Beispiel, welches illustrieren soll, dass die eindeutige Primfaktorzerlegung eine wichtige Rolle beim Lösen von Gleichungen spielen kann. (Tatsächlich trat Teilbarkeit auch schon in Beispiel 10.1 auf.)

Beispiel 10.2. Die Gleichung $Y^2 = X^3 + 5X^2 + X$ hat nur die triviale Lösung $(x,y) = (0,0)$ in den ganzen Zahlen. In der Tat, ist $(x,y) \in \mathbb{Z}^2$ eine Lösung, so ist $(x^2+5x+1)x = y^2$ ein Quadrat, also $\nu_p((x^2+5x+1)x) \in 2\mathbb{N}_0$ für alle Primzahlen p. Da aber x^2+5x+1 und x teilerfremd sind müssen x^2+5x+1 und x selbst schon Quadratzahlen sein. Wir unterscheiden einige Fälle.

- Für $x \geq 4$ ist $(x+2)^2 < x^2+5x+1 < (x+3)^2$ und also x^2+5x+1 nie ein Quadrat.
- Für $x \leq -5$ ist $(x^2+5x+1)x = ((x+2.5)^2 - 5.25)x$ negativ und darum sicher $\neq y^2 \geq 0$.
- Die Fälle $x \in \{-4,-3,-2,-1,1,2,3\}$ schließt man leicht per Hand aus und für $x = 0$ erhält man die Lösung $(x,y) = (0,0)$, die bereits oben erwähnt wurde.

Nun zur eigentlichen Frage: welche Tripel (x,y,z) natürlicher Zahlen treten als Seitenlängen rechtwinkliger Dreiecke auf? (Siehe Abbildung 21.) Beispielsweise haben wir

$$3^2 + 4^2 = 5^2$$

und der aus der Geometrie bekannte ***Kosinussatz*** (siehe Abbildung 22) impliziert auch, dass Lösen der Gleichung

$$X^2 + Y^2 = Z^2 \tag{10.3}$$

hinreichend *und* notwendig ist, damit es zu $(x,y,z) \in \mathbb{N}^3$ ein rechtwinkliges Dreieck mit eben diesen Seitenlängen gibt. Solche Tripel nennt man ***pythagoreische Tripel***.

Zu jeder Lösung $(x,y,z) \in \mathbb{N}^3$ von (10.3) und $k \in \mathbb{N}$ ist auch $(kx,ky,kz) \in \mathbb{N}^3$ eine Lösung von (10.3). Setzt man $g = \operatorname{ggT}(x,y,z)$, so ist auch $(x/g, y/g, z/g)$ eine

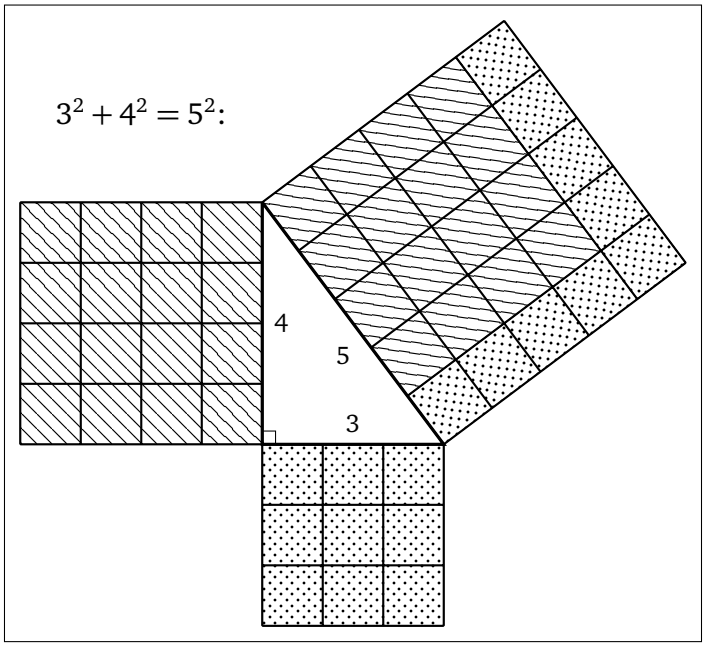


Abbildung 21. Veranschaulichung des primitiven pythagoreischen Tripels $(3, 4, 5)$.

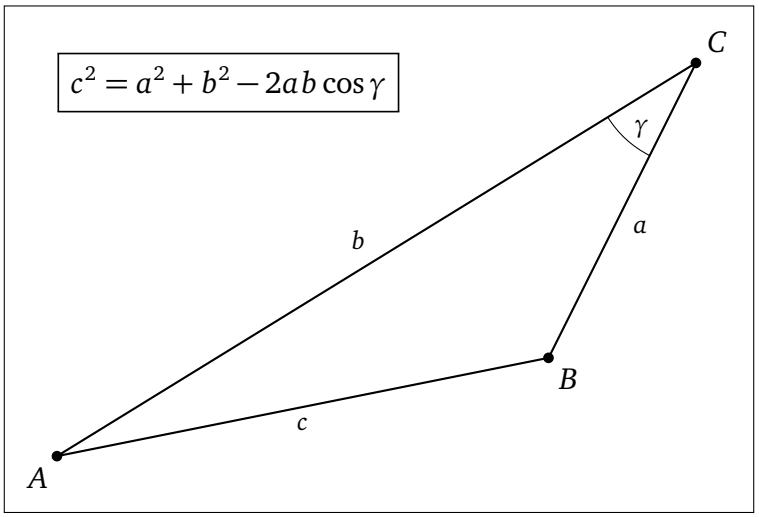


Abbildung 22. Der ***Kosinussatz***: In einem Dreieck $\triangle ABC$ Seitenlängen $a = |BC|$, $b = |AC|$, $c = |AB|$ und Winkel $\gamma = \sphericalangle ACB$ gilt $c^2 = a^2 + b^2 - 2ab\cos\gamma$. Offenbar gilt genau dann $c^2 = a^2 + b^2$, wenn $\cos\gamma = 0$, also wenn γ ein rechter Winkel ist.

Lösung von (10.3) und für diese neue Lösung gilt $\mathrm{ggT}(x/g, y/g, z/g) = 1$. Allgemein

nennt man ein pythagoreisches Tripel (x,y,z) mit $\mathrm{ggT}(x,y,z)=1$ ***primitiv***. Offensichtlich gewinnt man jedes pythagoreische Tripel durch Skalierung eines primitives pythagoreischen Tripels mit einer Zahl $k\in\mathbb{N}$ wie oben. Es genügt daher, sich auf die Suche *primitver pythagoreischer* Tripel beschränken.

Satz 10.3 (Parametrisierung primitiver pythagoreischer Tripel)**.** *Die Formel*

$$\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}a^2-b^2\\2ab\\a^2+b^2\end{pmatrix}$$

mit $a,b\in\mathbb{N}$, $a>b$, liefert nur pythagoreische Tripel. Das so produzierte Tripel ist genau dann primitiv wenn a und b teilerfremd und nicht beide ungerade sind. Ferner kommt jedes primitive pythagoreische Tripel in dieser Form oder als (y,x,z) vor.

Beweis. Dass die obige Formel pythagoreische Tripel produziert lässt sich leicht nachrechnen. Die Charakterisierung, wann die Formel primitive Tripel produziert, ist ebenfalls leicht nachzuprüfen und sei den geneigten Leserinnen und Lesern als einfache Übungsaufgabe überlassen.

Spannend ist hauptsächlich die Frage, ob jedes primitive pythagoreische Tripel (x,y,z) durch die fragliche Formel produziert wird. Da jeder Teiler von zwei der Zahlen x,y,z wegen $x^2+y^2=z^2$ auch ein Teiler der dritten ist, folgt wegen der Primitivität $\mathrm{ggT}(x,y)=\mathrm{ggT}(x,z)=\mathrm{ggT}(y,z)=1$. Insbesondere sind x und y nicht beide gerade. Wäre z gerade, so folgt $x^2+y^2\equiv 0 \bmod 4$. Herumprobieren mit Restklassen zeigt, dass dies nur möglich ist, wenn x und y beide gerade sind; das ist aber ausgeschlossen. Also ist z ungerade. Dann ist aber entweder x gerade oder y gerade, aber nicht beide zugleich. Durch etwaiges Vertauschen der Rollen von x und y dürfen wir davon ausgehen, dass y gerade ist.

Wir faktorisieren nun

$$z^2=x^2+y^2=(x+\mathrm{i}y)(x-\mathrm{i}y) \tag{10.4}$$

und behaupten, dass $\zeta=x+\mathrm{i}y$ und $\overline{\zeta}=x-\mathrm{i}y$ in $\mathbb{Z}[\mathrm{i}]$ teilerfremd sind. (Wichtig für die folgenden Überlegungen: $\mathbb{Z}[\mathrm{i}]$ ist euklidisch (Aufgabe T9.2) und somit faktoriell.) In der Tat sei $\pi\in\mathbb{Z}[\mathrm{i}]$ ein Primelement, welches ζ und $\overline{\zeta}$ teilt. Dann teilt π auch $\zeta+\overline{\zeta}=2x$ und $\zeta-\overline{\zeta}=2\mathrm{i}y$. Da x und y in $\mathbb{Z}$ teilerfremd sind, sind sie es auch in $\mathbb{Z}[\mathrm{i}]$, denn wäre $x=qu$ und $y=qv$, so hätten wir nach Übergang zu Normen (siehe Aufgabe T9.2) $x^2=N(q)N(u)$ und $y^2=N(q)N(v)$, weswegen x^2 und y^2 nicht teilerfremd in $\mathbb{Z}$ wären — im Widerspruch zu $\mathrm{ggT}(x,y)=1$. Daraus folgt $\pi\mid 2=(1+\mathrm{i})(1-\mathrm{i})=\mathrm{i}(1-\mathrm{i})^2$ und somit $p\sim 1-\mathrm{i}$. Wegen $z^2=\zeta\overline{\zeta}=N(\zeta)$ erhielten wir hieraus $2\mid z^2$. Das widerspricht der Tatsache, dass z ungerade ist. Also sind ζ und $\overline{\zeta}$ teilerfremd in $\mathbb{Z}[\mathrm{i}]$.

Aus (10.4) folgt nun, dass $x+\mathrm{i}y$ bereits selbst ein Quadrat sein muss (vgl. das Argument aus Beispiel 10.2). Wir haben also

$$x+\mathrm{i}y=(a+\mathrm{i}b)^2=(a^2-b^2)+\mathrm{i}(2ab).$$

für geeignete $a, b \in \mathbb{Z}$. Wegen $y > 0$ haben a und b dasselbe Vorzeichen und durch etwaiges Ersetzen durch $-a$ und $-b$ dürfen wir $a, b \in \mathbb{N}$ annehmen. Wegen $x > 0$ muss dann weiter $a > b$ gelten. □

10.3. Fermats Großer Satz für $n = 4$

Im 17. Jahrhundert (ca. 1637) notierte der französische Jurist und Mathematiker Pierre de Fermat in seiner Ausgabe der *Arithmetica* von Diophantos von Alexandria die Behauptung, dass die Gleichung (vgl. (10.3))

$$X^n + Y^n = Z^n \tag{10.5}$$

für $n \in \mathbb{N}$ mit $n \geq 3$ keine Lösungen in den *positiven* ganzen Zahlen besäße. (Man beachte natürlich, dass die obige Gleichung sehr wohl Lösungen in den ganzen Zahlen besitzt: $(t, 0, t)$ und $(0, t, t)$ für beliebige $t \in \mathbb{Z}$ und zusätzliche $(t, -t, 0)$, falls n ungerade ist. Alle diese Lösungen erfüllen $XYZ = 0$.)

Heutzutage geht man davon aus, dass Fermat seine Behauptung für den Spezialfall $n = 4$ und vielleicht für auch für $n = 3$ beweisen konnte, aber nicht im Besitz eines allgemeingültigen Beweises war. Seine Behauptung konnte erst 1994 von Andrew Wiles (mit zusätzlicher Unterstützung von Richard Taylor) bewiesen werden. Obgleich diese Ergebnisse weit jenseits dessen liegen, was wir mit den hier entwickelten Methoden besprechen können, ist uns zumindest der Fall $n = 4$ trotzdem zugänglich. Wir beweisen Folgendes:

Satz 10.4. *Die Gleichung*

$$X^4 + Y^4 = W^2 \tag{10.6}$$

hat keine Lösung in den positiven ganzen Zahlen.

Korollar 10.5. *Die Gleichung (10.5) hat für $n = 4$ keine Lösung in den positiven ganzen Zahlen.*

Beweis. Jede hypothetisch existente Lösung $(x, y, z) \in \mathbb{N}^3$ von (10.5) liefert mit $w = z^2$ eine Lösung $(x, y, w) \in \mathbb{N}^3$ von (10.6). Solche Lösungen existieren laut Satz 10.4 aber nicht. □

Beweis von Satz 10.4. Angenommen, (10.6) besäße Lösungen in $\mathbb{N}^3$. Dann können wir eine solche Lösung $(x, y, w) \in \mathbb{N}^3$ mit *minimalem* w auswählen. Wir zeigen nun, dass sich aus dieser Lösung eine weitere Lösung von (10.6) mit noch kleinerer rechten Seite konstruieren lässt. Der so erzeugte Widerspruch zeigt dann die Behauptung des Satzes.

Wir behaupten, dass x und y teilerfremd sind. Denn angenommen nicht, also $x = p\tilde{x}$ und $y = p\tilde{y}$ mit $\tilde{x}, \tilde{y} \in \mathbb{N}$ und primem p, so liefert (10.6)

$$p^4(\tilde{x}^4 + \tilde{y}^4) = w^2.$$

Mittels eindeutiger Primfaktorzerlegung sieht man, dass p^2 ein Teiler von w ist. Damit ist $(\tilde{x}, \tilde{y}, w/p^2)$ eine weitere Lösung von (10.6) mit kleinerer rechter Seite als w, im Widerspruch zu unserer Wahl von (x, y, w).

Ferner sind x und y nicht beide ungerade, denn anderenfalls erhielte man nach Reduktion modulo 4

$$x^4 + y^4 \equiv 1 + 1 = 2 \equiv w^2 \mod 4,$$

aber Quadrate sind stets $\equiv 0, 1 \mod 4$.

Durch etwaige Vertauschung von x und y dürfen wir davon ausgehen, dass x ungerade ist. Es folgt, dass (x^2, y^2, w) ein *primitives* pythagoreisches Tripel mit x^2 ungerade ist. Laut Satz 10.3 ist dieses also von der Form

$$\begin{cases} x^2 = a^2 - b^2, \\ y^2 = 2ab, \\ w = a^2 + b^2, \end{cases}$$

mit geeigneten teilerfremden $a, b \in \mathbb{N}$ mit $a > b$, nicht beide ungerade. Insbesondere haben wir

$$x^2 + b^2 = a^2;$$

D.h. (x, b, a) ist ebenfalls ein pythagoreisches Tripel und x ist nach obiger Annahme ungerade. Bei (x, b, a) handelt es sich sogar um ein *primitives* pythagoreisches Tripel, da jeder gemeinsame Teiler von x, b und a ja auch $y^2 = 2ab$ teilt, aber x und y jedoch teilerfremd sind. Eine abermalige Anwendung von Satz 10.3 liefert somit

$$\begin{cases} x = r^2 - s^2, \\ b = 2rs, \\ a = r^2 + s^2, \end{cases}$$

mit teilerfremden $r, s \in \mathbb{N}$ mit $r > s$, nicht beide ungerade. Wegen $a = r^2 + s^2$ sind a, r und s sogar paarweise teilerfremd. Aus der Gleichung $y^2 = 2ab = 4ars$ folgern wir nun mittels eindeutiger Primfaktorzerlegung, dass die (paarweise teilerfremden!) Zahlen a, r und s selbst Quadratzahlen sein müssen:

$$\begin{cases} a = u^2, \\ r = m^2, \\ s = n^2, \end{cases}$$

für geeignete $u, m, n \in \mathbb{N}$. Allerdings ist

$$m^4 + n^4 = r^2 + s^2 = a = u^2$$

und bei (m, n, u) handelt es sich also um eine Lösung von (10.6), die wegen

$$w = a^2 + b^2 > a^2 = u^4 \geq u$$

unserer minimalen Wahl von w widerspricht. □

10.4. Summen von Quadraten

Wir betrachten nun die Frage, welche ganzen Zahlen z sich als Summe zweier Quadratzahlen schreiben lassen, d.h. wir wollen

$$X^2 + Y^2 = Z \tag{10.7}$$

lösen. Offensichtlich genügt jede Lösung $(x, y, z) \in \mathbb{Z}^3$ von (10.7) den Ungleichungen $z \geq 0$ und $|x|, |y| \leq \sqrt{z}$. Ein wenig Herumexperimentieren mit kleinen Werten liefert die ersten paar Zahlen z, die sich so darstellen lassen:

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37.$$

Insbesondere lassen sich 3 und 6 nicht als Summe zweier Quadratzahlen schreiben.

Wir betrachten nun die Gleichung (10.7) in $\mathbb{Z}[\mathrm{i}]$. Für jede Lösung (x, y, z) davon ist dann

$$z = x^2 + y^2 = (x + \mathrm{i}y)(x - \mathrm{i}y).$$

Wir zerlegen $x + \mathrm{i}y$ nun in ein Produkt $\pi_1 \cdots \pi_n$ vom Primelementen von $\mathbb{Z}[\mathrm{i}]$. Ferner zerlegen wir z in ein Produkt von Primzahlen $z = p_1 \cdots p_r$, wobei wir $z \geq 2$ annehmen. Wir erinnern an die Notation $\overline{\cdot}$ für die komplexe Konjugation. Nun ist

$$p_1 \cdots p_r = z = (\pi_1 \cdots \pi_n)(\overline{\pi_1} \cdots \overline{\pi_n}) = (\pi_1 \overline{\pi_1}) \cdots (\pi_n \overline{\pi_n}). \tag{10.8}$$

Bei den Produkten $\pi_i \overline{\pi_i} = N(\pi_i)$ handelt es sich um Normen von Primelementen (vgl. Aufgaben T9.2 und 13.4 und Aufgabe 9.4). Das folgende Ergebnis wurde in der Lösung von Aufgabe 13.4 bewiesen:

Lemma 10.6. *$\pi = a + \mathrm{i}b$ mit $a, b \in \mathbb{Z}$ ist genau dann ein Primelement von $\mathbb{Z}[\mathrm{i}]$ wenn einer der beiden Fälle eintritt:*

(1) $a^2 + b^2$ ist eine Primzahl,
(2) $a^2 + b^2$ ist das Quadrat einer Primzahl, welche sich nicht als Summe zweier Quadrate darstellen lässt.

Beweis. Siehe die Lösung zu Aufgabe 13.4 für mehr Details; wir skizzieren dennoch einige wichtige Kernargumente. Wir wissen, dass $N(\pi) = 1$ genau dann gilt, wenn π eine Einheit ist. Ist $\pi = a + \mathrm{i}b$ prim, so ist $\pi\overline{\pi} = N(\pi) = p_1 \cdots p_r$ mit der Primfaktorzerlegung von $N(\pi)$ in $\mathbb{N}$. Also teilt π eine der Primzahlen p_i, die wir kurz p nennen wollen. Es gilt also $N(\pi) \mid N(\pi) = p^2$ und somit $N(\pi) \in \{p, p^2\}$.

Sei nun umgekehrt $\pi = a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$ beliebig mit $N(\pi) \in \{p, p^2\}$. Im Falle $N(\pi) = p$ folgt, dass π irreduzibel (also prim) ist, denn aus einer Gleichung $\pi = \pi_1\pi_2$ folgt $p = N(\pi) = N(\pi_1)N(\pi_2)$ und also $N(\pi_1) = 1$ oder $N(\pi_2) = 1$, womit π_1 oder π_2 eine Einheit sein muss. Ist $N(\pi) = p^2$ mit einer Primzahl p, die keine Summe zweier Quadrate ist, so gibt es kein Element π' mit $N(\pi') = p$ und ein ähnliches Argument wie eben zeigt, dass π prim ist. Ist hingegen $N(\pi) = p^2$ mit einer Primzahl $p = a^2 + b^2$, so schreibt sich

$$\pi\overline{\pi} = N(\pi) = (a^2 + b^2)^2 = (a + \mathrm{i}b)^2(a - \mathrm{i}b)^2.$$

Man sieht hieran, dass π nicht prim ist. □

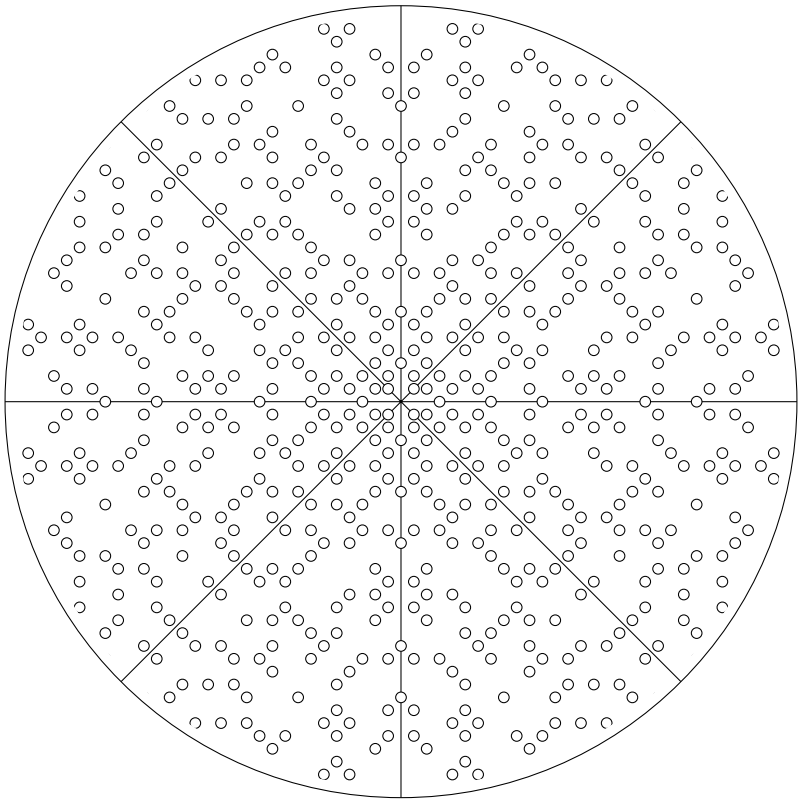


Abbildung 23. Die Primelemente $\pi = a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$ mit $a^2 + b^2 \leq 30^2$. (Siehe Satz 10.7 und auch Aufgabe 13.4.)

Der folgende Satz charakterisiert die Primelemente von $\mathbb{Z}[\mathrm{i}]$ (siehe Abbildung 23).

Satz 10.7. *Die Primelemente π von $\mathbb{Z}[\mathrm{i}]$ sind bis auf Assoziierte wie folgt gegeben:*

(1) $\pi = 1 + \mathrm{i}$,

(2) $\pi = a + \mathrm{i}b$ *mit* $a^2 + b^2 = p$ *(prim in* $\mathbb{Z}$*),* $p \equiv 1 \bmod 4$, $a > |b| > 0$,

(3) $\pi = p$ *mit einer Primzahl* $p \equiv 3 \bmod 4$.

Beweis. Gemäß Lemma 10.6 genügt es einzusehen, dass die Primzahlen $p \neq 2$, welche sich als Summe zweier Quadrate schreiben lassen, genau die Primzahlen sind, die kongruent 1 modulo 4 sind. In Aufgabe 13.4 (c) hatten wir schon gesehen, dass keine zu 3 modulo 4 kongruente Zahl als Summe zweier Quadrate geschrieben werden kann. Sei also $p = 4n + 1$ prim. Es genügt dann zu zeigen, dass p Summe zweier Quadrate ist. Hierzu beachte man die Gleichung

$$X^{p-1} - 1 = (X-1)(X-2)\cdots(X-(p-1)) \quad \text{in} \quad (\mathbb{Z}/p\mathbb{Z})[X].$$

(Diese folgt, da beide Polynome dieselben Nullstellen und denselben Grad haben; beachte Korollar 1.10.) Ausmultiplizieren der rechten Seite und Vergleichen der

konstanten Koeffizienten liefert

$$-1 \equiv (-1)\cdot(-2)\cdots(-(p-1)) = (p-1)!\cdot(-1)^{p-1} \mod p.$$

(Die obige Kongruenz ist auch als ***Satz von Wilson*** bekannt.) Da p ungerade ist, folgt

$$\begin{aligned} -1 &\equiv (p-1)! = (4n)! \\ &= (1\cdot 2\cdots(2n))((p-1)\cdot(p-2)\cdots(p-2n)) \\ &\equiv (2n)!\cdot(-1)^{2n}\cdot(2n)! \mod p. \end{aligned}$$

Sei $x = (2n)!$. Dann ist p ein Teiler von $x^2+1 = (x+\mathrm{i})(x-\mathrm{i})$, aber kein Teiler von $x \pm \mathrm{i}$, denn in $\mathbb{Q}(\mathrm{i}) \supset \mathbb{Z}[\mathrm{i}]$ ist $(x\pm\mathrm{i})/p = \frac{x}{p} \pm \mathrm{i}\frac{1}{p} \notin \mathbb{Z}[\mathrm{i}]$. Insbesondere ist p kein Primelement in $\mathbb{Z}[\mathrm{i}]$. Für jedes Primelement $\pi = a+\mathrm{i}b$ von $\mathbb{Z}[\mathrm{i}]$, welches p teilt, gilt dann $N(\pi) \mid N(p) = p^2$, da aber π nicht assoziiert zu p ist (denn p ist ja kein Primelement von $\mathbb{Z}[\mathrm{i}]$), muss $N(\pi) \neq p^2$ gelten. Es folgt $a^2+b^2 = N(\pi) = p$. □

Satz 10.8. *Eine natürliche Zahl $z \geq 2$ ist genau dann als Summe von zwei Quadraten darstellbar, wenn in der Primfaktorzerlegung $z = \prod_p p^{\nu_p(z)}$ von z alle Exponenten $\nu_p(z)$ zu $p \equiv 3 \bmod 4$ gerade sind.*

Beweis. Aus (10.8) und Satz 10.7 folgt, dass die im Satz angegebene Bedingung jedenfalls notwendig ist. Um zu sehen, dass sie auch hinreichend ist, schreibe man

$$z = p_1^{\nu_1}\cdots p_r^{\nu_r}\cdot q_1^{2\mu_1}\cdots q_k^{2\mu_k}$$

mit Primzahlen $p_i \not\equiv 3 \bmod 4$ und Primzahlen $q_j \equiv 3 \bmod 4$. Jede solche Primzahl p_i ist Summe von zwei Quadraten, wie wir im Beweis von Satz 10.7 gesehen hatten; wir schreiben $p_i = a_i^2+b_i^2 = (a_i+\mathrm{i}b_i)(a_i-\mathrm{i}b_i)$. Es folgt, dass

$$z = N((a_1+\mathrm{i}b_1)^{\nu_1}\cdots(a_r+\mathrm{i}b_r)^{\nu_r}q_1^{\mu_1}q_k^{\mu_k})$$

Summe zweier Quadrate ist. □

Bemerkung 10.9. Landau [35] zeigte 1908 die asymptotische Formel

$$\#\{\,n \leq x : n \text{ ist als Summe zweier Quadrate darstellbar}\,\} \sim \frac{bx}{\sqrt{\log x}} \quad (x\to\infty).$$

Hier ist

$$b = \frac{1}{\sqrt{2}}\prod_{\substack{p \text{ prim}\\ p\equiv 3 \bmod 4}}\left(1-\frac{1}{p^2}\right)^{-1/2} = 0{,}76422365358922\ldots$$

die sogenannte ***Landau–Ramanujan-Konstante***. Für Details, siehe etwa [7, § 1.8] oder [38, § 6.2, Ex. 21 auf Seite 187].

KAPITEL 11

Konstruktionen mit Zirkel und Lineal

Für das vorliegende, letzte Kapitel dieser Vorlesung schlagen wir einen Bogen zu dem bereits in der Einleitung erwähnten Zitat von Atiyah (siehe Seite iii), welches die Algebra für ein mächtiges Instrument zum Lösen von (geometrischen) Problemen proklamiert, wenn man geometrische Argumente beiseite legt. In seiner berühmten Arbeit „*Analysis situs*“, in der er die Topologie durch Einführung algebraischer Methoden revolutionierte (Fundamentalgruppe und simpliziale Homologie), schreibt Poincaré:

> „*On a bien souvent répété que la Géométrie est l'art de bien raisonner sur des figures mal faites; [...]*“[1]
>
> — Henri Poincaré [41]

In diesem Kapitel gibt es ebenfalls so manche Abbildung, deren korrekte und stichhaltige Auslegung wohl im Detail noch so manche Mühe fordern könnte. Mithin setzen wir eine gewisse geometrische Intuition stillschweigend voraus und hoffen, dass genügend Vorwissen aus der *Analytischen Geometrie* im Rahmen der *Linearen Algebra* vorhanden ist, sodass Leserinnen und Leser die stellenweise weniger rigorosen Schlüsse, bei denen wir uns auf Schaubilder berufen, nötigenfalls in rigorose Formeln packen könnten, sofern ihnen denn der Sinn danach stünde.

Das vorliegende Kapitel mag auch einen Vorgeschmack auf die Vorlesung „Algebra“ liefern, in welcher insbesondere die Körpertheorie näher studiert wird. Diese wird besonders davon belebt, dass jeder Ringhomomorphismus $f\colon K \to L$ zwischen Körpern K und L den Körper L mit einer K-Vektorraumstruktur ausstattet, indem man eine Skalarmultiplikation $K \times L \to L$ durch $(\lambda, v) \mapsto f(\lambda) \cdot v$ definiert. (In der Sprache der *Algebren*, wie in § 8.5 definiert, wird also jede K-Algebra L zu einem K-Vektorraum.)

Wir vereinfachen diese Betrachtungen für die vorliegenden Untersuchungen, indem wir nur Algebren $f\colon K \to L$ betrachten, bei denen K ein Teilkörper von L ist und $f = \mathrm{id}_L|_K$ die gewöhnliche Inklusion bezeichnet. Tatsächlich ist dies sogar gar keine wesentliche Einschränkung, da jeder Homomorphismus $f\colon K \to L$ zwischen Körpern K und L injektiv ist — denn sein Kern ist ja ein Ideal im Körper K — und man

[1] „*[Negativ zur Vorlesung:] Exkurse in Physik und Französisch (erschwert teilweise das Verständnis, bei wenig bis keinen Kenntnissen in diesen Bereichen)*“ — Rückmeldung einer Studentin oder eines Studenten aus einer anonymen Evaluierung zu einer Vorlesung „Lineare Algebra 2“, in welcher der Verfasser der vorliegenden Notizen dasselbe Zitat von Poincaré angeführt hatte.

darum K mit seinem Bild $f(K) \subseteq L$ in L identifizieren kann. Wir wollen allerdings nicht weiter auf diesen Aspekt eingehen.

11.1. Grad einer Körpererweiterung

Ist K ein Teilkörper des Körpers L, so nennt man dies eine ***Körpererweiterung***.[2] Wir schreiben hierfür L/K und weisen explizit darauf hin, dass dies nicht mit einem Faktorring zu verwechseln ist! (Bei K handelt es sich wegen $1_L = 1_K \in K$ ohnehin nur im Falle $K = L$ um ein Ideal von L.)

Eine Körpererweiterung L/K stattet L in offensichtlicher Weise mit einer K-Vektorraumstruktur aus: Skalarmultiplikation mit „Skalaren“ λ und einem „Vektor“ $v \in L$ ist einfach das gewöhnliche Produkt $\lambda \cdot v$ mit der Körpermultiplikation aus L. Die Dimension $\dim_K L =: [L : K]$ nennt man ***Grad der Körpererweiterung L/K***.

Für eine Körpererweiterung L/K und $x \in L$ bezeichnet man mit $K(x)$ den kleinsten Teil*körper* von L, der $K \cup \{x\}$ als Teilmenge enthält. (Man beachte die runden Klammern; $K[x]$ hingegen bezeichnet den kleinsten Teil*ring* von L, der $K \cup \{x\}$ als Teilmenge enthält.) Eine Körpererweiterung L/K der Form $L = K(x)$ mit einem $x \in L$ nennt man ***einfach***.

Beispiele 11.1. Die folgenden Punkte illustrieren den Grad einer Körpererweiterung. Die darin gemachten Behauptungen zu beweisen sei den Leserinnen und Lesern selbst überlassen (siehe auch Satz 11.3).

(1) $\mathbb{Q}(\mathrm{i}) = \mathbb{Q}[\mathrm{i}] = \{a + b\mathrm{i} \in \mathbb{C} : a, b \in \mathbb{Q}\}$ und $[\mathbb{Q}(\mathrm{i}) : \mathbb{Q}] = 2$.
(2) $\mathbb{C}(\mathrm{i}) = \mathbb{C}$ und $[\mathbb{C}(\mathrm{i}) : \mathbb{C}] = 1$.
(3) $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{C} : a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$ und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
(4) $[\mathbb{C} : \mathbb{R}] = 2$ (mögliche $\mathbb{R}$-Basis: $\{1, \mathrm{i}\}$).
(5) $[\mathbb{C} : \mathbb{Q}] = \infty$ aus Kardinalitätsgründen, da endliche Erweiterungen von $\mathbb{Q}$ (wie man sich überlegen kann) stets abzählbar sind, $\mathbb{C}$ aber überabzählbar ist.

Satz 11.2 (Gradformel). *Sind $K \subseteq L \subseteq L'$ Körper, so gilt $[L' : K] = [L' : L][L : K]$.*

Beweis. Ist $(b_i)_i$ eine K-Basis von L und $(v_j)_j$ eine L-Basis von L', so rechnet man leicht nach, dass $(b_i v_j)_{i,j}$ eine K-Basis von L' ist. In der Tat, ist $x' \in L'$ gegeben, so hat x' eine Darstellung $x' = \sum_j \mu_j v_j$ mit Skalaren $\mu_j \in L$. Gleichermaßen hat jedes μ_j eine Darstellung $\mu_j = \sum_i \lambda_{ij} b_i$ mit Skalaren $\lambda_{ij} \in K$. Einsetzen liefert $x' = \sum_j \sum_i \lambda_{ij} b_i v_j$. Also handelt es sich bei $(b_i v_j)_{i,j}$ um ein K-Erzeugendensystem von L'. Dieses System ist auch linear unabhängig, denn ist $\sum_{i,j} \lambda_{ij} b_i v_j = 0_{L'}$ eine Darstellung des Nullvektors mit Skalaren $\lambda_{ij} \in K$, so ist $\sum_j \big(\sum_i \lambda_{ij} b_i\big) v_j = 0_{L'}$ eine Darstellung des Nullvektors bezüglich der L-Basis $(v_j)_j$ von L', wobei die eingeklammerten Terme als Skalare aus L

[2] Wir weisen abermals darauf hin, dass wir später in der Vorlesung *Algebra* einen beliebigen Ringhomomorphismus $K \to L$ zwischen Körpern K und L als Körpererweiterung bezeichnen werden.

zu interpretieren sind. Die L-lineare Unabhängigkeit von $(v_j)_j$ liefert $\sum_i \lambda_{ij} b_i = 0_L$ für alle j. Mit der K-linearen Unabhängigkeit von $(b_i)_i$ schließt man nun, dass sämtliche λ_{ij} gleich 0_K sein müssen. □

Beispiel. Für $K = \mathbb{Q}$ betrachte

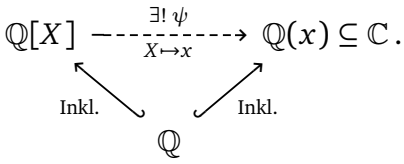
$$L := \mathbb{Q}(\mathrm{i}) = \{\, a + b\mathrm{i} : a, b \in \mathbb{Q} \,\},$$
$$L' := \mathbb{Q}(\mathrm{i}, \sqrt{2}) = \{\, a + b\mathrm{i} + c\sqrt{2} + d\mathrm{i}\sqrt{2} : a, b, c, d \in \mathbb{Q} \,\}.$$

Hierbei ist $\{1, \mathrm{i}\}$ eine $\mathbb{Q}$-Basis von L und $\{1, \sqrt{2}\}$ ist eine L-Basis von L'. Eine $\mathbb{Q}$-Basis von L' ist gegeben durch

$$\{1, \mathrm{i}, \sqrt{2}, \mathrm{i}\sqrt{2}\} = \{\, bv : (b, v) \in \{1, \mathrm{i}\} \times \{1, \sqrt{2}\} \,\}.$$

Wir wollen nun einfache Körpererweiterungen $\mathbb{Q}(x)/\mathbb{Q}$ näher beschreiben und insbesondere verstehen, wie man deren Grad berechnen kann. Das Ergebnis, auf welches wir abzielen ist Satz 11.3 (siehe unten). Es zeigt sich, dass hier Polynomringe eine Schlüsselrolle spielen.

Ist $x \in \mathbb{C}$ beliebig, so gibt es gemäß Satz 7.4 genau einen Ringhomomorphismus $\mathbb{Q}[X] \to \mathbb{Q}(x)$, der X auf x abbildet und das folgende Diagramm kommutativ macht:



Der Kern von ψ ist die Menge aller Polynome $f \in \mathbb{Q}[X]$ mit $f(x) = 0$.[3] Bei $\ker \psi$ handelt es sich um ein Ideal von $\mathbb{Q}[X]$ und dieses ist wegen $1_{\mathbb{Q}[X]} \notin \ker \psi$ von $\mathbb{Q}[X]$ verschieden. Wir unterscheiden zwei Fälle.

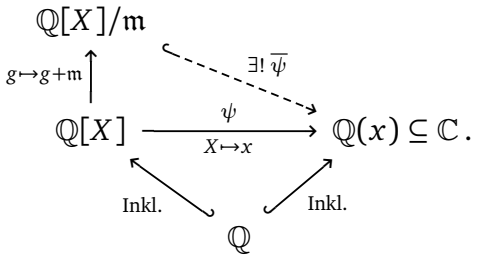
Fall 1: Ist $\ker \psi = \{0_{\mathbb{Q}[X]}\}$, so ist ψ injektiv. Fasst man $\mathbb{Q}[X]$ nun als $\mathbb{Q}$-Vektorraum auf,[4] so sieht man, dass ψ eine injektive $\mathbb{Q}$-*lineare* Abbildung ist. Es folgt $\dim_{\mathbb{Q}} \mathbb{Q}(x) \geq \dim_{\mathbb{Q}} \mathbb{Q}[X] = \infty$, also $[\mathbb{Q}(x) : \mathbb{Q}] = \infty$ (sogar im Sinne von Kardinalzahlen, wobei uns das hier aber nicht interessieren braucht).

Fall 2: Sei nun $\mathfrak{m} := \ker \psi \neq \{0_{\mathbb{Q}[X]}\}$. Da $\mathbb{Q}[X]$ ein Hauptidealbereich ist (siehe Satz 8.2 und Beispiel 8.1), gibt es ein Polynom $f \in \mathbb{Q}[X] \setminus \{0_{\mathbb{Q}[X]}\}$ mit $\mathfrak{m} = \langle f \rangle =$

[3] Man beachte, dass die Auswertung $f(x)$ von f bei x gerade als $\psi(f)$ *definiert* war.

[4] Man vergesse einfach, dass man beliebige Polynome multiplizieren kann und betrachte die Multiplikation mit $\lambda \in \mathbb{Q} \subseteq \mathbb{Q}[X]$ als Skalarmultiplikation.

$f\,\mathbb{Q}[X]$. Gemäß Satz 6.7 erhält man eine Einbettung $\overline{\psi}$ von $\mathbb{Q}[X]/\mathfrak{m}$ nach $\mathbb{Q}(x)$:



Da $\mathbb{Q}(x)$ als Körper natürlich auch ein Integritätsbereich ist, muss $\mathbb{Q}[X]/\mathfrak{m}$ als zu einem Teilring davon isomorpher Ring selbstverständlich auch schon nullteilerfrei sein und $\mathfrak{m}$ ist also ein Primideal von $\mathbb{Q}[X]$. (Dieses Argument ist ein Spezialfall von Aufgabe 10.4.) Dann ist f allerdings ein Primelement von $\mathbb{Q}[X]$, also insbesondere irreduzibel (Lemma 8.5). Laut Proposition 8.8 ist $\mathfrak{m}$ dann sogar ein maximales Ideal und $\mathbb{Q}[X]/\mathfrak{m}$ demnach ein Körper (Korollar 6.10). Nun ist aber $\overline{\psi}(\mathbb{Q}[X]/\mathfrak{m})$ ein Teilkörper von $\mathbb{Q}(x)\subseteq\mathbb{C}$, der $\mathbb{Q}\cup\{x\}$ enthält. Da $\mathbb{Q}(x)$ bereits schon als minimaler solcher Teilkörper (von $\mathbb{C}$) definiert ist, folgt $\overline{\psi}(\mathbb{Q}[X]/\mathfrak{m})=\mathbb{Q}(x)$. Wir haben also $\mathbb{Q}[X]/\mathfrak{m}\cong\mathbb{Q}(x)$ als $\mathbb{Q}$-Algebren, aber insbesondere auch als $\mathbb{Q}$-Vektorräume. Somit ist $[\mathbb{Q}[X]/\mathfrak{m}:\mathbb{Q}]=[\mathbb{Q}(x):\mathbb{Q}]$. Jedoch ist $\dim_{\mathbb{Q}}(\mathbb{Q}[X]/\mathfrak{m})$ einfach zu bestimmen: man rechnet leicht nach, dass die Restklassen modulo $\mathfrak{m}$ der Monome $X^0,X^1,\ldots,X^{\deg f-1}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[X]/\mathfrak{m}$ bilden (Division mit Rest!).

Alle Erzeuger f von $\ker\psi$ sind paarweise assoziiert zueinander (vgl. Korollar 8.4). Insbesondere haben alle diese Erzeuger denselben Grad. Im Falle $\ker\psi\neq\{0_{\mathbb{Q}[X]}\}$ ist dieser Grad ≥ 1 und es gibt genau einen *normierten* Erzeuger von $\ker\psi$ (d.h. mit Leitkoeffizient 1). Diesen nennen wir ***Minimalpolynom von x*** und x nennen wir ***algebraisch***. Wir schreiben oft m_x für das Minimalpolynom einer algebraischen Zahl x. Ist $\ker\psi=\{0_{\mathbb{Q}[X]}\}$, d.h. gibt es kein nichtverschwindendes Polynom $f\in\mathbb{Q}[X]$ mit $f(x)=0$, so nennen wir x ***transzendent***.

Satz 11.3. *Für $x\in\mathbb{C}$ gelten die folgenden Aussagen:*

(1) Ist x algebraisch mit Minimalpolynom m_x, so ist $[\mathbb{Q}(x):\mathbb{Q}]=\deg m_x$.

(2) Ist x transzendent, so ist $[\mathbb{Q}(x):\mathbb{Q}]=\infty$.

Beispiele 11.4.

(1) Ist $x\in\mathbb{Q}$, so ist $X-x$ ein irreduzibles, normiertes Polynom, welches x als Nullstelle besitzt. Es folgt $m_x=X-x$ und also $\deg m_x=1$. Satz 11.3 liefert $[\mathbb{Q}(x):\mathbb{Q}]=1$, was uns auch nicht wundern braucht, da hier $\mathbb{Q}(x)=\mathbb{Q}$ gilt und $\{1\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(x)$ bildet.

(2) $x=\sqrt{2}$ ist Nullstelle des normierten Polynoms X^3-2X, dieses ist allerdings nicht irreduzibel. Ungeachtet dessen folgt aber schon, dass die oben betrachtete Abbildung ψ nicht-trivialen Kern besitzt. Also ist $\sqrt{2}$ jedenfalls algebraisch. Das Minimalpolynom m_x von $\sqrt{2}$ ist der Erzeuger von $\ker\psi\ni X^3-2X$, also ein Teiler von $X^3-2X=(X^2-2)X$. Tatsächlich stellen

wir fest, dass $X^2-2 \in \mathbb{Q}[X]$ irreduzibel (und normiert) ist. Demnach ist das Minimalpolynom von $\sqrt{2}$ gleich X^2-2 und es folgt $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. Wir haben $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2} : a,b\in\mathbb{Q}\}$ und $\{1,\sqrt{2}\}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2})$.

(3) $x=\sqrt[3]{2}$ ist Nullstelle des normierten, irreduziblen[5] Polynoms X^3-2. Es folgt $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. Eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt[3]{2})$ ist durch $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ gegeben.

(4) Die Kreiszahl π ist transzendent nach einem berühmten Ergebnis von Lindemann (1882). Hermite (1873) bewies wenige Jahre zuvor die Transzendenz der Eulerschen Zahl e. Satz 11.3 liefert dann $[\mathbb{Q}(\pi):\mathbb{Q}]=\infty$, wie auch $[\mathbb{Q}(e):\mathbb{Q}]=\infty$.

Man kann zeigen, dass es in einem mengentheoretischen Sinne deutlich mehr transzendente Zahlen gibt, als algebraische. ($\mathbb{Q}[X]$ ist abzählbar und jedes Polynom aus $\mathbb{Q}[X]\setminus\{0_{\mathbb{Q}[X]}\}$ hat nur endlich viele Nullstellen in $\mathbb{C}$; die Menge der algebraischen Zahlen in $\mathbb{C}$ ist demnach abzählbar und ihr Komplement in $\mathbb{C}$, — die Menge der transzendenten Zahlen, — ist darum überabzählbar.)

Man kann auch (mehr oder minder) einfach transzendente Zahlen konstruieren, z.B. die Zahl

$$\sum_{k=1}^{\infty}\frac{1}{10^{k!}} = 0.110001\underbrace{00\ldots00}_{17\text{ Nullen}}1\underbrace{00\ldots00}_{94\text{ Nullen}}10\ldots,$$

welche in ihrer Dezimaldarstellung hinter dem Komma Einsen genau an den Stellen 1, 2, 6, 24, 120, usw. besitzt (und sonst nur Nullen), ist nach einem Ergebnis von J. Liouville transzendent. (Grobe Begründung: man kann sich mit etwas Analysis überlegen, dass nicht-rationale algebraische Zahlen (in einem präzisierbaren Sinne) nicht „zu gut“ durch rationale Zahlen approximierbar sind, aber die Partialsummen der obigen Reihe geben „zu gute“ Approximationen an den Reihengrenzwert, da die Reihenreste sehr rapide klein werden.)

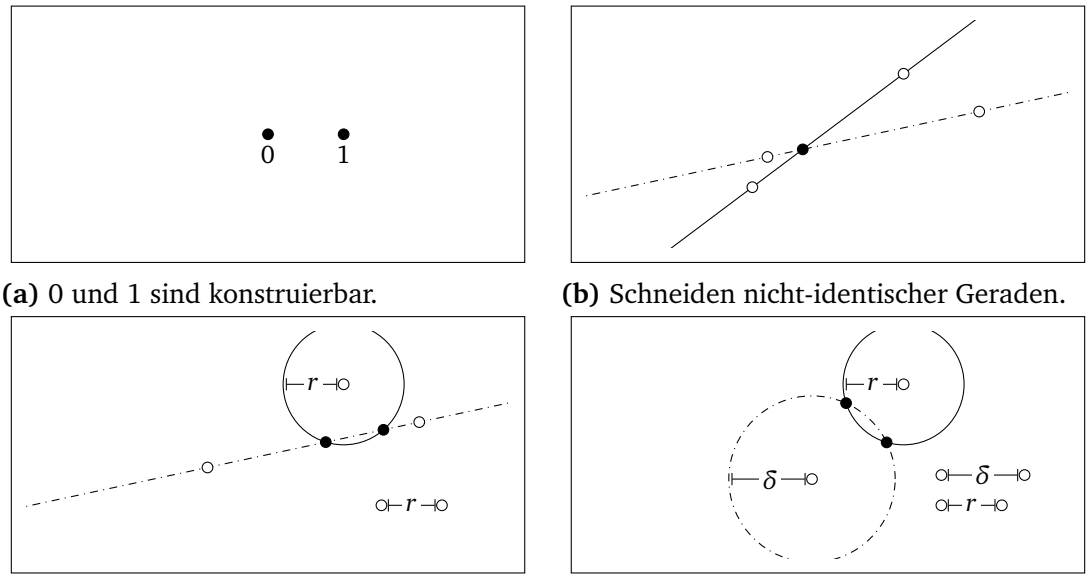
Von einer gegebenen Zahl x nachzuweisen, dass diese transzendent ist, ist im Allgemeinen sehr schwierig. Man muss ja schließlich nachweisen, dass es *kein* Polynom $f\in\mathbb{Q}[X]$ außer dem Nullpolynom mit $f(x)=0$ gibt. Man hat also Eigenschaften von x auszumachen, welche von keiner Nullstelle eines Polynoms ($\neq 0_{\mathbb{Q}[X]}$) geteilt werden. Die in Beispiel 11.4 (4) proklamierte Transzendenz von e und π werden wir hier also nicht beweisen, da uns dies zu tief in die *Analysis* führen würde. Wir verweisen auf [37, Appendix 1] oder [39] für umfangreichere Behandlung.

11.2. Konstruierbare Zahlen

Wir betrachten $\mathbb{C}=\{a+ib : a,b\in\mathbb{R}\}\cong\mathbb{R}^2$ in kartesischen Koordinaten, wobei es sich bei der letzten Isomorphie um eine Isomorphie von $\mathbb{R}$-Vektorräumen

[5] Die Irreduzibilität kann man (wie auch schon bei X^2-2) z.B. mittels des Eisenstein-Kriteriums nachweisen. Alternativ kann man sich auch auf Aufgabe 13.2 berufen, wenn man z.B. mittels Aufgabe T13.3 feststellt, dass die fraglichen Polynome keine rationalen Nullstellen besitzen.

handelt.[6] Auf $\mathbb{R}^2$ hat man auch das gewöhnliche Euklidische Skalarprodukt, welches uns Winkelmessung ermöglicht. Die hiervon induzierte Norm korrespondiert unter der angesprochenen Isomorphie $\mathbb{C} \cong \mathbb{R}^2$ zu dem Absolutbetrag komplexer Zahlen.



(a) 0 und 1 sind konstruierbar.

(b) Schneiden nicht-identischer Geraden.

(c) Schneiden von Geraden und Kreisen.

(d) Schneiden von Kreisen und Kreisen.

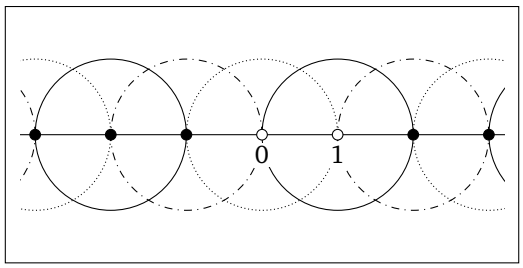
Abbildung 24. Die erlaubten Grundkonstruktionen beim Konstruieren mit Zirkel und Lineal (siehe § 11.2.1).

11.2.1. Erlaubte Grundkonstruktionen. Wir definieren nun die Menge $\mathbb{K} \subseteq \mathbb{C}$ der ***mit Zirkel und Linear konstruierbaren Zahlen*** als jene komplexe Zahlen, die man durch Anwendung von *endlich vielen* der folgenden Schritte erhalten kann:

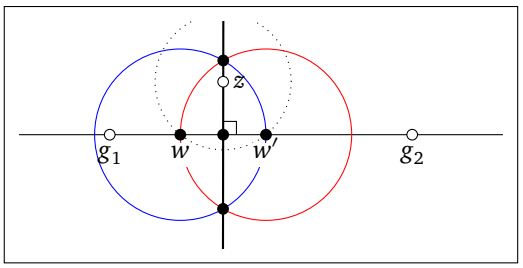
- 0 und 1 sind konstruierbar (siehe Abbildung 24 (a)).
- Ist $z \in \mathbb{C}$ Schnittpunkt zweier nichtidentischer Geraden, wobei jede der Geraden zwei verschiedene konstruierbare Zahlen enthält, so ist auch z konstruierbar (siehe Abbildung 24 (b)).
- Ist $z \in \mathbb{C}$ Schnittpunkt einer Geraden, die zwei verschiedene konstruierbare Zahlen enthält, mit einem Kreis dessen Mittelpunkt eine konstruierbare Zahl ist und dessen Radius Betrag einer konstruierbaren Zahl ist, so ist auch z konstruierbar (siehe Abbildung 24 (c)).
- Ist $z \in \mathbb{C}$ Schnittpunkt zweier nichtidentischer Kreise wie in der obigen Situation, so ist z ebenfalls konstruierbar (siehe Abbildung 24 (d)).

[6] Man beachte, dass das direkte Produkt $\mathbb{R} \times \mathbb{R}$ von *Ringen* hier kein Körper ist, ja nicht mal ein Integritätsbereich: $(1,0) \cdot (0,1) = (1 \cdot 0, 0 \cdot 1) = (0,0) = 0_{\mathbb{R}\times\mathbb{R}}$.

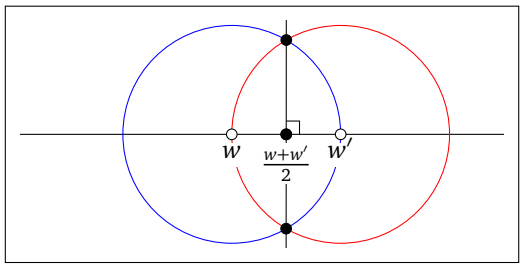
11.2.2. Ableitbare Hilfskonstruktionen. Wir wollen nun die Menge $\mathbb{K}$ der konstruierbaren Zahlen näher studieren. Dafür besprechen wir zunächst einige Hilfskonstruktionen, die mit konstruierbaren Zahlen möglich sind. Wir beziehen uns dafür auch auf die „konstruierbaren Kreise und Geraden“, die wir streng genommen nicht definiert haben, doch sollte deren Definition den Leserinnen und Lesern klar sein.



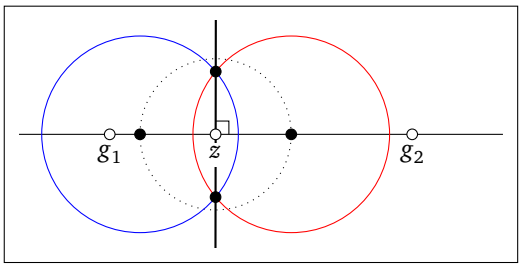
(a) Alle ganzen Zahlen sind konstruierbar (§ 11.2.2.1).



(b) Fällen eines Lotes (§ 11.2.2.2). (Für den hinreichend großen Radius für den gepunkteten Kreis beachte man § 11.2.2.1.)



(c) Mittelpunktskonstruktion (§ 11.2.2.3), vgl. Fällen eines Lotes (§ 11.2.2.2).



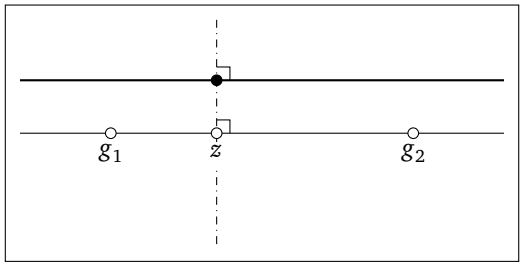
(d) Konstruktion der Senkrechten auf eine Gerade durch einen Punkt (siehe § 11.2.2.4), vgl. Konstruktion des Lotes, § 11.2.2.4.

Abbildung 25. Ableitbare Hilfskonstruktionen beim Konstruieren mit Zirkel und Lineal (siehe § 11.2.2), Teil 1.

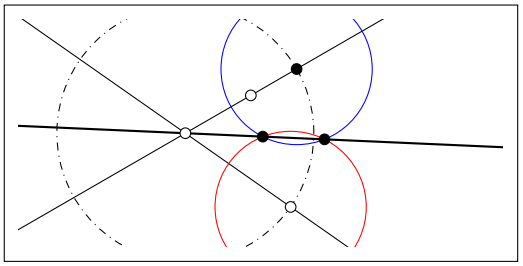
11.2.2.1. *Beliebig große Radien.* Zunächst sei $\mathbb{Z} \subseteq \mathbb{K}$ bemerkt, wie man durch wiederholtes Abtragen der Strecke von 0 auf 1 auf der Geraden durch 0 und 1 sieht (siehe Abbildung 25 (a)). Insbesondere lassen sich beliebig lange Strecken erzeugen, die man als Radien für Kreise verwenden kann.

11.2.2.2. *Lot fällen.* Man kann das Lot von einer konstruierbaren Zahl z auf eine Gerade fällen, welche durch zwei konstruierbare Punkte g_1 und g_2 beschrieben wird, welche z nicht enthält (siehe Abbildung 25 (b)).

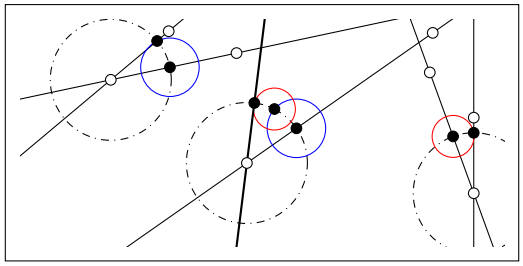
Insbesondere ist der Abstand von z zu der Geraden durch g_1 und g_2 in der obigen Situation eine konstruierbare Zahl. (Man trage diesen auf der Geraden durch 0 und 1 ab.) Man sieht auch, dass es sich bei der zu $z = a+\mathrm{i}b$ $(a, b \in \mathbb{R})$ komplex-konjugierten Zahl $\overline{z} = a - \mathrm{i}b$ um eine konstruierbare Zahl handelt.



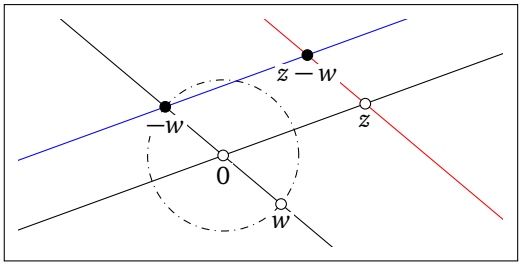
(a) Parallelverschiebung (§ 11.2.2.5).



(b) Winkelhalbierung (§ 11.2.2.6).

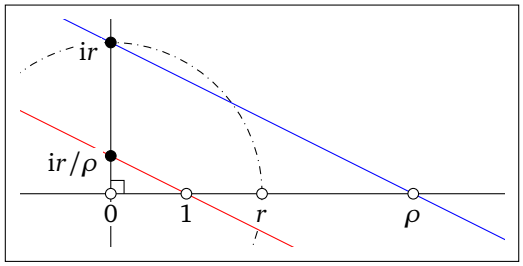


(c) Addition von Winkeln (§ 11.2.2.7).

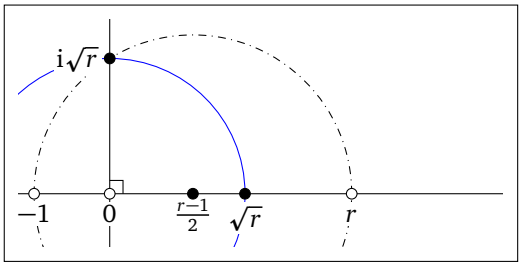


(d) Sind z und w konstruierbar, so auch $z-w$ (§ 11.2.2.8).

Abbildung 26. Ableitbare Hilfskonstruktionen beim Konstruieren mit Zirkel und Lineal (siehe § 11.2.2), Teil 2.



(a) Sind $r, \rho > 0$ konstruierbar, so auch ir/ρ (für eine Verallgemeinerung, siehe § 11.2.2.9).



(b) Konstruktion von Quadratwurzeln (§ 11.2.2.10).

Abbildung 27. Ableitbare Hilfskonstruktionen beim Konstruieren mit Zirkel und Lineal (siehe § 11.2.2), Teil 3.

11.2.2.3. *Mittelpunkte.* Man kann zu je zwei konstruierbaren Punkten w und w' deren Mittelpunkt $(w+w')/2$ konstruieren (siehe Abbildung 25 (c)).

11.2.2.4. *Senkrechte auf eine Gerade durch einen Punkt.* Man kann zu jedem konstruierbaren Punkt z, der auf einer konstruierten Gerade liegt, auch die Senkrechte auf die fragliche Gerade durch z konstruieren (siehe Abbildung 25 (d)).

11.2.2.5. *Parallelverschiebung.* Indem man auf einer konstruierten Senkrechten eine bereits konstruierte Länge abträgt und dort eine weitere Senkrechte konstruiert, kann man eine beliebige Gerade um eine konstruierte Strecke parallelverschieben (siehe Abbildung 26 (a)).

11.2.2.6. *Winkelhalbierende.* Zu zwei sich in z schneidenden, durch konstruierbare Punkte gegebene Geraden lässt sich die Gerade konstruieren, welche z enthält und den[7] Winkel zwischen den beiden Ausgangsgeraden halbiert (siehe Abbildung 26 (b)).

11.2.2.7. *Winkeladdition und Winkelsubtraktion.* Ein Winkel, der von zwei konstruierbaren Geraden eingeschlossen wird, soll konstruierbarer Winkel heißen. Zu je zwei konstruierbaren Winkeln α und β kann man zu jeder konstruierbaren Geraden und jedem konstruierbaren Punkt auf dieser, eine Gerade durch diesen Punkt konstruieren, welche die ursprüngliche Gerade im Winkel $\alpha+\beta$ bzw. $\alpha-\beta$ schneidet (siehe Abbildung 26 (c)).

11.2.2.8. *Subtraktion.* Sind z und w konstruierbar, so ist auch $z-w$ konstruierbar (siehe Abbildung 26 (d)). Die blaue und rote Gerade in der Abbildung entstehen durch Parallelverschiebung (§ 11.2.2.5) der Geraden durch 0 und z bzw. 0 und w um den Abstand von $-w$ bzw. z zu der jeweils ursprünglichen Geraden. Man beachte, dass, wie bei der Erörterung zur Fällung des Lotes (§ 11.2.2.2) erwähnt wurde, die fraglichen Abstände, um die hier parallel-verschoben werden soll, ebenfalls konstruierbar sind.

11.2.2.9. *Division.* Sind $z, w \neq 0$ konstruierbar, so ist auch z/w konstruierbar. In der Tat ist z/w die komplexe Zahl, deren Argument (modulo 2π) die Differenz der Argumente von z und w ist und deren Betrag der Quotient der Beträge von z und w ist. Da wir schon wissen, dass man Winkel subtrahieren kann, genügt es daher zu zeigen, dass man aus den konstruierbaren Zahlen $r=|z|$ und $\rho=|w|$ die Zahl r/ρ konstruieren kann (siehe Abbildung 27 (a)). In der Abbildung entsteht die rote Gerade aus der blauen durch Parallelverschiebung um den Abstand von 1 zur blauen Geraden.

11.2.2.10. *Quadratwurzeln.* Zu einer konstruierbaren Zahl z ist auch jede Lösung der Gleichung X^2-z (also $\pm\sqrt{z}$) konstruierbar. Betrachtet man die Situation nämlich abermals in Polarkoordinaten, so genügt es einen Winkel zu halbieren — was wir schon als möglich nachgewiesen haben —, sowie die Quadratwurzel $\sqrt{r}$ aus der konstruierbaren Zahl $r=|r|$ zu konstruieren. Daraus konstruiert sich dann jedenfalls eine Lösung $\sqrt{z}$ der fraglichen Gleichung und die zweite Lösung bekommt man durch Subtraktion: $-\sqrt{z}=0-\sqrt{z}$; — eine Differenz konstruierbarer Zahlen! Siehe Abbildung 27 (b). Um zu sehen, dass der in der Abbildung mit $\mathrm{i}\sqrt{r}$ beschriftete Punkt wirklich zu Recht diese Beschriftung trägt, also der Schnittpunkt des schwarzen

[7] Zwei sich schneidende Geraden liefern, sofern man diese nicht orientiert, eigentlich i.Allg. zwei Winkel (es sei denn, sie stehen senkrecht). Kombiniert man diese Konstruktion mit der Senkrechten-Konstruktion, so erhält man aber auch die zweite Winkelhalbierende.

Kreises und der vertikalen Achse gleich $\mathrm{i}\sqrt{r}$ ist, muss man nur bemerken, dass

$$\left|\frac{r-1}{2}-\mathrm{i}\sqrt{r}\right|^2=\frac{(r-1)^2}{4}+r=\frac{r^2+2r+1}{4}=\left(r-\frac{r-1}{2}\right)^2=\left|r-\frac{r-1}{2}\right|^2$$

gilt; Alternativ könnte man auch die Punkte -1, r und $z=\mathrm{i}\sqrt{r}$ [ohne den Wert des dritten Punktes wirklich zu kennen] zu einem Dreieck verbinden. Dieses Dreieck ist rechtwinklig gemäß des *Satzes von Thales*. Die Länge $|z|$ der Strecke von 0 zu z ist die Höhe des Dreiecks und diese entspricht gemäß des *Höhensatzes von Euklid* genau der Wurzel aus dem Produkt der Abstände von -1 zu 0 und 0 zu r, also $|z|=\sqrt{1\cdot r}$, wie gewünscht.)

11.2.3. Zusammenfassung. Wir sammeln einige wichtige Erkenntnisse aus den in § 11.2.2 besprochenen Hilfskonstruktionen in dem folgenden Lemma:

Lemma 11.5. *Die Menge $\mathbb{K}$ der konstruierbaren Zahlen bildet einen Teilkörper von $\mathbb{C}$. Dieser ist abgeschlossen unter Ziehung beliebiger Quadratwurzeln, d.h. ist $z\in\mathbb{K}$, so ist auch $\pm\sqrt{z}\in\mathbb{K}$. Zudem ist eine komplexe Zahl z genau dann in $\mathbb{K}$, wenn* $\mathrm{Re}\,z$ *und* $\mathrm{Im}\,z$ *in $\mathbb{K}$ liegen.*

Beweis. Definitionsgemäß ist $0,1\in\mathbb{K}$. Ferner zeigen § 11.2.2.8 und § 11.2.2.9 zusammen mit dem Untergruppenkriterium (Proposition 1.3) $\mathbb{K}\leq(\mathbb{C},+)$ und $\mathbb{K}\setminus\{0\}\leq(\mathbb{C},\cdot)$. Die Abgeschlossenheit unter Ziehung von Quadratwurzeln wurde in § 11.2.2.10 begründet.

Sei nun $z\in\mathbb{K}$. In § 11.2.2.2 hatten wir bereits begründet, dass $\overline{z}$ in $\mathbb{K}$ liegt. Dann liegen aber auch $\mathrm{Re}\,z=\frac{1}{2}(z+\overline{z})$ und $\mathrm{i}\,\mathrm{Im}\,z=\frac{1}{2}(z-\overline{z})$ in $\mathbb{K}$. Wegen $\mathrm{i}\in\mathbb{K}$ ist dann allerdings auch $\mathrm{Im}\,z\in\mathbb{K}$.

Gilt umgekehrt für $z\in\mathbb{C}$, dass $\mathrm{Re}\,z$ und $\mathrm{Im}\,z$ in $\mathbb{K}$ liegen, so auch $z=\mathrm{Re}\,z+\mathrm{i}\,\mathrm{Im}\,z$. □

11.2.4. Charakterisierung konstruierbarer Zahlen. Wir setzen $Q_0:=\mathbb{Q}$ und $Q_{n+1}:=Q_n(\{\sqrt{z}:z\in Q_n\})\subseteq\mathbb{C}$ für $n=0,1,2,\ldots$. Dann ist $Q_0\subseteq Q_1\subseteq Q_2\subseteq\ldots$ eine aufsteigende Kette von Teilkörpern von $\mathbb{C}$. Insbesondere ist $Q:=\bigcup_{n=0}^{\infty}Q_n$ ein Teilkörper von $\mathbb{C}$ und dieser ist abgeschlossen unter Ziehung beliebiger Quadratwurzeln. Tatsächlich ist aus der Konstruktion von Q unmittelbar klar, dass Q der *kleinste* Teilkörper von $\mathbb{C}$ ist, der abgeschlossen unter Ziehung beliebiger Quadratwurzeln ist. Die Elemente von Q sind alle Zahlen, die sich aus arithmetischen Operationen (Addition, Subtraktion, Multiplikation, Division) und Quadratwurzelziehen bilden lassen, z.B. $z_\pm=2(17\pm\sqrt{17})\in Q$ und auch

$$\frac{1}{16}\left(-1+\sqrt{17}+\sqrt{z_-}+2\sqrt{17+3\sqrt{17}-\sqrt{z_-}-2\sqrt{z_+}}\right)\in Q.$$

Proposition 11.6. $\mathbb{K}=Q$.

Beweis. Lemma 11.5 zeigt $Q \subseteq \mathbb{K}$ und es verbleibt lediglich die umgekehrte Inklusion nachzuweisen. Hierzu genügt es einzusehen, dass Q abgeschlossen bezüglich der in § 11.2.1 beschriebenen Grundkonstruktionen ist.

Die komplexe Konjugation $\overline{\cdot}\colon \mathbb{C} \to \mathbb{C}$ ist ein Körperautomorphismus[8] von $\mathbb{C}$. Induktiv zeigt man $\overline{Q_n} = Q_n$ für $n = 0, 1, 2, \ldots$, wobei der Induktionsanfang wegen $Q_0 = \mathbb{Q}$ trivial ist. Für den Induktionsschritt beachte man

$$\begin{aligned}\overline{Q_{n+1}} &= \overline{Q_n(\{\sqrt{z} : z \in Q_n\})} = \overline{Q_n}(\{\overline{\sqrt{z}} : z \in Q_n\}) \\ &= \overline{Q_n}(\{\sqrt{\overline{z}} : z \in Q_n\}) = \overline{Q_n}(\{\sqrt{w} : w \in \overline{Q_n}\}) \\ &= Q_n(\{\sqrt{w} : w \in Q_n\}) = Q_{n+1},\end{aligned}$$

wobei beim Übergang zur letzten Zeile die Induktionsvoraussetzung benutzt wurde. Hieraus ergibt sich $\overline{Q} = Q$. Wie im Beweis von Lemma 11.5 ergibt sich für $z \in \mathbb{C}$ dann $z \in Q \iff \operatorname{Re} z, \operatorname{Im} z \in Q$. Außerdem folgt für $z, w \in Q$ auch $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2} \in Q$ und allgemein $|z - w| \in Q$.

Sind nun z, w, z', w' vier paarweise verschiedene Punkte in Q, so ist die Gerade durch z und w genau $\{\, t(z-w) + w \in \mathbb{C} : t \in \mathbb{R} \,\}$. Analog für die Gerade $\{\, t'(z'-w') + w' \in \mathbb{C} : t' \in \mathbb{R} \,\}$ durch z' und w'. Sind diese beiden Geraden nicht gleich und auch nicht parallel, so ist der (eindeutig bestimmte) Schnittpunkt beider Geraden durch $v = t_0(z-w) + w$ mit

$$t_0 = \frac{w' - w}{z - z' + w' - w}.$$

gegeben. Man sieht $t_0 \in Q$ und also $v \in Q$.

Ganz analog behandelt man das Schneiden einer durch Punkte $z, w \in Q$ definierte Gerade mit einem Kreis, dessen Mittelpunkt in Q liegt und dessen Radius durch $|z' - w'| \in Q$ für zwei Punkte $z', w' \in Q$ gegeben ist. Real- und Imaginärteil von etwaigen Schnittpunkten sind dann über eine lineare und eine quadratische Gleichung miteinander verbunden, wobei die Koeffizienten jeweils Elemente von Q sind. Auflösen dieser Gleichungen führt aber (nach Definition von Q) nicht aus Q heraus und wir erkennen, dass etwaige Schnittpunkte auch in Q liegen.

Das Schneiden zweier Kreise verläuft ähnlich. □

Beispiel. Wir wollen einsehen, dass $x = \cos(2\pi/5)$ konstruierbar ist. Hierfür setzen wir $\zeta_5 = \exp(2\pi \mathrm{i}/5)$. Wegen $\zeta_5^5 = 1$ ist ζ_5 Nullstelle von $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1) = (X-1)\Phi_5$ (vgl. Beispiel 9.14) und wegen $\zeta_5 \neq 0$ folgt

$$\Phi_5(\zeta_5) = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0. \tag{11.1}$$

Nun ist $2x = 2\operatorname{Re}(\zeta_5) = \zeta_5 + \zeta_5^{-1}$. Wir wollen eine algebraische Gleichung für x finden. Hierzu quadrieren wir und erhalten $(2x)^2 = \zeta_5^2 + 2 + \zeta_5^{-2}$. Mit dem Ziel schließlich (11.1) zum Einsatz bringen zu können, betrachten wir $(2x)^2 + 2x =$

[8] Das ist ein bijektiver Ringhomomorphismus dessen Definitions- und Zielbereich derselbe Körper ist.

$\zeta_5^2+\zeta_5+2+\zeta_5^{-1}+\zeta_5^{-2}$ und schließlich $((2x)^2+2x-1)\zeta_5^2 = (\zeta_5^2+\zeta_5+1+\zeta_5^{-1}+\zeta_5^{-2})\zeta_5^2 = \Phi_5(\zeta_5) = 0$. Also haben wir $4x^2+2x-1=0$. Löst man diese Gleichung nun mit der bekannten quadratischen Lösungsformel nach x auf, so erhält man $x = \frac{1}{4}(\sqrt{5}-1)$. Daran erkennt man $x \in Q = \mathbb{K}$ gemäß Proposition 11.6.

Satz 11.7. *Eine komplexe Zahl z ist genau dann konstruierbar, wenn es ein $n \in \mathbb{N}$ und komplexe Zahlen $z_1, \ldots, z_n$ gibt derart, dass die folgenden Eigenschaften erfüllt sind:*

- *Für $K_0 := \mathbb{Q}$ und $K_{i+1} := K_i(z_{i+1})$ $(i = 0, 1, 2, \ldots, n-1)$ gilt $[K_{i+1} : K_i] \leq 2$.*
- *$z \in K_n$.*

Insbesondere ist $[\mathbb{Q}(z) : \mathbb{Q}]$ für jedes $z \in \mathbb{K}$ eine Zweierpotenz.

Beweis. Jedes $z \in \mathbb{K}$ lässt sich durch endlich viele Grundkonstruktionen konstruieren. Real- und Imaginärteil der konstruierten Zahlen $w_1, w_2, \ldots$ genügen dabei jeweils immer einer linearen oder quadratischen Gleichung mit Koeffizienten aus dem Teilkörper von $\mathbb{C}$, der von den bereits konstruierten Zahlen aus $\mathbb{Q}$ erzeugt wird (vgl. den Beweis von Proposition 11.6). Für den Körperturm $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$ kann man dann

$$\mathbb{Q} \subseteq \mathbb{Q}(\mathrm{i}) \subseteq \mathbb{Q}(\mathrm{i}, \operatorname{Re} w_1) \subseteq \mathbb{Q}(\mathrm{i}, \operatorname{Re} w_1, \operatorname{Im} w_1) \subseteq \mathbb{Q}(\mathrm{i}, \operatorname{Re} w_1, \operatorname{Im} w_1, \operatorname{Re} w_2) \subseteq \ldots$$

wählen.

Für die Umkehrung sei $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$ ein Körperturm mit $[K_{i+1} : K_i] \leq 2$ an jeder Stelle. Wir dürfen $[K_{i+1} : K_i] = 2$ annehmen, da sonst $K_i = K_{i+1}$ gilt und dieser Zwischenschritt weggelassen werden kann. Es genügt $K_i \subseteq \mathbb{K}$ per Induktion über $i = 0, 1, 2, \ldots$ zu zeigen. Der Induktionsanfang ist klar. Für den Induktionsschritt beachte man, dass für jedes $w \in K_{i+1} \setminus K_i$ der Körper $K_i(w)$ zwischen K_i und K_{i+1} liegt: $K_i \subsetneq K_i(w) \subseteq K_{i+1}$. Gemäß Satz 11.2 folgt $1 < [K_i(w) : K_i] \leq [K_{i+1} : K_i] = 2$ und somit erfüllt w eine quadratische Gleichung mit Koeffizienten aus $K_i \subseteq \mathbb{K}$. Also gilt $w \in Q = \mathbb{K}$ (beachte die aus der Schule bekannte quadratische Lösungsformel).

Zum Beweis der Zusatzaussage sei $z \in \mathbb{K}$ und $K_0, \ldots, K_n$ seien wie oben definiert. Man beachte, dass $\mathbb{Q}(z)$ wegen $z \in K_n$ ein Teilkörper von K_n. Dann liefern Satz 11.2 und eine triviale Induktion, dass

$$\begin{aligned}[K_n : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}] &= [K_n : \mathbb{Q}] \\ &= [K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_0] = \ldots = \prod_{i=1}^{n} [K_i : K_{i-1}]\end{aligned}$$

eine Zweierpotenz ist. Demnach ist auch $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Zweierpotenz. □

Bemerkung. Man kann zeigen, dass keine der vier komplexen Nullstellen des Polynoms $X^4 + X + 1$ konstruierbar sind. Für jede solche Nullstelle x ist allerdings $[\mathbb{Q}(x) : \mathbb{Q}] = 4$ einer Zweierpotenz. Hierzu äquivalent ist die Behauptung, dass zwischen $\mathbb{Q}$ und $\mathbb{Q}(x)$ kein Körper K mit $[K : \mathbb{Q}] = 2$ passt. Derartige Aussagen lassen sich mit Galois-Theorie beweisen. Wir verweisen auf die Vorlesung „Algebra“ für Details.

11.3. Klassische Konstruktionsprobleme

Wir besprechen hier abschließend einige Anwendungen auf klassische Konstruktionsprobleme.

11.3.1. Regelmäßige n-Ecke. Im Jahre 1796 verblüffte der damals 19-jährige Carl Friedrich Gauß (1777–1855) die mathematische Fachwelt mit einer Entdeckung, welche dem Gebiet der *Elementargeometrie*, die damals seit EUKLIDS Zeiten (ca. 3. Jh. v. Chr.) als abgeschlossen erachteten wurde, neue Wege ebnete.

Bis zur Entdeckung von Gauß, welcher heutzutage als einer der bedeutendsten Mathematiker schlechthin gilt, war nicht bekannt, ob neben den Dreiecken, Vierecken, Fünfecken und Fünfzehnecken, und denen, welche durch Verdopplung von Seitenzahlen entstehen, weitere reguläre Vielecke mit Zirkel und Lineal konstruierbar sind.[9] Gauß fügte dieser Liste unter anderem das regelmäßige Siebzehneck hinzu.

Gauß selbst gab keine Konstruktionsanleitung für die Konstruktion regelmäßiger Siebzehnecke. Seine Demonstration der Konstruierbarkeit fußte alleinig auf der beeindruckenden trigonometrischen Identität

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\Bigg(\sqrt{17}-1+\sqrt{2(17-\sqrt{17})}+ \\ +2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-\sqrt{8(17+\sqrt{17})}}\Bigg). \tag{11.2}$$

Glaubt man diese Identität, so folgt aus Satz 11.7 offenbar die Konstruierbarkeit regelmäßiger 17-Ecke.

Die folgende Konstruktion stammt von Callagy [10]. Man starte mit Punkten $O = 0 \in \mathbb{C}$ und $P = 1 \in \mathbb{C}$ und konstruiere sodann:[10]

(1) Q, R und S (wie in der Abbildung);
(2) A auf OR mit $|OA| = \frac{1}{4}|OR|$;
(3) B und C auf QP derart, dass AB und AC die internen und externen Winkelhalbierenden von OAP sind;
(4) D und E auf OP derart, dass $|CD| = |CA|$ und $|BE| = |BA|$ gilt;
(5) M als Mittelpunkt der Strecke von Q nach D;
(6) F auf OS derart, dass $|MF| = |MQ|$;
(7) G auf dem Halbkreis mit Durchmesser $|OE|$ derart, dass $|OG| = |OF|$ gilt;
(8) H auf OP derart, dass $|EH| = |EG|$ gilt;

[9] Für reguläre Dreiecke und Vierecke ist das leicht ohne große Überlegungen zu erkennen. Für das reguläre Fünfeck beachte man, dass das Beispiel auf Seite 175 die Konstruierbarkeit von $\cos(2\pi/5)$ liefert und somit auch $\exp(2\pi\mathrm{i}/5)$ (der Punkt auf dem Einheitskreis oberhalb von $\cos(2\pi/5)$) konstruierbar ist. Die (also konstruierbaren!) Punkte $\exp(2\pi\mathrm{i}j/5)$ mit $j = 1, 2, 3, 4, 5$ bilden die Eckpunkte eines regulären Fünfecks.

[10] Wir benutzen hier die in der Geometrie übliche Notation, dass für Punkte $A \neq B$ die (eindeutig bestimmte) Gerade, welche durch A und B verläuft, mit AB bezeichnet wird. Ähnlich bezeichnet $|AB|$ den Abstand von A und B.

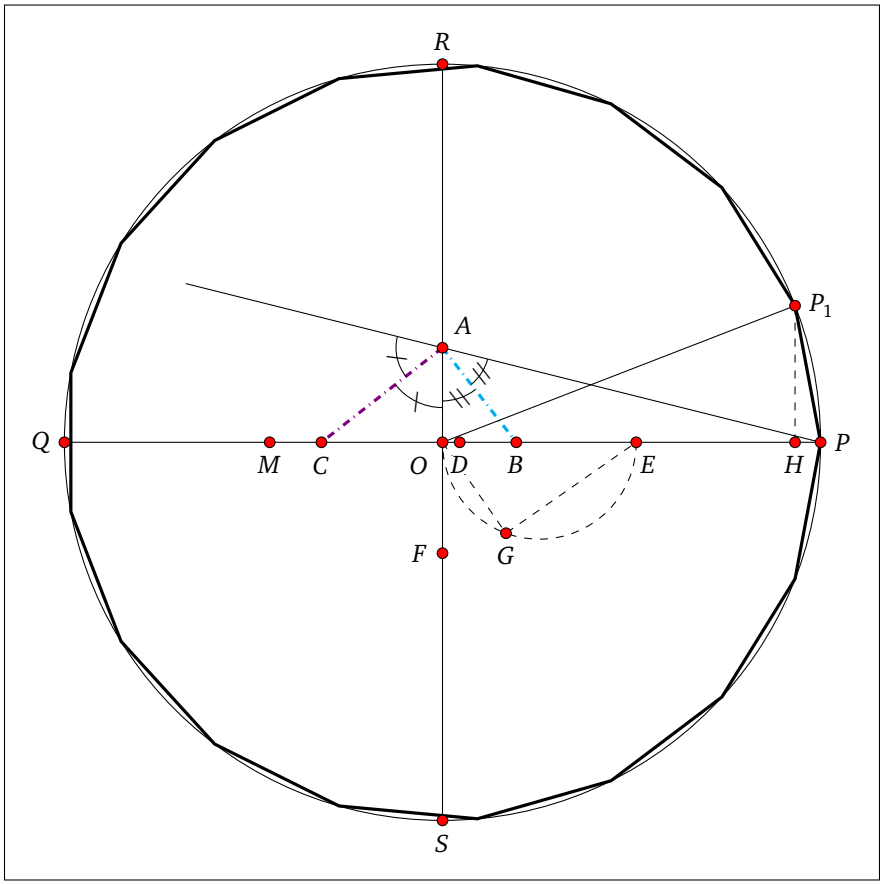


Abbildung 28. Zur Konstruktion eines regulären 17-Ecks nach Callagy [10].

(9) P_1 als Schnittpunkt des Lotes auf OP im Punkt H mit dem Kreis um O mit Radius $|OP|$.

Die Punkte P und P_1 sind nun aufeinander folgende Eckpunkte eines regulären Siebzehnecks mit Schwerpunkt O und Umkreis = Kreis um O mit Radius $|OP|$. Die übrigen Ecken erhält man durch iteriertes Abtragen der Länge $|PP_1|$ auf dem Umkreis.

Eine animierte Darstellung dieser Konstruktion (mit allen dabei benötigten Teilschritten) findet man online unter der folgenden Adresse:

`https://www.math.tugraz.at/~mtechnau/ruler-and-compass.html`

Wir bemühen uns hier nicht um einen Beweis dessen, dass die hier beschriebene Konstruktion tatsächlich ein regelmäßiges 17-Eck liefert. Um dennoch einen kurzen Einblick in das zu geben, was geschieht beachte man, dass es sich bei R tatsächlich um die komplexe Zahl i handelt. Dementsprechend ist $A = \frac{1}{4}\mathrm{i}$ und mit einer kurzen Rechnung zeigt man auch $B = (1+\sqrt{17})^{-1}$, sowie $C = (-1-\sqrt{17})/16$. Anschließend

lässt sich auch

$$D = \frac{1}{16}\left(-1 - \sqrt{17} + \sqrt{2(17+\sqrt{17})}\right)$$

bestätigen, und so fährt man fort, bis hin dazu, dass H die rechte Seite von (11.2) ergibt.

Der zur Durchführung der Konstruktion nötige Aufwand ist beeindruckend und wirft Fragen auf:

(1) *Wie findet man solche Konstruktionen?* Tatsächlich lassen sich diese mit den zuvor beschriebenen Hilfskonstruktionen aus dem oben für $\cos(2\pi/17)$ angegebenen Wurzelausdruck ableiten.
(2) *Wie findet man solche Wurzelausdrücke?*
(3) *Für welche n ist das Auffinden eines solchen Wurzelausdrucks für* $\cos(2\pi/n)$ *möglich?*

Mehr Details gibt es im Rahmen der Vorlesung „Algebra“. Hier beweisen wir jedenfalls, dass man regelmäßige Siebenecke *nicht* mit Zirkel und Lineal konstruieren kann:

Satz 11.8. *Das regelmäßige Siebeneck ist nicht mit Zirkel und Linear konstruierbar.*

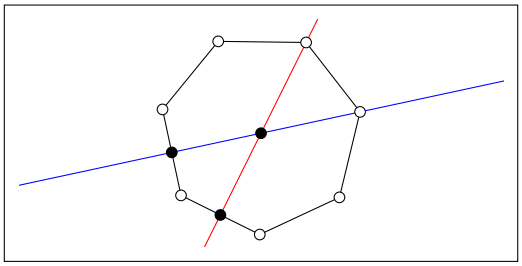
Beweis. Angenommen man könnte ein regelmäßiges Siebeneck konstruieren. Die in Abbildung 29 beschriebenen Argumente zeigen dann, dass die Zahl $\zeta = \exp(2\pi\mathrm{i}/7)$ konstruierbar ist. Diese ist Nullstelle von

$$X^7 - 1 = (X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) =: (X-1)\Phi_7.$$

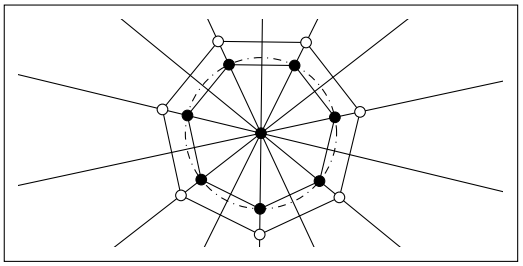
Also ist $\Phi_7(\zeta) = 0$. Andererseits ist Φ_7 aber auch irreduzibel (siehe Beispiel 9.14). Aus Satz 11.3 folgt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$. Dies ist allerdings keine Zweierpotenz, was wegen Satz 11.7 im Widerspruch zur eingangs angenommenen Konstruierbarkeit von ζ steht. □

Der Beweis von Satz 11.8 lässt erahnen, dass die Konstruierbarkeit regelmäßiger n-Ecke viel mit den Nullstellen des Polynoms $X^n - 1$ zu tun hat. In der Vorlesung „Algebra“ beschäftigen wir uns näher damit. Unsere hier benutzte Argumentation lässt sich so zusammenfassen:

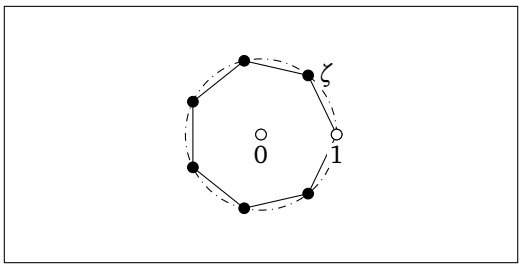
(1) Konstruierbarkeit von $\zeta \in \mathbb{C}$ kann man gemäß Satz 11.7 aus dem Teilkörperverband der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ablesen.
(2) Der Grad $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ ist eine Invariante, welche der Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ zugeordnet ist, und diese erlaubt Rückschlüsse auf den zugehörigen Teilkörperverband. (Gemäß der Gradformel, Satz 11.2, ist der Grad nämlich multiplikativ in Türmen und gewisse Teilerweiterungen spiegeln sich in Form von Teilbarkeitseigenschaften des Grades wieder.)
(3) In günstigen Fällen erhält man somit ausreichend viel Information über den Teilkörperverband von $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$, um die Konstruierbarkeit von ζ ausschließen zu können.



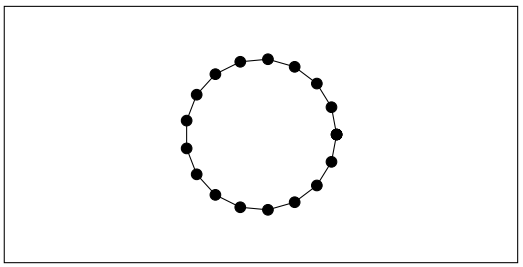
(a) Angenommen, die Eckpunkte eines regelmäßigen 7-Ecks wären konstruierbar. Dann lässt sich auch der Mittelpunkt konstruieren.



(b) Durch Subtraktion des Mittelpunktes lässt sich davon ausgehen, dass dieser der Nullpunkt ist. Durch Schneiden der Geraden durch Mittelpunkt und Eckpunkte mit einem Kreis mit Radius 1 ergibt sich ein normiertes regelmäßiges 7-Eck.



(c) Durch Abtragen der also (hypothetisch!) konstruierbaren Seitenlänge eines normierten 7-Ecks auf dem Einheitskreis erkennt man die vermeintliche Konstruierbarkeit von $\zeta = \exp(2\pi i/7)$.



(d) Erstaunliche Randbemerkung: regelmäßige 17-Ecke kann man — so ein berühmtes Ergebnis von Gauß — konstruieren.

Abbildung 29. Zur (Nicht-)Konstruierbarkeit regelmäßiger 7-Ecke (siehe Satz 11.8).

Es liegt auf der Hand, dass wir nicht erwarten dürfen, mit diesem Argument die konstruierbare Zahlen wirklich vollständig behandeln zu können: der Grad ist eine zu schwache Invariante, um die volle Komplexität des Teilkörperverbandes einer Körpererweiterung abbilden zu können. (Um zu sehen, dass dieses Bauchgefühl auch stimmt, fehlen uns hier jedoch auch die Methoden. Die Bemerkung auf Seite 176 mag aber als weiterer Hinweis dienen.) In der Vorlesung „Algebra“ beschäftigen wir uns damit, eine hinreichend starke Invariante, die sogenannte ***Galois-Gruppe*** $\mathrm{Gal}(L/K)$ einer algebraischen, separablen[11] Körpererweiterung L/K zu konstruieren. Bei dieser handelt es sich um

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L) := \{\, \sigma \in \mathrm{Aut}(L) : \sigma|_K = \mathrm{id}_K \,\},$$

[11] Bei „Separabilität“ handelt es sich um eine technische Bedingung, auf die wir hier nicht näher eingehen.

die sogenannte ***relative Automorphismengruppe*** von L über K. Der sogenannte ***Hauptsatz der Galois-Theorie*** besagt dann im Wesentlichen, dass die Galois-Gruppe von L/K alle Information über den Teilkörperverband von L/K abbildet.

Durch Berechnung der Galois-Gruppen von $\mathbb{Q}(\exp(2\pi\mathrm{i}/n))/\mathbb{Q}$ $(n = 3, 4, 5, \ldots)$ erhält man so genügend Information zur vollständigen Klärung der Frage nach der Konstruierbarkeit regelmäßiger n-Ecke. So beweisen wir im Rahmen der „Algebra"-Vorlesung auch den folgenden berühmten Satz (Satz 11.9). Hierzu noch etwas Sprechweise: eine Primzahl p heißt ***Fermat-Primzahl***, falls $p = 2^k + 1$ für ein $k \in \mathbb{N}$ gilt. Man kann zeigen, dass k dann notwendigerweise eine Zweierpotenz ist. Die Fermat-Primzahlen treten also alle in der Folge der ***Fermat-Zahlen*** $F_n = 2^{2^n} + 1$ $(n = 0, 1, 2, 3, \ldots)$ auf. Die ersten paar Fermat-Zahlen sind

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537,$$
$$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417,$$
$$F_6 = 18\,446\,744\,073\,709\,551\,617 = 274\,177 \cdot 67\,280\,421\,310\,721, \quad \ldots$$

Unter den hier aufgelisteten Fermat-Zahlen sind nur $F_0, \ldots, F_4$ prim. Eine bis heute *offene Vermutung* besagt, dass es sich hierbei um *alle* Fermat-*Prim*zahlen handelt.

Satz 11.9 (Gauß–Wantzel)**.** *Sei $n \geq 3$. Ein reguläres n-Eck lässt sich genau dann mit Zirkel und Lineal konstruieren, wenn $n = 2^\nu p_1 \cdots p_t$ mit $\nu, t \in \mathbb{N}_0$ und verschiedenen Fermat-Primzahlen $p_1, \ldots, p_t$ gilt.*

Bemerkung. Mittels Satz 11.9 und Faktorisieren kleiner Zahlen kommt man darauf, dass für $3 \leq n < 80$ ein regelmäßiges n-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn n in der folgenden Liste von Zahlen vorkommt:

3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68.

11.3.2. Würfelverdopplung. Einer gewissen Anekdote zufolge, wurden die Bewohner der Insel Delos im antiken Griechenland von einem Orakel zwecks der Abwehr einer schweren Seuche dazu aufgefordert, den Würfelförmigen Altar im Apollontempel der Insel in seinem Volumen zu verdoppeln. Mit den hier besprochenen Methoden lässt sich zeigen, dass sich diese Aufgabe, welche ja auf die Konstruktion von $\sqrt[3]{2}$ hinausläuft, nicht allein mit Zirkel und Lineal bewerkstelligen lässt:

Proposition 11.10 (Delisches Problem der Würfelverdopplung)**.** *Es ist unmöglich mit Zirkel und Lineal allein zu gegebener konstruierter Seitenlänge eines Würfels, die Seitenlänge eines Würfels mit doppeltem Volumen zu konstruieren.*

Beweis. Angenommen das Problem wäre doch mit Zirkel und Lineal lösbar. Ganz analog zu den in Abbildung 29 beschriebenen Reduktionen zeigt man, dass dann $\sqrt[3]{2} \in \mathbb{K}$ gelten müsste. Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (siehe Beispiel 11.4 (3)) widerspricht dies allerdings Satz 11.7. □

11.3.3. Quadratur des Kreises. Eine andere berühmte unmögliche Aufgabe ist es, zu einem Kreis mit Radius 1 mittels Zirkel und Lineal ein flächengleiches Quadrat zu konstruieren.

Proposition 11.11 (Quadratur des Kreises)**.** *Die Quadratur des Kreises ist bei bloßer Verwendung von Zirkel und Lineal nicht möglich.*

Beweis. Angenommen doch. Die Seitenlänge des zu konstruierenden Quadrats ist $\sqrt{\pi}$. Man überlegt sich (analog zum Beweis von Satz 11.3) $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] \leq 2$. Wegen $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)][\mathbb{Q}(\pi) : \mathbb{Q}]$ (Satz 11.2) und dem Transzendenzergebnis von Lindemann aus Beispiel 11.4 (4) folgt $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$. Insbesondere ist $\sqrt{\pi} \notin \mathbb{K}$ gemäß Satz 11.7. □

11.3.4. Winkeldreiteilung. Das Problem mit Zirkel und Lineal einen „Winkel zu n-teln“ bedeutet, zu zwei konstruierbaren Geraden, die sich in genau einem Punkt schneiden, eine weitere Gerade zu konstruieren, welche den Schnittpunkt enthält und mit einer der beiden ursprünglichen Geraden genau ein n-tel des ursprünglichen Schnittwinkels einschließt. In § 11.2.2.6 (vgl. Abbildung 26 (b)) haben wir gesehen, dass Winkelhalbierung möglich ist. Durch Wiederholung dieses Verfahrens lassen sich also auch beliebige Winkel 2^k-teln ($k = 1, 2, \ldots$). Da sich Winkel auch addieren lassen (§ 11.2.2.7, Abbildung 26 (c)), lassen sich *gewisse* Winkel auch dritteln („dreiteilen“). Das nächste Ergebnis zeigt jedoch, dass es konstruierbare Winkel gibt, welche sich *nicht* dreiteilen lassen:

Proposition 11.12. *Der Winkel von* $60° = \pi/3$ *ist konstruierbar, kann nicht mit Zirkel und Lineal gedrittelt werden.*

Beweis. Der 60°-Winkel kommt als Innenwinkel eines jeden gleichseitigen Dreiecks vor und solche Dreiecke lassen sich konstruieren (z.B. das Dreieck mit Eckpunkten 0, 1, $\mathrm{i}\sqrt{3}/2$). Wir nehmen nun zwecks Erzeugung eines Widerspruchs an, dass sich ein 60°-Winkel dritten ließe. Dann überlegt man sich, dass $x = \cos(20°)$ konstruierbar sein müsste. Wegen

$$\begin{aligned}\cos(3\alpha) &= \mathrm{Re}(\exp(3\mathrm{i}\alpha)) = \mathrm{Re}(\exp(\mathrm{i}\alpha)^3) = \mathrm{Re}[(\cos(\alpha) + \mathrm{i}\sin(\alpha))^3] \\ &= \cos(\alpha)^3 - 3\cos(\alpha)\sin(\alpha)^2 = \cos(\alpha)^3 - 3\cos(\alpha)(1 - \cos(\alpha)^2) \\ &= 4\cos(\alpha)^3 - 3\cos(\alpha)\end{aligned}$$

ist x eine Nullstelle von $f = 4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X]$ (beachte $\cos(60°) = \frac{1}{2}$). Dieses Polynom ist irreduzibel (benutze Aufgabe 13.2 in Kombination mit Aufgabe T13.3, wobei man wahlweise auch zunächst zum Polynom $2f(X/2) = X^3 - 3X - 1$ übergehen kann, um Rechenarbeit zu sparen). Mit Satz 11.3 folgt $[\mathbb{Q}(x) : \mathbb{Q}] = \deg f = 3$.[12] Insbesondere ist $x \notin \mathbb{K}$ gemäß Satz 11.7. □

[12] Alternativ hätte man auch nachweisen können, dass das Minimalpolynom von $\exp(\pi\mathrm{i}/9)$ gleich $X^6 - X^3 + 1$ ist und also $[\mathbb{Q}(\exp(\pi\mathrm{i}/9)) : \mathbb{Q}] = 6$ gilt.

ANHANG A

Ergänzungen

Im vorliegenden Kapitel besprechen wir einige Anwendungen der Kongruenzrechnung aus Kapitel 6, in der Hoffnung, dass dies deren Nützlichkeit illustriert. Außerdem untersuchen wir in Anhang A.3 den *Ring* $\mathrm{Int}(\mathbb{Z})$ *der ganzwertigen Polynome*. Dieser ist ein Ring mit interessanten Faktorisierungseigenschaften.

A.1. Kryptosysteme und RSA

Wir besprechen eine Anwendung der Algebra auf die Kryptographie.

A.1.1. Kryptosysteme. Ein ***Kryptosystem*** ist ein Fünftupel $(\mathscr{P}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$ bestehend aus

- einer Menge $\mathscr{P}$, dem ***Klartextraum***,
- einer Menge $\mathscr{C}$, dem ***Chiffretextraum***,
- einer Menge $\mathscr{K}$, dem ***Schlüsselraum***,
- einer Familie $\mathscr{E} = \{ E_k : k \in \mathscr{K} \}$ von Funktionen $E_k \colon \mathscr{P} \to \mathscr{C}$, den ***Verschlüsselungsfunktionen***,
- einer Familie $\mathscr{D} = \{ D_k : k \in \mathscr{K} \}$ von Funktionen $D_k \colon \mathscr{C} \to \mathscr{P}$, den ***Entschlüsselungsfunktionen***,

welches zusätzlich die folgende ***Entschlüsselungseigenschaft*** besitzt: Für jedes $e \in \mathscr{K}$ gibt es ein $d \in \mathscr{K}$ mit

$$D_d \circ E_e = \mathrm{id}_{\mathscr{P}}. \tag{A.1}$$

Eine Person („Alice“), die sicher Nachrichten von einer anderen Person („Bob“) empfangen möchte, kann dies wie folgt bewerkstelligen, wenn wir davon ausgehen, dass Alice und Bob sich zuvor auf ein Kryptosystem zur Verständigung geeinigt haben und den Elementen des Klartextraums eine Bedeutung zugewiesen haben, welche von beiden verstanden wird:

(1) Alice generiert zwei Schlüssel $e, d \in \mathscr{K}$ mit der Eigenschaft (A.1);
(2) Alice teilt Bob den Schlüssel e mit; Sofern sich aus e nicht leicht ein d mit (A.1) gewinnen lässt, kann der Schlüssel e sogar an einem öffentlichen Ort hinterlegt werden. Den Schlüssel d merkt sich Alice für später;
(3) Bob kann nun (nach Erhalt des Schlüssels e) einen beliebigen Klartext P mit E_e verschlüsseln: Bob berechnet $E_e(P)$;
(4) Bob verschickt $E_e(P)$ an Alice;

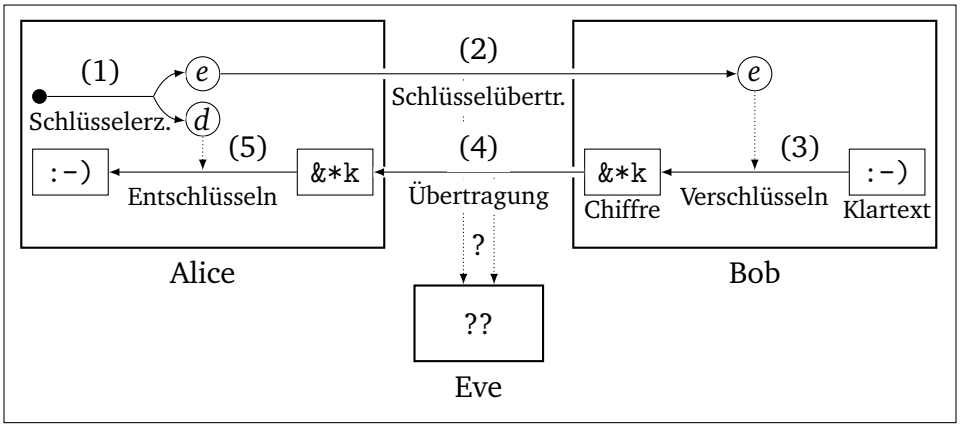


Abbildung 30. Schematische Darstellung der Verwendung eines Kryptosystems.

(5) Alice berechnet nach dem Erhalt von $E_e(P)$ den Wert $D_d(E_e(P))$; Dieser stimmt wegen (A.1) mit P überein.

In der Praxis geht man davon aus, dass eine Person („Eve“), die bei der Kommunikation von Alice und Bob mithören möchte, das benutzte Kryptosystem kennt. Dadurch entstehen diverse Angriffspunkte:

(1) Falls sich zu gegebenem e leicht ein passendes d mit (A.1) berechnen lässt, kann versucht werden den Austausch von e zu belauschen;
(2) Sofern sich Strukturen im Klartext P auf erkennbare Strukturen in $E_e(P)$ übertragen, kann versucht werden daraus P oder teile von P zu rekonstruieren; (Wir gehen davon aus, dass der von Bob verschickte Wert $E_e(P)$ stets komplett abgehört werden kann.)
(3) Unter Umständen kann die Kenntnis von diversen Nachrichten P *und* deren Verschlüsselten Gegenstücken $E_e(P)$ die Möglichkeiten für d soweit eingrenzen, dass man d effizient berechnen kann.

Man sollte beachten, dass all diese Überlegungen eine *praktische* Durchführbarkeit mit einschließen; Beispielsweise darf zu jedem $e \in \mathscr{K}$ das d mit (A.1) durchaus eindeutig bestimmt sein (was die Berechnung von e aus d somit theoretisch stets ermöglicht), solange die Berechnung desselben schwierig ist. Derartige Überlegungen hängen eng mit dem zugrunde gelegten Berechnungsmodell zusammen und stehen daher im Bezug zur *theoretischen Informatik*; Wir können dies hier nicht in einem angemessenen Umfang thematisieren.

A.1.2. Zusammenhang mit Algebra. Durch Gruppierung von Buchstabenfolgen in Blöcke, kann man von einem endlichen Klartextraum ausgehen. Der Wunsch, auf diesem Klartextraum Berechnungen durchzuführen, legt eine Identifizierung von

jenem mit Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ (oder geeigneten Unterstrukturen davon) nahe:[1]

$$\text{„:-)“} \quad \longmapsto \quad [\![29\,2a\,3a]\!]_{16} = 2\,698\,554 \quad \longmapsto \quad (2\,698\,554 \bmod n);$$

Hier kann man nun arithmetische Sätze zur Konstruktion von Kryptosystemen heranziehen. Die Schwierigkeit ein so konstruiertes Kryptosystem zu brechen kann dann beispielsweise dadurch begründet werden, dass ein Brechen des Kryptosystems ein bislang ungelöstes *altes Problem* lösen würde, das schon von vielen Mathematikerinnen und Mathematikern lediglich unzureichend erfolgreich gelöst wurde. (Das ist vielleicht besser, als die Sicherheit des Kryptosystems auf einem *neuen Problem* auszurichten, das man selbst zwar für schwer hält, sich aber bei näherer Betrachtung durch einen Experten vielleicht sofort als trivial entpuppt.)

Die folgenden Untersuchungen stellen Beispiele dar, welche die hier getätigten Aussagen untermauern sollen.

A.1.3. Das RSA-Kryptosystem. Zu verschiedenen Primzahlen p, q und setze man $n = pq$ und definiere ein Kryptosystem[2] $\mathrm{RSA}_n = (\mathscr{P}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$ wie folgt:

- Der Klartextraum $\mathscr{P}$ und Chiffretextraum $\mathscr{C}$ sind beide jeweils
$$\mathscr{P} = \mathscr{C} = \mathbb{Z}/n\mathbb{Z};$$
- Der Schlüsselraum $\mathscr{K}$ ist $\{\, 1 \le k < \varphi(n) : \mathrm{ggT}(k, \varphi(n)) = 1 \,\}$;
- Die Verschlüsselungsfunktionen E_k sind gegeben durch
$$E_k : (x \bmod n) \mapsto (x^k \bmod n);$$
- Die Menge der Entschlüsselungsfunktionen stimme mit der Menge der Verschlüsselungsfunktionen überein.

Satz A.1. RSA_n *ist ein Kryptosystem.*

Beweis. Es gilt nur die Entschlüsselungseigenschaft (A.1) zu verifizieren. Sei also e ein beliebig gewählter Schlüssel. Dazu gibt es einen Schlüssel d mit $ed \equiv 1 \bmod \varphi(n)$. Wir zeigen nun $E_d \circ E_e = \mathrm{id}_{\mathscr{P}}$: Wegen dem Chinesischen Restsatz (Korollar 6.17) ist

$$E_d(E_e(x \bmod n)) \stackrel{!}{=} (x \bmod n) \quad \Longleftrightarrow \quad x^{ed} \stackrel{!}{\equiv} x \mod \begin{cases} p, \\ q. \end{cases}$$

Nach Wahl von d gilt $ed = 1 + m\varphi(n)$ für ein $m \in \mathbb{N}_0$. Ferner gilt

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) \tag{A.2}$$

und daher für $p \nmid x$

$$(x^e)^d = x^{ed} = x^{1+m(p-1)(q-1)} = x \cdot (x^{m(q-1)})^{p-1} \equiv x \cdot 1 = x \mod p$$

[1] Der Text wurde hier mittels der UTF-8-Kodierung in eine Zahl übersetzt.

[2] Benannt nach den Anfangsbuchstaben derjenigen, die diesen Algorithmus im Jahr 1978 publizierten: Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman. Das Verfahren wurde jedoch schon im Jahr 1973 von Clifford Cocks beim Britischen Nachrichtendienst GCHQ vorgeschlagen [11].

nach dem kleinen Satz von Fermat (Korollar 1.10). Gilt $p \mid x$, so gilt trivialerweise auch $(x^e)^d \equiv 0 \equiv x \bmod p$. Eine analoge Rechnung mit q statt p zeigt $(x^e)^d \equiv x \bmod q$. □

Das im Beweis gewählte d wird zum Entschlüsseln benutzt; Zur Berechnung wird $\varphi(n)$ herangezogen. Die Person, die das $n = pq$ für RSA_n wählt, kennt p und q und damit $\varphi(n)$ (siehe (A.2)).

Bemerkung. Ein Angreifer, der e kennt und entschlüsseln möchte, muss *vermutlich* auch $\varphi(n)$ kennen, aber daraus lässt sich bereits die Faktorisierung von n wie folgt bestimmen: Aus (A.2) folgt

$$\varphi(n) = n - (p+q) + 1.$$

Kennt man n und $\varphi(n)$, so kennt man also auch $p+q$ und wegen

$$(p-q)^2 = (p+q)^2 - 4n$$

dann (nach Wurzelziehen) auch $p-q$, also auch $p = \frac{1}{2}((p+q)+(p-q))$ und schließlich auch $q = n/p$. Es gilt also zu vermuten, dass ein Angreifer, der d aus e berechnen möchte, die Zahl n faktorisieren können muss.

Das Problem, eine beliebige Zahl (auch wenn man weiß, dass diese genau zwei Primfaktoren hat) zu faktorisieren, kennt man seit Jahrhunderten, wurde allerdings aber (zumindest nach öffentlichem Wissensstand) bisher noch nicht effizient gelöst.

Bemerkung. Leserinnen und Leser sollten sich darüber im Klaren sein, dass RSA *naiv angewandt* nicht sicher ist: Verschlüsselt man eine Nachricht beispielsweise buchstabenweise,[3] so kann ein Angreifer (der natürlich auch n und e kennt) leicht sämtliche Buchstaben selbst verschlüsseln und deren Werte mit einer abgefangenen Nachricht abgleichen. Außerdem werden kleine Nachrichten $x < n^{1/e}$ durch E_e auf $x^e < n$ abgebildet; Hier kann ein Angreifer leicht die e-te Wurzel in $\mathbb{R}$ ziehen, um x zu erhalten. Für weitere Sicherheitsbedenken sei der Leser auf einschlägige Literatur verwiesen (siehe etwa [8]).

Zur praktischen Durchführung des Verfahrens müssen einige Aspekte geklärt werden:

(1) Wie wählt man „zufällig“ Zahlen?
(2) Wie findet man Primzahlen?
(3) Wie berechnet man $(e \bmod n)^{-1}$?
(4) Wie berechnet man $x^e \bmod n$?

Frage (3) klärt sich über den euklidischen Algorithmus.

Für Frage (4) kann man mittels

$$x^{2e} = (x^2)^e \quad \text{und} \quad x^{2e+1} = (x^2)^e \cdot x$$

die Anzahl der benötigten Multiplikationen logarithmisch in e halten; Reduziert man nach jeder Multiplikation wieder modulo n, so werden die Zwischenergebnisse auch

[3] Buchstaben entsprechen in Kodierungen wie etwa UTF-8 Zahlen und diese kann man, wenn man deren Größe beschränken kann, wiederum durch Restklassen modulo n kodieren.

nie exzessiv groß. Einzelne Multiplikationen und Divisionen (potentiell mit Rest) lassen sich dabei gut praktisch durchführen.

Frage (1) ist vor allem von Relevanz, wenn man das Verfahren einem Computer beibringen möchte und dieser nicht wie ein Mensch würfeln kann. Hierfür ist man vielleicht versucht Zahlenfolgen zu konstruieren, die beispielsweise in bestimmten Restklassen besonders gleichmäßig verteilt sind und somit „zufällig aussehen“; — Wieder ein Frage, die auch Zahlentheoretikinnen und Zahlentheoretiker interessieren mag.

Frage (2) ist natürlich ganz offensichtlich von großem Interesse; Darum betrachten wir diesen Aspekt im Folgenden etwas genauer.

A.2. Miller–Rabin-Primzahltest

Eine zusammengesetzte Zahl n hat stets einen Primteiler p mit $1 < p \leq \sqrt{n}$ und man kann Primalität von n daher naiv durch $\sqrt{n}$ Probedivisionen prüfen. Für große n ist dies allerdings zu aufwändig.

Das Themengebiet der Primzahltests ist äußerst weitläufig. Wir versuchen daher gar nicht, breit darauf einzugehen. Interessierten Leserinnen und Lesern sei das Werk von Cohen [12] ans Herz gelegt, welches sich neben Primzahltests noch mit vielen weiteren algorithmischen Fragen auf der Schnittstelle zwischen Algebra und Zahlentheorie beschäftigt.

Der ***Miller–Rabin-Test*** ist ein *probabilistischer Primzahltest*. Er erkennt bei kontrollierbarem Aufwand eine zusammengesetzte Zahl mit hoher Wahrscheinlichkeit als zusammengesetzt. (Unsere Darstellung orientiert sich stark an [14, „The Miller–Rabin test“].) Der Ausgangspunkt ist die folgende Eigenschaft von Primzahlen:

Proposition A.2. *Zu primem n sei*

$$\begin{cases} s = \nu_2(n-1) = \max\{\, r \in \mathbb{N}_0 : 2^r \text{ teilt } n-1 \,\}, \\ d = (n-1)/2^s. \end{cases} \tag{A.3}$$

Für jede zu n teilerfremde Zahl a gilt dann

$$a^d \equiv 1 \mod n, \tag{A.4}$$

oder es gibt ein $r \in \{0, 1, \ldots, s-1\}$ mit

$$a^{2^r d} \equiv -1 \mod n. \tag{A.5}$$

Beweis. Durch sukzessives Anwenden der Identität $X^2 - 1 = (X+1)(X-1)$ erhält man

$$\begin{aligned} a^{n-1} - 1 = a^{2^s d} - 1 &= \left(a^{2^{s-1} d}\right)^2 - 1 \\ &= \left(a^{2^{s-1} d} + 1\right)\left(a^{2^{s-1} d} - 1\right) \\ &= \left(a^{2^{s-1} d} + 1\right)\left(a^{2^{s-2} d} + 1\right)\left(a^{2^{s-2} d} - 1\right) \\ &\vdots \end{aligned}$$

$$= \big(a^{2^{s-1}d}+1\big)\big(a^{2^{s-2}d}+1\big)\cdots\big(a^{2^0 d}+1\big)\big(a^{2^0 d}-1\big).$$

und wegen dem kleinen Satz von Fermat (Korollar 1.10) wird die linke Seite hierin von n geteilt. Nach dem Lemma von Euklid (Lemma 3.2) teilt n daher einen der Faktoren auf der rechten Seite; Das war zu zeigen. □

Eine prime Restklasse $a \bmod n$ heißt ***Zeuge gegen die Primalität von n***, wenn weder (A.4) noch (A.5) für ein $r \in \{0,1,\ldots,s-1\}$ gilt. Will man nun für eine Zahl n prüfen, ob diese prim ist, so kann man folgende Prozedur benutzen:

(1) Wähle eine zufällige Zahl a mit $1 < a < n$;
(2) Ist $\mathrm{ggT}(a,n) > 1$, so ist n nicht prim;
(3) Ist $a \bmod n$ ein Zeuge gegen die Primalität von n, so ist n nicht prim.

Laut Proposition A.2 gibt es zumindest keine Zeugen gegen die Primalität von Primzahlen; Allerdings ist für zusammengesetztes n nicht unbedingt jedes zu n teilerfremde a mit $1 < a < n$ ein Zeuge:

Beispiel. Für $n = 65 = 2^6+1$ sind die primen Restklassen $a \bmod n$, die *keine* Zeugen gegen die Primalität von n, durch $a \in \{1,8,18,47,57,64\}$ gegeben.

Wir zeigen im Folgenden jedoch, dass es zumindest nicht zu viele „falsche Zeugen“ gibt:

Satz A.3. *Sei $\mathscr{F}_n$ die Menge der primen Restklassen $a \bmod n$, die keine Zeugen für die Nichtprimalität von n sind. Ist n ungerade und zusammengesetzt, so gilt $\#\mathscr{F}_n < (n-1)/2$.*[4]

Wiederholt man die obige Prozedur also mit $(n-1)/2$ verschiedenen Werten von a, so wird die etwaige Nichtprimalität von n sicher erkannt. Führt man die Prozedur jedoch nur k mal mit jeweils zufällig gewähltem a durch, so ist die Wahrscheinlichkeit ein zusammengesetztes n nicht als solches zu erkennen sicher $\le 2^{-k}$. Diese Eigenschaft kann man benutzen, um sich mit wenig Rechenaufwand zu überzeugen, dass eine gegebene Zahl zusammengesetzt oder mit hoher Wahrscheinlichkeit prim ist.

Lemma A.4. *Sei $n = p^\nu$ eine Primzahlpotenz. Dann genügt jede prime Restklasse $a \bmod p^\nu$, die kein Zeuge für die Nichtprimalität von p^ν ist, der Kongruenz*

$$a^{p-1} \equiv 1 \mod p^\nu. \tag{A.6}$$

Beweis. Sei $a \bmod p^\nu$ eine prime Restklasse, die kein Zeuge für die Nichtprimalität von $n = p^\nu$ ist. Dann gilt $a^{\varphi(n)} \equiv 1 \bmod n$ wegen Korollar 1.10, aber auch $a^d \equiv 1 \bmod n$ oder $a^{2^r d} \equiv -1 \bmod n$ für ein $r < s$ (siehe (A.3)); In beiden Fällen folgt

[4] Tatsächlich kann man mit etwas mehr Aufwand sogar $\#\mathscr{F}_n \le (n-1)/4$ zeigen (siehe [43], oder [14, 8]).

$a^{n-1} = a^{2^e d} \equiv 1 \bmod n$. Also gilt

$$\begin{aligned}\operatorname{ord}(a;n) \mid \operatorname{ggT}(\varphi(n), n-1) &= \operatorname{ggT}(p^{\nu-1}(p-1), p^\nu - 1)\\ &= (p-1)\operatorname{ggT}(p^{\nu-1}, 1+p+\ldots+p^{\nu-1})\\ &= p-1,\end{aligned}$$

und daraus folgt (A.6). □

Der Beweis von Satz A.3 basiert nun auf dem folgenden Spezialfall des Satzes von Lagrange (Satz 1.7) aus der Gruppentheorie:

Lemma A.5. *Eine Menge $\mathscr{F}$, die in einer echten Untergruppe U von $(\mathbb{Z}/n\mathbb{Z})^\times$ enthalten ist, enthält höchstens $\varphi(n)/2 \le (n-1)/2$ Elemente.*[5]

Beweis. Der Index $[(\mathbb{Z}/n\mathbb{Z})^\times : U]$ jeder echten Untergruppe U von $(\mathbb{Z}/n\mathbb{Z})^\times$ erfüllt

$$2 \le [(\mathbb{Z}/n\mathbb{Z})^\times : U] = \frac{\#(\mathbb{Z}/n\mathbb{Z})^\times}{\#U}.$$

Zusammen mit $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ folgt die Behauptung. □

Beweis von Satz A.3. Sei n ungerade und zusammengesetzt. Die Zahlen s und d seien wie in (A.3). Wir unterscheiden zwei Fälle:

Fall 1: Ist $n = p^\nu$ ($\nu \ge 2$) eine Primzahlpotenz, so genügt es nach Lemma A.4 und Lemma A.5 zu sehen, dass es sich bei

$$U_n = \{\, a \bmod n : a \text{ erfüllt (A.6)} \,\}$$

um eine echte Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ handelt. Zu diesem Zweck beachte man, dass man leicht mit Induktion und dem binomischen Lehrsatz zeigt, dass $(1+kp^n)^p$ ($k \in \mathbb{Z}$) stets von der Form $1 + k'p^{n+1}$ ($k' \in \mathbb{Z}$ geeignet) ist. ν-fach wiederholtes Anwenden dieser Tatsache zeigt $(1+p)^{p^\nu} \equiv 1 \bmod p^\nu$ und darum $1 < \operatorname{ord}(1+p; p^\nu) \mid p^\nu$ (die Ordnung ist > 1 wegen $\nu \ge 2$). Da für $(a \bmod p^\nu) \in U_n$ stets $\operatorname{ord}(a; p^\nu) \mid (p-1)$ gilt (siehe (A.6)), kann $1+p \bmod p^\nu$ nicht in U_n liegen.

Fall 2: Ist $n = p^\nu n'$ mit einer Primzahlpotenz $p^\nu > 1$ und $p \nmid n' > 1$, so wähle $r_0 \in \{0, \ldots, s-1\}$ maximal derart, dass es $a_0 \in \mathbb{Z}$ mit $a_0^{2^{r_0}} \equiv -1 \bmod n$ gibt. Fixiere ein dazu passendes a_0. (Wegen $(-1)^{2^0} = -1$ ist r_0 zumindest wohl-definiert und a_0 ist außerdem zwangsweise teilerfremd zu n.) Die Menge

$$U_n = \{\, a \bmod n : a^{2^{r_0} d} \equiv \pm 1 \bmod n \,\}$$

ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ und enthält $\mathscr{F}_n$, denn jedes $a \bmod n$ mit (A.4) ist in U_n enthalten und aus (A.5) folgt zumindest $r \le r_0$ wegen der maximalen Wahl von r_0 und dann $a^{2^{r_0} d} \equiv \mp 1 \bmod n$ je nachdem, ob $r = r_0$, oder $r < r_0$; In beiden Fällen ist $(a \bmod n) \in U_n$.

[5] Ist n zusammengesetzt, so ist die letzte Ungleichung offensichtlich sogar strikt.

Wir zeigen nun, dass U_n eine echte Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist. Wegen dem chinesischen Restsatz gibt es ein $a \in \{1, \ldots, n-1\}$ mit

$$a \equiv \begin{cases} a_0 & \bmod p^\nu, \\ 1 & \bmod n'. \end{cases}$$

Wegen $\mathrm{ggT}(a_0, n) = 1$ folgt $\mathrm{ggT}(a, n) = 1$. Ferner ist

$$a^{2^{r_0} d} \equiv a_0^{2^{r_0} d} \equiv (-1)^k \equiv -1 \mod p^\nu$$

und daher $a^{2^{r_0} d} \not\equiv 1 \bmod n$ wegen $-1 \not\equiv 1 \bmod p^\nu$ (beachte, dass $n = p^\nu n'$ als ungerade vorausgesetzt wurde). Analog folgert man aus $a^{2^{r_0} d} \equiv 1 \bmod n'$ und $-1 \not\equiv 1 \bmod n'$ dann $a^{2^{r_0} d} \not\equiv -1 \bmod n$. Also gilt $a^{2^{r_0} d} \not\equiv \pm 1 \bmod n$ und somit $(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^\times \setminus U_n$. Auch hier impliziert Lemma A.5 nun die Behauptung. □

Bemerkung. Im Beweis von Satz A.3 kann man im ersten Fall sogar $U_n = \mathscr{F}_n$ zeigen. D.h. die Bedingung (A.6) in Lemma A.4 charakterisiert $\mathscr{F}_n$. Im zweiten Fall ist zu beachten, dass $U_n \supsetneq \mathscr{F}_n$ gelten kann und $\mathscr{F}_n$ bildet hier auch nicht mehr notwendigerweise eine Gruppe: Etwa im Beispiel auf Seite 188 gilt $(8, 18 \bmod 65) \in \mathscr{F}_{65}$, aber $(8 \cdot 18 \bmod 65) \notin \mathscr{F}_{65}$.

In der Praxis treten nur wenige zusammengesetzte Zahlen n auf, für die keine $a \bmod n$ der Restklassen mit $a = 2, 3, 5, 7, 11 \ldots$ (Primzahlen) ein Zeuge gegen die Primalität von n ist. Beispielsweise wird in [42, Seite 1023] bemerkt, dass ein Test mit $a = 2, 3, 5, 7, 11$ ausreicht, um *alle* zusammengesetzten Zahlen $n < 25 \cdot 10^9$ als solche zu erkennen. Mit mehr Aufwand kommt man noch weiter (siehe etwa [32] für eine vergleichsweise neue Arbeit).

Wir erwähnen noch abschließend, dass bezüglich Primzahltests im Jahre 2002 die lange offene Frage, ob sich Primalität in ***Polynomialzeit***[6] testen lässt, von Agrawal, Kayal und Saxena (A–K–S) positiv beantwortet werden konnte. Für Details verweisen wir auf die (mit dem hier zur Verfügung stehenden Wissen sehr gut lesbare) Originalarbeit [1]. Es ist erwähnenswert, dass der von A–K–S vorgeschlagene Algorithmus eine zusammengesetzte Zahl zwar als solche erkennt, aber keine Faktorisierung von dieser liefert. Ob sich beliebige natürliche Zahlen in Polynomialzeit faktorisieren lassen, ist bis heute noch ein offenes Problem von herausragender Bedeutung (auch mit Blick auf das in Anhang A.1 besprochene RSA-Verfahren).

[6] Was das bedeutet, lernt man in der Vorlesung *Theoretische Informatik*. Dort werden Entscheidungsprobleme spezieller Kenngrößen, wie zum Beispiel der Laufzeit von diese lösenden Algorithmen in Abhängigkeit der Länge der den Algorithmen übergebenen Eingabe, in sogenannte ***Komplexitätsklassen*** eingeteilt. Die Zugehörigkeit von Entscheidungsproblemen zur Polynomialzeitklasse **P** = **PTIME** („Lösbarkeit in Polynomialzeit“) kann man für die Diskussion hier als „für praktische Belange schnell lösbar“ lesen, obwohl diese Vereinfachung auch mit einigen Fußnoten zu versehen wäre.

A.3. Ganzwertige Polynome

In diesem Abschnitt untersuchen wir den Ring $\mathrm{Int}(\mathbb{Z})$ der ***ganzwertigen Polynome***, bestehend aus denjenigen Polynomen $f \in \mathbb{C}[X]$ mit $f(\mathbb{Z}) \subseteq \mathbb{Z}$. Natürlich gilt $\mathbb{Z}[X] \subseteq \mathrm{Int}(\mathbb{Z})$, aber tatsächlich ist diese Inklusion strikt (siehe Beispiel A.7, sowie Proposition A.11 zur Eingrenzung der Rolle von $\mathbb{C}$). Wir charakterisieren $\mathrm{Int}(\mathbb{Z})$ im Folgenden durch Angabe einer $\mathbb{Q}$-Basis. Abschließend stellen wir fest, dass $\mathrm{Int}(\mathbb{Z})$ nicht faktoriell ist und Faktorisierungen in $\mathrm{Int}(\mathbb{Z})$ in irreduzible Elemente sehr wild aussehen können (Korollar A.27); Für mehr sei auf den Übersichtsartikel [9] von Cahen und Chabert verwiesen.

A.3.1. Binomialpolynome. Wir definieren die *Binomialpolynome* durch

$$P_0 := \binom{X}{0} := 1, \quad P_n := \binom{X}{n} := \frac{X(X-1)\cdots(X-n+1)}{n!} = \frac{1}{n!}\prod_{k=0}^{n-1}(X-k) \tag{A.7}$$

für $n = 1, 2, 3, \ldots$; Das folgende Lemma zeigt zwei einfache Eigenschaften der Binomialpolynome:

Lemma A.6.

(1) $\binom{X}{n}$ *ist ein Polynom vom Grad n.*

(2) Für $n, x \in \mathbb{N}_0$ *mit* $0 \le n \le x$ *ist*

$$\binom{X}{n} \text{ ausgewertet bei } x = \text{der Binomialkoeffizient } \binom{x}{n}.$$

Beweis. Das folgt sofort aus der Definition (A.7). □

Man beachte, dass der Binoialkoeffizient auf der rechten Seite in Lemma A.6 (2) nur für $0 \le n \le x$ definiert ist, das Einsetzen von x in das Binomialpolynom auf der linken Seite jedoch für beliebige $x \in \mathbb{Z}$ (oder, allgemeiner: für $x \in \mathbb{C}$) Sinn ergibt.

Zur Einstimmung betrachten wir ein Beispiel.

Beispiel A.7. Das Polynom $P_2 = \binom{X}{2} = \frac{X(X-1)}{2}$ nimmt auf ganzen Zahlen nur ganzzahlige Werte an. In der Tat ist für $x \in \mathbb{Z}$ entweder x oder $x-1$ gerade. Darum ist $x(x-1)/2$ für jedes $x \in \mathbb{Z}$ eine ganze Zahl.

Wir wollen nun das obige Beispiel verallgemeinern.

Satz A.8. *Sei* $n \in \mathbb{N}_0$. *Dann ist das Polynom* $P_n = \binom{X}{n}$ ganzwertig, *d.h. es ist* $P_n(x) \in \mathbb{Z}$ *für alle* $x \in \mathbb{Z}$.

Der Beweis erfolgt mittels Induktion. Zur Vorbereitung führen wir etwas Notation ein. Für ein Polynom $f \in \mathbb{C}[X]$ sei Δf das Polynom $f(X+1) - f(X)$. Wir erhalten somit eine Abbildung $\Delta\colon \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]$.

Lemma A.9. $\Delta\colon \mathbb{C}[X] \to \mathbb{C}[X]$ *ist* $\mathbb{Q}$*-linear, wenn man* $\mathbb{C}[X]$ *in der offensichtlichen Weise als* $\mathbb{C}$*-Vektorraum auffasst. Zudem gilt* $\deg(\Delta f) = (\deg f) - 1$ *für alle* $f \in \mathbb{C}[X] \setminus \{0\}$.

Beweisidee. Nachrechnen. □

Lemma A.10. *Für* $n \in \mathbb{N}$ *gilt* $\Delta\binom{X}{n} = \binom{X}{n-1}$.

Beweis. Für $n = 1$ ist $\Delta P_1 = P_1(X+1) - P_1 = X + 1 - X = 1 = P_0$. Für $n \geq 2$ hat man

$$\begin{aligned}\Delta\binom{X}{n} = \binom{X+1}{n} - \binom{X}{n} &= \frac{1}{n!}\prod_{k=0}^{n-1}(X+1-k) - \frac{1}{n!}\prod_{k=0}^{n-1}(X-k)\\ &= ([X+1]-[X-n+1])\frac{1}{n!}\prod_{\kappa=0}^{n-2}(X-\kappa)\\ &= \frac{1}{(n-1)!}\prod_{\kappa=0}^{(n-1)-1}(X-\kappa) = \binom{X}{n-1}.\end{aligned}$$

□

Beweis von Satz A.8. Wie angekündigt, führen wir eine Induktion über n. Für $n = 0$ ist $P_0 = 1$ trivialerweise ganzwertig. Sei nun also die Ganzwertigkeit von P_{n-1} bereits für ein $n \in \mathbb{N}$ bewiesen. Wir zeigen nun, dass dann auch P_n ganzwertig ist. Genau genommen zeigen wir mittels Induktion, dass $P_n(x)$ für alle $x = 0, 1, 2, \ldots$ ganzwertig ist; Für negative x lässt sich ähnlich argumentieren. Für $x = 0$ ist die Behauptung dank $P_n(0) = 0 \in \mathbb{Z}$ klar (siehe (A.7)). Sei nun für ein $x \in \mathbb{N}_0$ bereits die Ganzzahligkeit von $P_n(x)$ bekannt. Wegen Lemma A.10 haben wir $P_n(x+1) - P_n(x) = P_{n-1}(x)$ für alle $x \in \mathbb{Z}$. Der zweite Summand ($P_n(x)$) ist dank unserer Induktionsannahme in der Induktion über x ganzzahlig und $P_{n-1}(x)$ ist dank unserer Induktionsannahme von der Induktion über n als ganzzahlig bekannt. Daraus folgt $P_n(x+1) = P_{n-1}(x) + P_n(x) \in \mathbb{Z}$. □

A.3.2. Charakterisierung ganzwertiger Polynome. Wir erinnern an die Definition aus Satz A.8. Ein Polynom $P \in \mathbb{C}[X]$ heißt *ganzwertig*, wenn $P(x)$ für alle $x \in \mathbb{Z}$ in $\mathbb{Z}$ liegt. Die Menge aller ganzwertigen Polynome wird mit $\mathrm{Int}(\mathbb{Z})$ bezeichnet. Selbstverständlich sind alle Polynome mit ganzzahligen Koeffizienten ganzwertig, d.h. wir haben $\mathbb{Z}[X] \subseteq \mathrm{Int}(\mathbb{Z})$. Andererseits zeigt Beispiel A.7 bzw. Satz A.8, dass $\mathrm{Int}(\mathbb{Z})$ echt mehr Polynome enthält als $\mathbb{Z}[X]$. Umgekehrt ist natürlich aber auch nicht jedes Polynom mit rationalen Koeffizienten ganzwertig (z.B. $(1/2)X^0 \notin \mathrm{Int}(\mathbb{Z})$). Wir haben daher eine Inklusionskette

$$\mathbb{Z} \subsetneq \mathbb{Z}[X] \subsetneq \mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{C}[X]$$

und alle darin auftretenden Inklusionen sind strikt.

A.3.2.1. *Charakterisierung über Binomialpolynome.* Die folgende Proposition besagt, dass unsere Betrachtung von Polynomen in $\mathbb{C}[X]$ für die Untersuchung ganzwertiger Polynome unnötig allgemein ist: Es genügt, sich auf Polynome mit rationalen Koeffizienten zu beschränken.

Proposition A.11. $\mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{Q}[X]$.

Beweisskizze. Sei $f \in \mathrm{Int}(\mathbb{Z})$. Dann lassen sich die Koeffizienten von f durch Polynominterpolation aus seinen Werten $f(0), f(1), \ldots, f(\deg f)$ rekonstruieren. Da jene Werte nach Voraussetzung alle ganzzahlig sind, liefert die Polynominterpolation allenfalls rationale Koeffizienten. Das zeigt $f \in \mathbb{Q}[X]$. Also gilt $\mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[X]$. Wegen $(1/2)X^0 \notin \mathrm{Int}(\mathbb{Z})$ ist die Inklusion strikt. □

Man kann leicht nachprüfen, dass es sich bei $\mathrm{Int}(\mathbb{Z})$ tatsächlich um einen Teilring von $\mathbb{Q}[X]$ handelt. In diesem Abschnitt zeigen wir die folgende Charakterisierung ganzwertiger Polynome:

Satz A.12. *Die ganzwertigen Polynome sind genau diejenigen Polynome in $\mathbb{Q}[X]$, welche sich als Linearkombination aus den Binomialpolynomen mit ganzzahligen Koeffizienten schreiben lassen; In Zeichen:*

$$\mathrm{Int}(\mathbb{Z}) = \mathrm{span}_{\mathbb{Z}}\left\{ \binom{X}{n} : n \in \mathbb{N}_0 \right\}.$$

A.3.2.2. *Beweis von Satz A.12.* Der Beweis dieses Satzes benötigt noch etwas Vorarbeit, die wir jetzt leisten. Wir definieren nun

$$\Delta^0 := \mathrm{id}_{\mathbb{C}[X]} \quad \text{und} \quad \Delta^k := \underbrace{\Delta \circ \ldots \circ \Delta}_{k \text{ mal}} \quad \text{für } n \in \mathbb{N}.$$

Wir schreiben kurz $\Delta^k f$ für das Bild $\Delta^k(f)$ von f unter der linearen Abbildung Δ^k.

Beispiel A.13. Für $k \in \mathbb{N}$ ist

$$\Delta(X^k) = (X+1)^k - X^k = \sum_{j=0}^{k-1} \binom{k}{j} X^j = \binom{k}{k-1} X^{k-1} + \ldots = kX^{k-1} + \ldots,$$

wobei „…“ für ein Polynom vom Grad $< k$ steht. Insbesondere folgt hieraus

$$\Delta^k X^k = k! = k\text{-te Ableitung von } X^k$$

und

$$\Delta^n X^k = 0 = n\text{-te Ableitung von } X^k$$

für $n > k$. Für ein Polynom f vom Grad $\leq n$ erhalten wir somit $\Delta^n f = f^{(n)}$.

Lemma A.14. *Für $f \in \mathbb{C}[X]$, $x \in \mathbb{Z}$ und $k \in \mathbb{N}_0$ ist*

$$(\Delta^k f)(x) = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} f(x+j).$$

Beweis. Wir betrachten den Verschiebungsoperator $S\colon \mathbb{C}[X] \longrightarrow \mathbb{C}[X]$, $g \mapsto g(X+1)$. Dieser ist offensichtlich linear und wir können Δ als $\Delta = S - \mathrm{id}_{\mathbb{C}[X]}$ schreiben. Also ist Δ^k die k-fache Verkettung von $S - \mathrm{id}_{\mathbb{C}[X]}$. Natürlich kommutiert S mit $-\mathrm{id}_{\mathbb{C}[X]}$ (d.h. es gilt $S \circ (-\mathrm{id}_{\mathbb{C}[X]}) = (-\mathrm{id}_{\mathbb{C}[X]}) \circ S$). Darum lässt sich der Binomische Lehrsatz im Endomorphismenring $\mathrm{End}(\mathbb{C}[X]) \ni -\mathrm{id}_{\mathbb{C}[X]}, S$ anwenden. Wir erhalten daher

$$\Delta^k = (S - \mathrm{id}_{\mathbb{C}[X]})^k = \sum_{j=0}^{k} \binom{k}{j} S^j \circ (-\mathrm{id}_{\mathbb{C}[X]})^{k-j}.$$

Wegen $(S^j f)(x) = f(x+j)$ erhalten wir daraus schon die Behauptung des Lemmas. □

Proposition A.15 (Gregory–Newton-Formel). $f = \sum_{k=0}^{\deg f} (\Delta^k f)(0) \binom{X}{k}$ *für* $f \in \mathbb{C}[X]$.

Beweis. Man rechnet leicht nach, dass es sich bei

$$L\colon \mathbb{C}[X] \longrightarrow \mathbb{C}[X], \quad f \longmapsto \sum_{k=0}^{\deg f} (\Delta^k f)(0) \binom{X}{k},$$

um eine lineare Abbildung handelt. (Dass die obere Summationsgrenze, $\deg f$, vom Argument f von L abhängt, gestaltet den Beweis der Additivitätseigenschaft $L(f+g) = Lf + Lg$, $f, g \in \mathbb{C}[X]$, geringfügig subtiler. Aus Lemma A.9 folgt allerdings, dass $(\Delta f)^k$ für $k > \deg f$ das Nullpolynom ist. Man darf die Summationsobergrenze also beliebig vergrößern und damit gelingt dann auch der Nachweis der fraglichen Additivität.)

Wir wollen einsehen, dass L die identische Abbildung $\mathrm{id}_{\mathbb{C}[X]}$ ist. Vermöge Linearität genügt es, dies auf einem Erzeugendensystem nachzuweisen. Aus Lemma A.6 lässt sich folgern, dass die Binomialpolynome $\binom{X}{n}$, $n = 0, 1, 2, \ldots$, ein Erzeugendensystem von $\mathbb{C}[X]$ bilden. (Tatsächlich bilden diese sogar eine Basis.) Der Beweis des Satzes folgt also, wenn wir $L\binom{X}{n} = \binom{X}{n}$ für alle $n \in \mathbb{N}_0$ nachweisen können. Für $n = 0$ sieht man das direkt durch Einsetzen. Für $n \in \mathbb{N}$ bemühen wir Lemma A.10. Induktiv folgt daraus

$$\Delta^0 \binom{X}{n} = \binom{X}{n}, \quad \Delta^1 \binom{X}{n} = \binom{X}{n-1}, \quad \ldots, \quad \Delta^k \binom{X}{n} = \binom{X}{n-k},$$

für $k = 0, 1, \ldots, n$. Für $k < n$ hat $\binom{X}{n-k}$ aber eine Nullstelle bei 0. Darum gilt

$$L\binom{X}{n} = \sum_{k=0}^{n} \left(\Delta^k \binom{X}{n}\right)(0) \binom{X}{k} = \sum_{k=0}^{n} \binom{X}{n-k}(0) \binom{X}{k} = \binom{X}{n-n}(0) \binom{X}{k} = \binom{X}{k}. \quad \square$$

Beweis von Satz A.12. Linearkombinationen von Binomialpolynomen mit ganzzahligen Koeffizienten sind gemäß Satz A.8 jedenfalls ganzwertig. Das beweist die Inklusion $\supseteq$ von der im Satz behaupteten Gleichung. Für die umgekehrte Inklusion müssen wir zeigen, dass ein jedes ganzwertiges Polynom f sich als Linearkombination

der Binomialpolynome mit ganzzahligen Koeffizienten schreiben lässt. Dafür wenden wir Proposition A.15 an und dürfen ohne Beschränkung der Allgemeinheit davon ausgehen, dass f nicht das Nullpolynom ist. Wir sind natürlich fertig, wenn wir $(\Delta^k f)(0) \in \mathbb{Z}$ für alle $k = 0, 1, \ldots, \deg f$ nachweisen können. Das ist aber klar, denn gemäß Lemma A.14 ist $(\Delta^k f)(0)$ eine Linearkombination von Auswertungen von f bei ganzen Zahlen, gewichtet mit (ganzzahligen!) Binomialkoeffizienten. — Das Ergebnis davon ist natürlich selbst ganzzahlig. □

A.3.2.3. *Ein Kriterium für Ganzwertigkeit.* Die nächste Proposition zeigt, dass man ein Polynom auf Ganzwertigkeit überprüfen kann, indem man dieses auf hinreichend vielen (aber endlich vielen!) ganzen Zahlen auswertet.

Proposition A.16. *Ein Polynom $f \in \mathbb{C}[X]$ vom Grad $n \in \mathbb{N}_0$ ist genau dann ganzwertig, wenn es auf $n+1$ aufeinander folgenden ganzen Zahlen ganzzahlige Werte annimmt.*

Beweis. Sei $f \in \mathbb{C}[X]$ vom Grad $n \in \mathbb{N}_0$ und $a, a+1, \ldots, a+n \in \mathbb{Z}$ mit $f(a), f(a+1), \ldots, f(a+n) \in \mathbb{Z}$. Wir betrachten das Polynom $g = f(a+X)$. Dieses hat ebenfalls Grad n und die Werte $g(0), g(1), \ldots, g(n)$ sind alle ganzzahlig. Aus Proposition A.15 und Lemma A.14 (angewendet auf g) folgt, dass g eine Linearkombination von Binomialpolynomen mit ganzzahligen Koeffizienten ist. Also ist g ganzwertig nach Satz A.12 bzw. gemäß Satz A.8. Wegen $f = g(X-a)$ erhalten wir daraus aber auch schon die Ganzwertigkeit von f. □

Beispiel A.17. Wir hatten in Beispiel A.7 bereits die Ganzwertigkeit des Binomialpolynoms P_2 begründet und jene dann auch in Form von Satz A.8 in größerer Allgemeinheit bewiesen. Um Proposition A.16 zu illustrieren, berechnen wir noch

$$P_2(0) = \frac{0(0-1)}{2} = 0, \quad P_2(1) = \frac{1(1-1)}{2} = 0, \quad P_2(2) = \frac{2(2-1)}{2} = 1.$$

Das Polynom P_2 (mit Grad 2) nimmt also auf 3 aufeinander folgenden ganzen Zahlen ganzzahlige Werte an. Proposition A.16 liefert damit auch die Ganzwertigkeit von P_2. (Das ist aber natürlich kein wirklich unabhängiger Beweis für die Ganzwertigkeit von P_2, da die Ganzwertigkeit der Binomialpolynome, Satz A.8, schon in den Beweis von Proposition A.16 eingeflossen ist.)

Beispiel A.18. Das Polynom $P = (5X + X^3)/6 \in \mathbb{Q}[X]$ ist ganzwertig. Zur Verifikation davon brauchen wir dank Beispiel A.7 nur feststellen, dass es auf -1, 0, 1 und 2 die Werte -1, 0, 1, respektive 3 annimmt, welche ganzzahlig sind. (Man kann auch $P = P_1 + P_2 + P_3$ verifizieren.)

A.3.2.4. *Vergleich von Δ und Differentiation.* Der Ausdruck

$$(\Delta f)(x) = f(x+1) - f(x) = \frac{f(x+1) - f(x)}{(x+1) - x}$$

ist offensichtlich ein Differenzenquotient. Dies legt nahe, dass zwischen Δf und der Ableitung f' von f ein Bezug bestehen könnte. Das folgende Ergebnis bestätigt diesen Verdacht und behandelt auch gleich Δ^k:

Proposition A.19. *Sei $k \in \mathbb{N}$ und $I := [a, a+k] \subset \mathbb{R}$ ein Intervall. Sei $f\colon I \to \mathbb{R}$ eine k-mal differenzierbare Funktion auf dem Intervall I. Dann gibt es einen Punkt $\xi \in (a, a+k)$ mit $(\Delta^k f)(a) = f^{(k)}(\xi)$.*

Beweis. Durch Polynominterpolation erhalten wir ein (eindeutig bestimmtes) Polynom $p \in \mathbb{R}[X]$ vom Grad $\leq k$, welches an den Stellen $a, a+1, \ldots, a+k$ mit f übereinstimmt.

Wir betrachten die Funktion $g\colon I \to \mathbb{R}$, $x \mapsto f(x) - p(x)$. Diese hat Nullstellen bei den $k+1$ Stellen $a, a+1, \ldots, a+k$. Mit dem aus der Analysis bekannten Satz von Rolle erhalten wir also k Nullstellen von g', welche sich auf die Intervalle zwischen den oben genannten $k+1$ Stellen verteilen. Durch Iteration dieses Verfahrens erhalten wir schließlich eine Nullstelle $\xi \in (a, a+k)$ von $g^{(k)}$. Es gilt also

$$0 = g^{(k)}(\xi) = f^{(k)}(\xi) - p^{(k)}(\xi) = f^{(k)}(\xi) - (\Delta^k p)(\xi) = f^{(k)}(\xi) - (\Delta^k p)(a), \tag{A.8}$$

wobei wir für die vorletzte Gleichung das Ergebnis aus Beispiel A.13 benutzt haben und für die letzte Gleichung zum Tagen kommt, dass das Polynom $\Delta^k p$ Grad $\leq k-k = 0$ hat und also konstant ist.

Darüber hinaus gilt wegen Lemma A.14

$$(\Delta^k f)(a) - (\Delta^k p)(a) = (\Delta^k f - \Delta^k p)(a) = (\Delta^k g)(a) = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} g(a+j) = 0.$$

Zusammen mit (A.8) erhalten wir daraus $(\Delta^k f)(a) = (\Delta^k p)(a) = f^{(k)}(\xi)$. □

Bemerkung A.20. Für eine Anwendung von Proposition A.19 siehe [4, S. 10–11, E.10, Teil f]. Für die hiesigen Untersuchungen wird Proposition A.19 aber nicht weiter benötigt.

A.3.3. Faktorisierungstheorie in $\mathrm{Int}(\mathbb{Z})$**.** In Proposition A.11 hatten wir schon gesehen, dass $\mathrm{Int}(\mathbb{Z})$ in $\mathbb{Q}[X]$ enthalten ist. Tatsächlich kann man leicht nachprüfen, dass es sich bei $\mathrm{Int}(\mathbb{Z})$ um einen Teilring von $\mathbb{Q}[X]$ handelt. Wir wollen im Folgenden sehen, dass der Ring $\mathrm{Int}(\mathbb{Z})$ nicht faktoriell ist. Das benötigt wieder etwas Vorbereitung.

A.3.3.1. *Einheiten von* $\mathrm{Int}(\mathbb{Z})$.

Lemma A.21. $\mathrm{Int}(\mathbb{Z}) \cap \mathbb{Z} = \mathbb{Z}$.

Beweis. Offensichtlich ist jede ganze Zahl aufgefasst als Polynom ganzwertig. Ist umgekehrt ein konstantes Polynom $a = aX^0$ ganzwertig, so folgt durch Auswertung bei 1, dass a in $\mathbb{Z}$ liegt. □

Proposition A.22. *Die Einheiten von* $\mathrm{Int}(\mathbb{Z})$ *sind genau die konstanten Polynome* ± 1.

Beweis. Die Polynome ± 1 sind jedenfalls ganzwertig und auch Einheiten. Wir zeigen nun, dass jede Einheit $\epsilon \in \mathrm{Int}(\mathbb{Z})$ gleich 1 oder -1 ist. Sei $\epsilon^{-1} \in \mathrm{Int}(\mathbb{Z})$ das Inverse Element zu ϵ. Aus $1 = \epsilon\epsilon^{-1}$ und der Gradformel folgt $0 = \deg 1 = \deg(\epsilon\epsilon^{-1}) = \deg \epsilon + \deg(\epsilon^{-1})$. Daraus sehen wir, dass ϵ und ϵ^{-1} beide Grad 0 haben. Aus Lemma A.21 folgt, dass ϵ schon eine Einheit in $\mathbb{Z}$ ist. Also ist $\epsilon \in \{-1, 1\}$. □

A.3.3.2. *Einige irreduzible Elemente in* Int($\mathbb{Z}$).

Lemma A.23. *Primzahlen $p \in \mathbb{N}$ sind (aufgefasst als konstante Polynome) irreduzibel in* Int($\mathbb{Z}$).

Beweis. Ist $p = ab$ eine Zerlegung von p in Elemente a, b aus Int($\mathbb{Z}$), so erkennen wir abermals durch Anwendung der Gradformel, dass a und b selbst konstante Polynome sein müssen. Wegen Lemma A.21 ist dann sogar $a, b \in \mathbb{Z}$ und weil p laut Annahme in $\mathbb{Z}$ irreduzibel ist, folgt $a = \pm 1$ oder $b = \pm 1$. Also handelt es sich bei a oder bei b um eine Einheit in $\mathbb{Z}$ (und somit *a-fortiori* um eine Einheit in Int($\mathbb{Z}$)). Also ist p irreduzibel in Int($\mathbb{Z}$). □

Lemma A.24. *Für jedes $a \in \mathbb{Z}$ ist das ganzwertige Polynom $X + a$ irreduzibel in* Int($\mathbb{Z}$).

Beweis. Sei $X + a = fg$ eine Faktorisierung von $X + a$ mit Polynomen $f, g \in \text{Int}(\mathbb{Z})$. Aus der Gradformel folgt, dass für die Grade von f und g nur die Kombinationen $(1,0)$ und $(0,1)$ in Frage kommen. Ohne Beschränkung der Allgemeinheit sei daher $f = bX + c$ und g ein Konstantes Polynom. Dann ist $X + a = fg = bgX + cg$ und ein Vergleich der Leitkoeffizienten zeigt $bg = 1$. Also ist g eine Einheit. Das zeigt, dass $X + a$ irreduzibel in Int($\mathbb{Z}$) ist. □

Satz A.25. *Für $n \in \mathbb{N}$ ist das Binomialpolynom $P_n = \binom{X}{n}$ irreduzibel in* Int($\mathbb{Z}$).

Beweis. Sei $P_n = fg$ eine Faktorisierung von P_n mit Polynomen $f, g \in \text{Int}(\mathbb{Z})$. Schreibe $r = \deg f$, $s = \deg g$. Wegen $n = \deg P_n = \deg(fg) = r + s$ ist $s = n - r$. Gemäß Satz A.12 ist f eine $\mathbb{Z}$-Linearkombination von $P_0, \ldots, P_r$ und g eine $\mathbb{Z}$-Linearkombination von $P_0, \ldots, P_s$. Aus der Definition (A.7) der Binomialpolynome folgt, dass $r!P_j$ für alle $j \leq r$ ein Polynom mit ganzzahligen Koeffizienten ist. Also ist $r!\,s!\,P_n = (r!f)(s!g) \in \mathbb{Z}$. Der Leitkoeffizient a von $r!\,s!\,P_n$ ist aber

$$a = \frac{r!\,s!}{n!} = \frac{r!\,(n-1)!}{n!} = \binom{n}{r}^{-1}.$$

Weil der hier auftretende Binomialkoeffizient jedoch auch eine (positive) ganze Zahl ist, folgt $a = 1$. Daraus folgt aber schon $r = 0$ oder $r = n$, denn die folgende Rechnung zeigt, dass für andere r die Zahl a nicht 1 sein kann:

$$a = \frac{r!\,s!}{n!} = \frac{r!\,(n-1)!}{n!} = \frac{1 \cdot 2 \cdots r}{n(n-1)\cdots(n-r+1)} = \prod_{j=1}^{r} \frac{j}{n-r+j}.$$

Also hat eines der Polynom f oder g Grad 0. Ohne Beschränkung der Allgemeinheit sei dies g, also $(r,s) = (n,0)$. Das Argument aus dem Beweis von Lemma A.24 (Vergleich von Leitkoeffizienten in der Zerlegung $r!\,s!\,P_n = (r!f)(s!g) = (n!f)g$) zeigt, dass g eine Einheit in Int($\mathbb{Z}$) ist. □

A.3.3.3. *Elastizität und Nicht-Faktorialität von* $\mathrm{Int}(\mathbb{Z})$. Sei R nun ein Integritätsbereich in welchem sich jede Nichteinheit $r \in R$, $r \neq 0_R$, als Produkt von (endlich vielen) irreduziblen Elementen schreiben lässt. Sind $p_1 \cdots p_m = q_1 \cdots q_n$ zwei solche Zerlegungen in irreduzible Faktoren von R, so betrachten wir den Buch m/n. Das Supremum über alle derartigen Brüche m/n, die man so aus R erhalten kann, bezeichnet man als die *Elastizität von* R.

Satz A.26. *Die Elastizität von* $\mathrm{Int}(\mathbb{Z})$ *ist unendlich.*

Beweisskizze. Wir zeigen *nicht*, dass sich jede Nichteinheit $\neq 0$ von $\mathrm{Int}(\mathbb{Z})$ als Produkt von irreduziblen Elementen schreiben lässt. Streng genommen bleibt damit also die Frage, ob die Elastizität von $\mathrm{Int}(\mathbb{Z})$ überhaupt definiert ist, offen. Wir zeigen hier nur, dass es Elemente in $\mathrm{Int}(\mathbb{Z})$ mit Faktorisierungen (in irreduzible Elemente) von sehr unterschiedlicher Länge gibt. Aus der Definition (A.7) der Binomialpolynome erhalten wir für $n \in \mathbb{N}$ leicht die Gleichung

$$n\binom{X}{n} = (X - n + 1)\binom{X}{n-1}.$$

Die beiden Faktoren auf der rechten Seite erkennen wir dank Lemma A.24 bzw. Satz A.25 als irreduzibel. Selbiges gilt für den zweiten Faktor auf der linken Seite. Wir wählen nun $n = 2^k$ für $k \in \mathbb{N}$. Dann hat die linke Seite der obigen Gleichung wegen Lemma A.23 eine Produktzerlegung in $k + 1$ irreduzible Faktoren. □

Korollar A.27. *Der Ring* $\mathrm{Int}(\mathbb{Z})$ *ist nicht faktoriell.*

Beweis. In einem faktoriellen Ring haben je zwei Faktorisierungen eines Elements in Produkte irreduzibler Elemente dieselbe Anzahl an Faktoren. Somit ist die Elastizität eines jeden faktoriellen Rings gleich 1. Wegen Satz A.26 kann $\mathrm{Int}(\mathbb{Z})$ also nicht faktoriell sein. □

Bemerkung A.28. Wir hatten im Beweis von Satz A.26 zwar nicht geklärt, ob die Elastizität für $\mathrm{Int}(\mathbb{Z})$ tatsächlich definiert ist, aber für die Anwendung auf Korollar A.27 ist dies tatsächlich unerheblich: Wäre $\mathrm{Int}(\mathbb{Z})$ nämlich faktoriell, so wäre (nach Definition von Faktorialität) auch die Zerlegbarkeit jeder Nichteinheit $\neq 0$ von $\mathrm{Int}(\mathbb{Z})$ in irreduzible Elemente sichergestellt. Der zu Satz A.26 geführte Beweis führt dann aber auf einen Widerspruch.

ANHANG B

Übungsaufgaben

Einige der hier aufgelisteten Aufgaben wurden in Zusammenarbeit mit Nicolas Potthast (Universität Paderborn) erstellt.

1. Übung

1.1. *(Fingerübungen)* (4 Punkte)
Es sei $(G, \circ)$ eine Gruppe mit neutralem Element 1. Beweisen Sie die folgenden Aussagen:
(a) Gilt $a \circ a = 1$ für alle $a \in G$, so ist G abelsch.
(b) Ist $M = \{\, a \in G : a \circ a \circ a = 1 \,\}$ endlich, so ist $\#M$ ungerade.

1.2. *(Schwache Gruppenaxiome)* (4 Punkte)
Es sei G eine Menge, $\circ\colon G \times G \to G$ eine zweistellige Verknüpfung und $1 \in G$ ein fixiertes Element. Ferner mögen die folgenden Eigenschaften gelten:

$$\begin{cases} (1) & \forall a, b, c \in G\colon \quad (a \circ b) \circ c = a \circ (b \circ c), \\ (2) & \forall a \in G\colon \quad a \circ 1 = a, \\ (3) & \forall a \in G\, \exists b \in G\colon a \circ b = 1. \end{cases}$$

(a) Zeigen Sie, dass G mit $\circ$ eine Gruppe bildet.
(b) Zeigen Sie, dass die Aussage aus Teil (a) i.Allg. nicht gültig bleibt, wenn man (3) durch die folgende Eigenschaft (3') ersetzt:

$$(3')\ \ \forall a \in G\, \exists b \in G\colon b \circ a = 1.$$

1.3. *(Ordnung von Elementen)* (4 Punkte)
Es sei $G = \mathrm{GL}_2(\mathbb{R})$ die Gruppe der reellen, invertierbaren 2×2-Matrizen zusammen mit der bekannten Matrixmultiplikation als Verknüpfung. Betrachten Sie

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{sowie} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Bestimmen Sie $\#\{\, X^n : n \in \mathbb{N} \,\}$ für alle $X \in \{A, B, AB\}$.

1.4. *(Fingerübungen, II)* (4 Punkte)
Es sei G eine endliche abelsche Gruppe. Es bezeichne $\pi = \prod_{g \in G} g$ das Produkt aller Elemente von G. (Auf die Reihenfolge der Faktoren kommt es hierbei nicht an, da G als abelsch vorausgesetzt wurde.) Zeigen Sie $\pi^2 = 1_G$.

2. Übung

2.1. *(Untergruppen endlicher Gruppen)* (4 Punkte)

(a) Zeigen Sie: für eine endliche Gruppe $(G, \circ)$ ist eine Teilmenge U von G genau dann eine Untergruppe von G, wenn 1_G in U enthalten ist und für je zwei Elemente $a, b \in U$ deren Produkt $a \circ b$ in U liegt.

(b) Gilt die Aussage aus Teil (a) auch noch, wenn man von $(G, \circ)$ nicht mehr voraussetzt endlich zu sein? (Geben Sie einen Beweis oder ein Gegenbeispiel.)

2.2. *(Turmsatz für den Index)* (4 Punkte)

Es sei $(G, \circ)$ eine Gruppe mit Untergruppen $V \leq U \leq G$. Ferner seien

$$G = \bigcup\!\!\!\cdot_n a_n U, \quad U = \bigcup\!\!\!\cdot_m b_m V,$$

disjunkte Zerlegungen von G und U in Linksnebenklassen. (Die Indizes n und m mögen hier jeweils geeignete Indexmengen durchlaufen.) Zeigen Sie:

(a) $G = \bigcup\!\!\!\cdot_{n,m} a_n b_m V$.

(b) $[G : V] = [G : U][U : V]$, falls G endlich ist.

2.3. *(Obere Schranke für Erzeuger endlicher Gruppen)* (4 Punkte)

Es sei G eine endliche Gruppe und $M := \{g_1, \dots g_n\}$ eine minimale Menge von Erzeugern von G. Zeigen Sie die folgenden Aussagen:

(a) Es gilt $n \leq \log_2(\#G)$.

(b) Für die Gruppe $V = \mathbb{F}_2^n$ (mit der Vektoraddition als Verknüpfung) gilt in (a) die Gleichheit. Man sagt auch, dass die obere Schranke in (a) scharf ist.

(Hinweis: Verwenden Sie in Teil (a) eine Induktion über geeignete Untergruppen und ihre Nebenklassen. Erinnern Sie sich in Teil (b) an die lineare Algebra und die Definition eines Vektorraums.)

2.4. *(Umkehrung des Satzes von Lagrange)* (4 Punkte)

Betrachten Sie die symmetrische Gruppe $\mathfrak{S}_4$ sowie ihre Untergruppe U, die von allen Elementen erzeugt wird, die genau einen Fixpunkt haben. (Das heißt, dass genau ein Element der Menge $\{1, 2, 3, 4\}$ invariant gelassen wird.)

(a) Beweisen Sie, dass $\#U = 12$ gilt.

(b) Beweisen Sie, dass U keine Untergruppe der Ordnung 6 hat.
Insbesondere gilt also die Umkehrung des Satzes von Lagrange, dass es zu jedem Teiler der Ordnung einer Gruppe auch eine Untergruppe mit diesem Teiler als Ordnung gibt, im Allgemeinen nicht.

(Hinweis: Zeigen Sie in Teil (a) zunächst, dass jeder der Erzeuger von U ein Produkt zweier Elemente mit genau zwei Fixpunkten ist. Schließen Sie damit, dass die Elemente von $\mathfrak{S}_4$ mit genau zwei Fixpunkten nicht in U enthalten sein können.
Nehmen Sie in Teil (b) an, dass U eine Untergruppe H der Ordnung 6 besitzt, untersuchen Sie die Nebenklassen $u^n H$ für ein Element $u \in U \backslash H$ mit genau einem Fixpunkt (also einen der Erzeuger von U) und bringen Sie dies zum Widerspruch. Die Existenz eines solchen Elements $u \notin H$ ist natürlich zu begründen.)

3. Übung

3.1. *(Zyklische Gruppen)* (4 Punkte)
Es seien $n, m \in \mathbb{N}$; $(C_n, \oplus)$ bezeichne die Gruppe aus § 1.2.2. Ferner sei t ein Teiler von n und $\varphi(t)$ bezeichne die Anzahl der natürlichen Zahlen k mit $1 \leq k \leq t$ und $\mathrm{ggT}(t,k) = 1$. Zeigen Sie die folgenden Aussagen:

(a) Das direkte Produkt $C_n \times C_m$ ist genau dann zyklisch, wenn n und m teilerfremd sind.

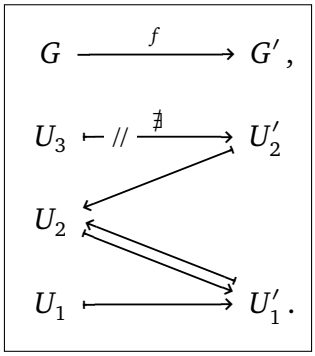
(b) In C_n gibt es genau $\varphi(t)$ Elemente der Ordnung t. (Das ist Satz 1.12 (2).)

Hinweis: Schlagen Sie Lemma 1.9 und Satz 1.12 (1) im Skript nach. Sie dürfen beide Ergebnisse benutzen. Für die auf $C_n \times C_m$ definierte Gruppenstruktur, siehe § 1.2.4.

3.2. *(Untergruppenverbände und Homomorphismen)* (4 Punkte)
Bekanntlich induziert jeder Gruppenhomomorphismus $f\colon G \to G'$ Abbildungen

$$\{\text{Untergruppen } U \text{ von } G\} \underset{f^{-1}(U') \hookleftarrow U'}{\overset{U \mapsto f(U)}{\rightleftarrows}} \{\text{Untergruppen } U' \text{ von } G'\}\,.$$

(Siehe Proposition 2.3 (4).) Finden Sie Gruppen G und G', sowie einen Gruppenhomomorphismus $f\colon G \to G'$ derart, dass es Untergruppen $U_1, U_2 \leq G$ und $U_1', U_2' \leq G'$ gibt, sodass f das folgende Abbildungsverhalten induziert:



D.h. es soll Folgendes gelten:

- $f(U_1) = U_1'$,
- $f^{-1}(U_1') = U_2 = f^{-1}(U_2')$,
- es gibt keine Untergruppe U_3 von G mit $f(U_3) = U_2'$.

3.3. *(Mehr zum Komplexprodukt)* (4 Punkte)
Seien U und V Untergruppen einer Gruppe G. Zeigen Sie:

(a) Die Menge UV ist genau dann eine Untergruppe von G, wenn $UV = VU$ gilt.

(b) Ist U ein Normalteiler von G, so gilt $\langle U \cup V \rangle = UV = VU$.

(c) Sind U und V endlich, so gilt $\#(UV) = \dfrac{\#U \cdot \#V}{\#(U \cap V)}$.

3.4. *(Einige Automorphismengruppen)* (4 Punkte)
Bestimmen Sie zu jeder der folgenden Gruppen jeweils eine „bekannte“ Gruppe, zu welcher diese isomorph ist:
(a) $\mathrm{Aut}(C_2)$,
(b) $\mathrm{Aut}(C_4)$,
(c) $\mathrm{Aut}(C_2 \times C_2)$.
Hinweis: Hier gilt $\#\mathrm{Aut}(C_2 \times C_2) > 4 = \#(C_2 \times C_2)$.

4. Übung

4.1. *(Semidirekte Produkte)* (4 Punkte)
Seien $(G, \bullet)$ und $(H, *)$ Gruppen und $\varphi\colon H \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus. Wir betrachten die binäre innere Verknüpfung

$$\star\colon (G \times H) \times (G \times H) \to G \times H, \quad ((g,h),(g',h')) \mapsto (g \bullet \varphi(h)(g'), h * h')$$

auf $G \times H$. Zeigen Sie:
(a) Die *Menge* $G \times H$ bildet zusammen mit $\star$ eine Gruppe, das sogenannte ***semidirekte Produkt von G mit H bezüglich*** φ. (Man schreibt hierfür $G \rtimes_\varphi H$, um diese vom direkten Produkt $G \times H$ zu unterscheiden, oder kurz $G \rtimes H$, falls der Bezug auf φ klar ist.)
(b) Es sind $G \times \{1_H\} \trianglelefteq G \rtimes H$ und $\{1_G\} \times H \leq G \rtimes H$.
(c) $\{1_G\} \times H \trianglelefteq G \rtimes H$ genau dann wenn $\varphi(h) = \mathrm{id}_G$ für alle $h \in H$ ist, d.h. wenn φ der triviale Homomorphismus $H \to \mathrm{Aut}(G)$ ist.
(d) Ist $N \trianglelefteq G$ und $U \leq G$ mit $N \cap U = \{1_G\}$, so ist $NU \cong N \rtimes_\varphi U$ für $\varphi \in \mathrm{Hom}(U, \mathrm{Aut}(N))$ gegeben durch $\varphi(u) = n \mapsto unu^{-1}$.

4.2. *(Korrespondenzsatz)* (4 Punkte)
Beweisen Sie Satz 2.9: es sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler von G und $\pi\colon G \to G/N$, $g \mapsto gN$, bezeichne die kanonische Projektion. Dann handelt es sich bei der Abbildung

$${}^{\mathrm{a}}\pi\colon \begin{cases} \{\text{Untergruppen } U \leq G/N\} \to \{\text{Untergruppen } V \leq G \text{ mit } V \supseteq N\}, \\ U \mapsto \pi^{-1}(U), \end{cases}$$

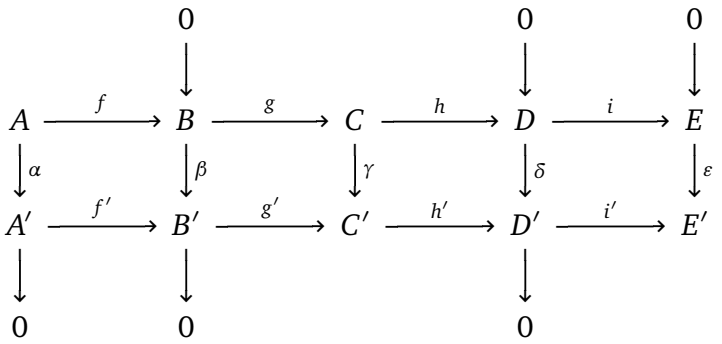
um eine inklusionserhaltende[1] Bijektion, welche sich zu einer Bijektion

$$\{\text{Normalteiler } U \trianglelefteq G/N\} \xrightarrow{1:1} \{\text{Normalteiler } V \trianglelefteq G \text{ mit } V \supseteq N\}$$

einschränkt.

[1] „*Inklusionserhaltend*“ heißt hier: $U \leq U' \leq G/N$ impliziert ${}^{\mathrm{a}}\pi(U) \subseteq {}^{\mathrm{a}}\pi(U')$.

4.3. *(Auf der Jagd nach einem Beweis)* (4 Punkte)
Gegeben sei das folgende kommutative Diagramm von Gruppen und Gruppenhomomorphismen



mit exakten Zeilen und exakten Spalten. Zeigen Sie, dass der darin gezeichnete Gruppenhomomorphismus $C \to C'$ ein Gruppenisomorphismus ist.
(Hinweis: führen Sie Diagrammjagd durch. Beispielsweise zum Nachweis der Injektivität von γ, starten Sie mit einem Element $c \in \ker\gamma \subseteq C$ und zeigen Sie dann $c = 1_C$. Hierzu sollten Sie zeigen, dass sogar $h(c) = 1_D$ gilt und es darum, vermöge Exaktheit, ein $b \in B$ mit $g(b) = c$ gibt. Wenn Sie nun auch noch sehen, dass es ein $a \in A$ mit $f(a) = b$ gibt, so käme $c = g(f(a)) = (g \circ f)(a) = 1_C$ wegen Exaktheit.)

4.4. *(Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches)*(4 Punkte)
Es seien $m, n \in \mathbb{N}_0$ und $a, b \in \mathbb{N}$ beliebig mit $a \mid b$. Das ***kleinste gemeinsame Vielfache*** $\mathrm{kgV}(m,n)$ von m und n ist $\mathrm{kgV}(m,n) = \min(m\mathbb{N} \cap n\mathbb{N})$, falls die Menge, deren Minimum auf der rechten Seite betrachtet nicht leer ist und $\mathrm{kgV}(m,n) = 0$ sonst.

(a) Zeigen Sie $m\mathbb{Z} + n\mathbb{Z} = \mathrm{ggT}(m,n)\mathbb{Z}$ und $m\mathbb{Z} \cap n\mathbb{Z} = \mathrm{kgV}(m,n)\mathbb{Z}$.
(b) Benutzen Sie Satz 2.12, um $\#(a\mathbb{Z}/b\mathbb{Z}) = b/a$ zu zeigen.
(c) Benutzen Sie Satz 2.11, um $\mathrm{ggT}(m,n)\,\mathrm{kgV}(m,n) = mn$ zu zeigen.

5. Übung

5.1. *(Opponierte Gruppen und Rechtsoperationen)* (4 Punkte)
Es sei $(G, \circ)$ eine Gruppe und M eine beliebige Menge. Zeigen Sie:

(a) Die Menge G bildet zusammen mit der Verknüpfung $\bullet\colon G \times G \to G$, $(a,b) \mapsto b \circ a$, eine Gruppe. (Diese Gruppe wird zur Abgrenzung von G auch mit G^{op} bezeichnet und heißt die ***opponierte Gruppe zu G***.)
(b) Die identische Abbildung $G^{\mathrm{op}} \to G$, $g \mapsto g$, ist genau dann ein Gruppenisomorphismus zwischen $(G^{\mathrm{op}}, \bullet)$ und $(G, \circ)$ wenn G abelsch ist.
(c) Es gilt $G^{\mathrm{op}} \cong G$ (sogar wenn G nicht abelsch ist).
(d) Übertragen Sie die Überlegungen aus Proposition 2.13, um eine Bijektion zwischen Gruppen-*Rechts*-Operationen $\triangleleft\colon M \times G \to M$ und der Menge $\mathrm{Hom}(G^{\mathrm{op}}, \mathrm{Sym}(M))$ zu gewinnen.

5.2. *(Projektive lineare Gruppe)* (4 Punkte)
Betrachten Sie den Körper $\mathbb{F}_5$, die lineare Gruppe $\mathrm{GL}_2(\mathbb{F}_5)$ der invertierbaren 2×2-Matrizen sowie die Faktorgruppe $\mathrm{PGL}_2(\mathbb{F}_5) := \mathrm{GL}_2(\mathbb{F}_5)/Z(\mathrm{GL}_2(\mathbb{F}_5))$, die als projektive lineare Gruppe bezeichnet wird.

(a) Zeigen Sie $Z(\mathrm{GL}_2(\mathbb{F}_5)) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{F}_5^\times \right\}$ sowie $|\mathrm{PGL}_2(\mathbb{F}_5)| = 120$.

(b) Zeigen Sie, dass die Gruppe $\mathrm{PGL}_2(\mathbb{F}_5)$ (via Matrixmultiplikation von links) transitiv und treu auf der projektiven Gerade $\mathbb{P}^1(\mathbb{F}_5) = \left(\mathbb{F}_5^2 \setminus \{(0,0)\}\right)/\mathbb{F}_5^\times$ operiert.
(Hinweis: In $\mathbb{P}^1(\mathbb{F}_5)$ betrachten wir die Vektoren aus $\mathbb{F}_5^2 \setminus \{(0,0)\}$ also nur bis auf skalare Vielfache mit Elementen aus $\mathbb{F}_5^\times$. Die Elemente aus $\mathbb{P}^1(\mathbb{F}_5)$ können wir also auch mit den eindimensionalen Untervektorräumen im Vektorraum $\mathbb{F}_5^2$ identifizieren.)

(c) Zeigen Sie $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$.
Hierbei dürfen Sie ohne Beweis verwenden, dass es zu jeder Untergruppe H von $\mathfrak{S}_6$ vom Index $[\mathfrak{S}_6 : H] = 6$ einen Automorphismus $\Phi : \mathfrak{S}_6 \to \mathfrak{S}_6$ gibt, der H isomorph auf die Untergruppe von $\mathfrak{S}_6$ abbildet, deren Elemente alle einen bestimmten Fixpunkt haben.

5.3. *(Struktur von (kleinen) p-Gruppen)* (4 Punkte)
In dieser Aufgabe soll Korollar 2.20 bewiesen werden. G bezeichne eine endliche Gruppe, p sei eine Primzahl und n sei eine natürliche Zahl. Zeigen Sie dann die folgenden Aussagen:

(a) Hat G Ordnung p^n, so hat G ein nichttriviales Zentrum: $Z(G) \supsetneq \{1_G\}$.
(Hinweis: benutzen Sie die Klassengleichung, Korollar 2.19.)

(b) Ist $G/Z(G)$ zyklisch, so ist G abelsch.

(c) Ist $N \leq G$ mit $[G : N] = 2$, so ist $N \trianglelefteq G$.

(d) Hat G Ordnung p^2, so ist G abelsch und es gilt $G \cong C_{p^2}$ oder $G \cong C_p \times C_p$.

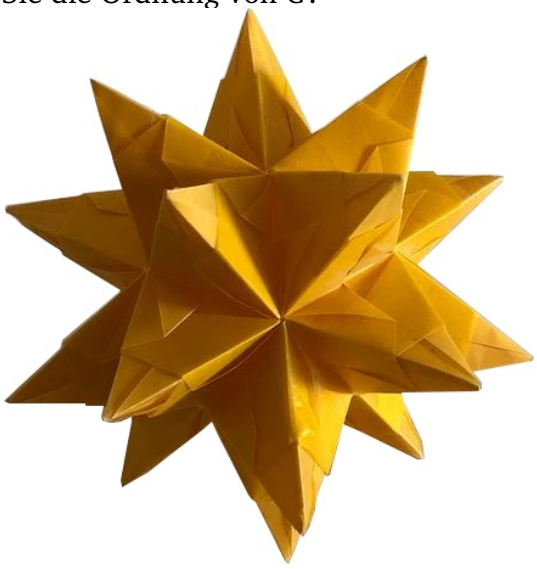
5.4. *(Operationen und Symmetrien: Bascetta-Stern, I)* (4 Punkte)
Bei dem unten abgebildeten Objekt handelt es sich um ein von Paolo Bascetta entworfenes modulares Origami-Modell eines Sterns. Es bezeichne G die Gruppe der Drehungen des dreidimensionalen Raumes, welche den Bascetta-Stern $\mathscr{B} \subseteq \mathbb{R}^3$ invariant lassen, wobei $\mathscr{B}$ als angemessen idealisiert anzusehen ist, sodass Faltungenauigkeiten vernachlässigt werden können.

(a) Falten Sie einen Bascetta-Stern gemäß der im PANDA-Kurs verfügbaren Anleitung.
(Hinweis: Auf einschlägigen Videoplattformen findet man ebenfalls Anleitungen. Es gibt 2 Bonuspunkte für die Gruppe, welche den kleinsten Stern abgibt und 2 Bonuspunkte für die Gruppe, die den größten Stern abgibt. Falls sich keine solche Gruppe eindeutig identifizieren lässt, verfallen die jeweiligen Bonuspunkte. Pro Gruppe darf nur ein Stern abgegeben werden. Bitte, denken Sie bei der Abgabe daran, auf geeignete Weise Ihre Namen kenntlich zu machen, damit Sie die Sterne zu Beginn der Präsenzübungen am 19. und 20. November zurückbekommen können. Die Abgabe des Sterns erfolgt bei Nicolas Potthast bis zum 18. November. — Siehe PANDA für mögliche Zeitfenster.)

Die folgenden Aufgaben werden in den Präsenzübungen besprochen (Aufgabe T6.1) und werden *nicht* bepunktet. Sie können Ihr gebasteltes Modell aber schon zuhause nutzen, um über diese Aufgaben nachzudenken:

(b) Zeigen Sie, dass G treu auf $\mathscr{B}$ operiert und endlich ist.

(c) Bestimmen Sie die Ordnung von G.



6. Übung

6.1. *(Färbungen eines Quadrats)* (4 Punkte)

Die Gruppen C_4 und $D_{2\cdot 4}$ operieren auf den Ecken E eines Quadrats durch Drehung bzw. Drehung und Spiegelung (vgl. das Beispiel über Satz 2.16, sowie Aufgabe T5.1).

(a) Bestimmen Sie die Anzahl der verschiedenen Färbungen von E mit drei[2] Farben unter der Operation von C_4.

(b) Bestimmen Sie die Anzahl der verschiedenen Färbungen von E mit drei Farben unter der Operation von $D_{2\cdot 4}$.

(c) Geben Sie zwei Färbungen von E mit drei Farben an, welche unter der Operation von C_4 zu verschiedenen Bahnen gehören, aber bezüglich der Operation von $D_{2\cdot 4}$ in derselben Bahn liegen.

6.2. *(Untergruppen von $\mathfrak{S}_5$)* (4 Punkte)

(a) Finden Sie ein Element $\sigma \in \mathfrak{S}_5$ mit Ordnung 6.

(b) Zeigen Sie, dass $\mathfrak{S}_5$ kein Element mit Ordnung 15 enthält.
(Hinweis: für $\sigma \in \mathfrak{S}_5$ operiert die Gruppe $\langle\sigma\rangle$ auf $M = \{1, \ldots, 5\}$ durch Funktionsauswertung. Überlegen Sie sich, wie die Ordnung von σ mit den Bahnen zusammenhängt, in welche M unter der genannten Operation zerfällt.)

[2] Färbungen, bei denen nicht alle drei Farben wirklich benutzt werden, sollen hier ebenfalls gezählt werden.

(c) Zeigen Sie, dass $\mathfrak{S}_5$ keine Untergruppe der Ordnung 15 enthält, obwohl 15 ein Teiler von $\#\mathfrak{S}_5 = 5! = 120 = 15 \cdot 8$ ist.
(Hinweis: Sie dürfen ohne Beweis die aus Proposition 3.5 folgende Tatsache benutzen, dass jede Gruppe der Ordnung 15 zyklisch ist.)

6.3. *(Exponentialbewertung)* (4 Punkte)
Es sei p eine Primzahl. Für $n \in \mathbb{Z}$ definiere dann $\nu_p(n) := \sup\{\, \nu \in \mathbb{N}_0 : p^\nu \text{ teilt } n \,\}$. (Für alle $n \neq 0$ darf man „sup“ durch „max“ ersetzen; für $n = 0$ hat man $\nu_p(0) = +\infty$.)

(a) Zeigen Sie: für $a, b \in \mathbb{Z}$ gilt $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
(Hinweis: Für $ab = 0$ gilt die obige Gleichung bei richtiger Konventionswahl auch, Sie dürfen sich aber auf den Fall $ab \neq 0$ beschränken. „$\geq$“ ist nicht schwierig. Für die umgekehrte Ungleichung kann man mittels Lemma 3.2 argumentieren.)

(b) Im Beweis von Satz 3.1 kam die folgende Aussage vor (mit Notation wie dort):

> *$G(\mathcal{M}_0)$ sei eine Bahn, deren Länge $\#G(\mathcal{M}_0) = [G : G_{\mathcal{M}_0}] = \#G/\#G_{\mathcal{M}_0}$ nicht durch p^{r+1} geteilt wird. Dann ist p^n ein Teiler von $\#G_{\mathcal{M}_0}$.*

Benutzen Sie (a), um die oben gemachte Aussage über Teilbarkeit von $\#G_{\mathcal{M}_0}$ durch p^n zu begründen.

6.4. *(Anzahl nicht isomorpher Graphen mit n Knoten)* (4 Punkte)
Ein Graph Γ ist ein Tupel (V, E), wobei V eine Menge von Knoten ist und E eine Menge von Kanten bezeichnet, die zwei Knoten miteinander verbinden können. Wenn die Kanten von Γ zusätzlich ungerichtet sind und es zwischen zwei Knoten keine Mehrfachkanten gibt, ist E eine Teilmenge aller 2-elementigen Teilmengen von V. Zwei ungerichtete Graphen $\Gamma_1 = (V_1, E_1)$ und $\Gamma_2 = (V_2, E_2)$ ohne Mehrfachkanten sind isomorph, wenn es eine bijektive Abbildung $p : V_1 \to V_2$ mit der folgenden Eigenschaft gibt: $\{v, w\}$ ist genau dann eine Kante von Γ_1, wenn $\{p(v), p(w)\}$ eine Kante von Γ_2 ist.

(a) Es sei nun $n \in \mathbb{N}$. Bestimmen Sie mit Satz 2.21 (Polya-Redfield) die Anzahl $\mathscr{A}(n)$ nicht isomorpher Graphen mit n Knoten. Die Anzahl der Bahnen der induzierten Operation $\varrho(g)$ muss nur für $g = 1_G$ explizit berechnet werden.

(b) Bestimmen Sie $\mathscr{A}(n)$ für $n \leq 4$ explizit.

(Hinweis: Überlegen Sie sich in Teil (a), wie sich die Operation der $\mathfrak{S}_n$ auf den n Knoten des Graphen auf die Kanten des Graphen überträgt.)

7. Übung

7.1. *(Gruppen der Ordnung 324 und Einfachheit)* (∗4 Punkte)
Zeigen Sie, dass es keine einfache Gruppe G mit Ordnung $324 = 2^2 3^4$ gibt.
(Hinweis: falls die Anzahlbetrachtung der Sylowgruppen von G nicht ausreichen,

betrachten Sie die Operation von G auf $\mathrm{Syl}_3 G$ durch Konjugation. Kann diese Operation treu sein?)

7.2. *(Erzeugen von $\mathfrak{S}_n$)* (∗4 Punkte)
Es sei $n \geq 2$. Zeigen Sie die folgenden Aussagen:
(a) $\mathfrak{S}_n = \langle (1\,2), (1\,3), \ldots, (1\,n) \rangle$;
(b) $\mathfrak{S}_n = \langle (1\,2), (2\,3), (3\,4), \ldots, ((n-1)\,n) \rangle$;
(c) $\mathfrak{S}_n = \langle \sigma, \tau \rangle$ mit $\sigma = (1\,2\,3\,\ldots\,n)$ und $\tau = (1\,2)$;
(d) Ist n prim, so kann man in (c) sogar $\tau = (r\,s)$ mit beliebigen $1 \leq r < s \leq n$ wählen.
(Hinweis: benutzen Sie, dass $\mathfrak{S}_n$ von allen Transpositionen erzeugt wird; Konjugation könnte helfen. Falls Sie noch keine richtige Idee haben, mag es helfen, für $n = 4$ oder $n = 5$ konkrete Rechnungen anzustellen.)

7.3. *(Isomorphe semidirekte Produkte)* (∗4 Punkte)
Es seien $(N, \bullet)$, $(U, *)$ und $(V, \star)$ Gruppen, $\varphi : U \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus sowie $f : V \to U$ ein Gruppenisomorphismus.
(a) Zeigen Sie, dass die Abbildung

$$\Phi : N \rtimes_{\varphi} U \to N \rtimes_{\varphi \circ f} V, \quad (n, u) \mapsto (n, f^{-1}(u))$$

ein Gruppenisomorphismus ist.
(b) Betrachten Sie nun die Situation aus Proposition 3.5 (1): Es sei G eine Gruppe der Ordnung $n = pq$ mit Primzahlen p und q mit der Eigenschaft $q \mid (p-1)$. Zeigen Sie, dass es mindestens einen nicht-trivialen Gruppenhomomorphismus $\varphi : C_q \to \mathrm{Aut}(C_p)$ gibt.
(Hinweis: Zeigen Sie $\mathrm{Aut}(C_p) \cong C_{p-1}$.)
(c) Verwenden Sie Teil (a) und (b), um zu beweisen, dass alle nicht-trivialen Gruppenhomomorphismen von C_q nach $\mathrm{Aut}(C_p)$ zueinander isomorphe semidirekte Produkte liefern.

7.4. *(Untergruppen von $\mathfrak{S}_n$)* (∗4 Punkte)
Zeigen Sie für $n \geq 2$, dass A_n die einzige Untergruppe von $\mathfrak{S}_n$ mit Index 2 ist.

8. Übung

8.1. *(Normalteiler von $\mathfrak{S}_n$)* (∗4 Punkte)
Bestimmen Sie alle Normalteiler von $\mathfrak{S}_n$ für $n = 1, 2, 3, \ldots$.
(Hinweis: für $n \geq 5$ betrachten Sie den Schnitt $N \cap A_n$ eines Normalteilers N von $\mathfrak{S}_n$ mit A_n und benutzen Sie Aufgabe 8.2. Für kleinere n finden Sie die Lösung in § 4.1 der Vorlesungsnotizen. Ihr Beweis sollte sich aber nicht darauf stützen, dass man dort den vollständigen Untergruppenverband von $\mathfrak{S}_3$ oder $\mathfrak{S}_4$ sieht, es sei denn, Sie leiten sich diesen eigenständig her.)

8.2. *(Untergruppen von $\mathfrak{S}_n$)* (∗4 Punkte)
(a) Es sei U eine echte Untergruppe einer endlichen Gruppe G derart, dass U keinen nichttrivialen Normalteiler enthält. Mit G/U sei die Menge der

Linksnebenklassen von G bezeichnet. Zeigen Sie, dass G isomorph zu einer Untergruppe von $\mathrm{Sym}(G/U)$ ist.

(b) Zeigen Sie, dass für $n \geq 5$ der Index $[\mathfrak{S}_n : U]$ jeder echten Untergruppe $U \neq A_n$ von $\mathfrak{S}_n$ die Ungleichung $[\mathfrak{S}_n : U] \geq n$ erfüllt.

8.3. *(Ein Zyklizitätskriterium für endliche abelsche Gruppen)* (4 Punkte)
Es sei G eine endliche abelsche Gruppe. Zeigen Sie, dass G genau dann zyklisch ist, wenn es für jeden Primteiler p von $\#G$ höchstens $p-1$ Elemente der Ordnung p in G gibt.

8.4. *(Hauptsatz über endlich erzeugte abelsche Gruppen)* (4 Punkte)
Für eine abelsche Gruppe H bezeichne $\mathrm{Tor}(H)$ die Menge der Elemente von H mit endlicher Ordnung.

(a) Zeigen Sie, dass für jede endlich erzeugte abelsche Gruppe G ein $k \in \mathbb{N}_0$ und eine endliche abelsche Gruppe $\mathrm{Tor}(G)$ existieren, sodass G zu

$$\mathbb{Z}^k \times \mathrm{Tor}(G)$$

isomorph ist.

(b) Betrachten Sie zwei endlich erzeugte abelsche Gruppen $G := \mathbb{Z}^k \times \mathrm{Tor}(G)$ und $G' := \mathbb{Z}^\ell \times \mathrm{Tor}(G')$ und zeigen Sie die folgende Äquivalenz:

$$G \cong G' \quad \Longleftrightarrow \quad k = \ell \text{ und } \mathrm{Tor}(G) \cong \mathrm{Tor}(G').$$

(Hinweis: Betrachten Sie für eine endlich erzeugte abelsche Gruppe G die Menge $\mathrm{Hom}(G, \mathbb{Q})$ der Gruppenhomomorphismen von G nach $(\mathbb{Q}, +)$ und überlegen Sie sich, dass $\mathrm{Hom}(G, \mathbb{Q})$ durch punktweise Definition eine $\mathbb{Q}$-Vektorraumstruktur trägt. Bestimmen Sie ferner die Dimension dieses $\mathbb{Q}$-Vektorraums.)

(c) Folgern Sie mithilfe von Satz 5.3 den Hauptsatz über endlich erzeugte abelsche Gruppen:

Satz. *Jede endlich erzeugte abelsche Gruppe G ist isomorph zu einer Gruppe*

$$\mathbb{Z}^k \times C_{q_1} \times C_{q_2} \times \ldots \times C_{q_t}$$

mit $k, t \in \mathbb{N}_0$ und Primzahlpotenzen $q_1, \ldots, q_t > 1$. Dabei sind k, t und die Primzahlpotenzen (bis auf Umnummerierung) durch G eindeutig bestimmt.

9. Übung

9.1. *(Adjunktion)* (4 Punkte)

(a) Zeigen Sie, dass $\mathbb{Q}[\sqrt{2}]$, der kleinste Teilring von $\mathbb{C}$, welcher $\mathbb{Q} \cup \{\sqrt{2}\}$ enthält, sogar ein Körper ist.

(b) Es sei $\alpha \in \mathbb{C}$ eine komplexe Zahl, welche Nullstelle keines nicht-konstanten Polynoms mit rationalen Koeffizienten ist (d.h. für alle $n \in \mathbb{N}_0$ und alle $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ mit $\{a_0, a_1, \ldots, a_n\} \neq \{0\}$ ist $a_0 + a_1\alpha + \ldots + a_n\alpha^n \neq 0$). Zeigen Sie, dass $\mathbb{Q}[\alpha]$ kein Körper ist.

9.2. *(Endliche Integritätsbereiche sind Körper)* (4 Punkte)
R sei ein ***Integritätsbereich***, d.h. ein kommutativer Ring ungleich dem Nullring, sodass für alle $a, b \in R$ aus $ab = 0_R$ schon $a = 0_R$ oder $b = 0_R$ folgt.

(a) Zeigen Sie, dass für alle $a \in R \setminus \{0_R\}$ die Abbildung $R \to R$, $b \mapsto ab$, injektiv ist.

(b) Folgern Sie: ist $\#R < \infty$, so ist R ein Körper.

9.3. *(Einheitengruppe von $\mathbb{Z}/2^\nu\mathbb{Z}$)* (4 Punkte)
Es sei $\nu \in \mathbb{N} \setminus \{1, 2\}$ und $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$ bezeichne die Einheitengruppe des Rings $\mathbb{Z}/2^\nu\mathbb{Z}$. Beweisen Sie die folgenden Aussagen:

(a) Es gibt ein $m \in \mathbb{N}$ mit $5^{2^{\nu-2}} = 1 + m2^\nu$. (Hinweis: Induktion über ν.)

(b) Für $\nu \geq 2$ liegt 5 mod 2^ν in $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$ und hat die Ordnung $2^{\nu-2}$.

(c) Für $\nu \geq 2$ ist $(\mathbb{Z}/2^\nu\mathbb{Z})^\times \cong C_2 \times C_{2^{\nu-2}}$.
(Hinweis: finden Sie zunächst zwei verschiedene Elemente von $(\mathbb{Z}/2^\nu\mathbb{Z})^\times$ mit Ordnung 2. Überlegen Sie sich dann, welche Möglichkeiten für $q_1, \ldots, q_t$ in Satz 5.3 im vorliegenden Fall in Frage kommen.)

9.4. *(Normen)* (4 Punkte)
Es sei $d \neq 1$ eine ***quadratfreie*** ganze Zahl, d.h. es gibt kein $n \in \mathbb{N} \setminus \{1\}$ mit $n^2 \mid d$. Mit $\sqrt{d}$ sei eine beliebige komplexe Nullstelle des Polynoms $X^2 - d$ bezeichnet. (Die zweite solche Nullstelle ist dann $-\sqrt{d}$.) Es sei $\vartheta = \sqrt{d}$ falls $d \equiv 2, 3 \bmod 4$ und $\vartheta = \frac{1}{2}(1 + \sqrt{d})$ falls $d \equiv 1 \bmod 4$. (Der Fall $d \equiv 0 \bmod 4$ kann wegen Quadratfreiheit von d nicht eintreten.) $\mathbb{Z}[\vartheta]$ bezeichne den kleinsten Teilring von $\mathbb{C}$, der $\mathbb{Z}$ und ϑ enthält. $\mathbb{Q}[\vartheta]$ sei analog definiert.

(a) Zeigen Sie $\vartheta \notin \mathbb{Q}$, $\mathbb{Z}[\vartheta] = \{a + b\vartheta \in \mathbb{C} : a, b \in \mathbb{Z}\}$ und $\mathbb{Q}[\vartheta] = \{a + b\vartheta \in \mathbb{C} : a, b \in \mathbb{Q}\}$.

(b) Bestimmen Sie für $a, b \in \mathbb{Z}$ die Darstellungsmatrix $A_{a+b\vartheta}$ der $\mathbb{Q}$-linearen Abbildung $\mathbb{Q}[\vartheta] \to \mathbb{Q}[\vartheta]$, $x \mapsto (a + b\vartheta)x$, bezüglich der $\mathbb{Q}$-Basis $1, \vartheta$ von $\mathbb{Q}[\vartheta]$.

(c) Zeigen Sie, dass $\det(A_{a+b\vartheta})$ für $a, b \in \mathbb{Z}$ eine ganze Zahl ist und die Abbildung $N\colon \mathbb{Z}[\vartheta] \to \mathbb{Z}$, $y \mapsto \det(A_y)$, multiplikativ ist (d.h. $N(xy) = N(x)N(y)$ für alle $x, y \in \mathbb{Z}[\vartheta]$).

(d) Zeigen Sie: $x \in (\mathbb{Z}[\vartheta])^\times \iff N(x) \in \mathbb{Z}^\times = \{\pm 1\}$.

10. Übung

10.1. *(Ringe in der Topologie)* (4 Punkte)
Es sei X ein kompakter Hausdorff-Raum. (Falls Sie damit nicht vertraut sind, dürfen Sie X durch das Intervall $[0, 1]$ ersetzen.) Es sei R der Ring der *stetigen*, reellwertigen Funktionen $f\colon X \to \mathbb{R}$ mit punktweise definierter Addition & Multiplikation. Zeigen Sie:

(a) Für $x \in X$ ist $\mathfrak{m}_x = \{f \in R : f(x) = 0\}$ ein maximales Ideal von R.

(b) Haben $f_1, \ldots, f_n \in R$ keine gemeinsame Nullstelle (d.h. es gibt kein $x \in X$ mit $f_1(x) = \ldots = f_n(x) = 0$), so ist $\langle f_1, \ldots, f_n \rangle = \langle 1 \rangle = R$.

(c) Jedes maximale Ideal $\mathfrak{m}$ von R ist von der Form $\mathfrak{m}_x$ für ein $x \in X$.

(d) Die Zuordnung $x \mapsto \mathfrak{m}_x$ stiftet eine Bijektion zwischen X und der Menge der maximalen Ideale von R. (Hinweis: Benutzen Sie das Lemma von Urysohn aus der Topologie, falls Sie dieses kennen, oder schränken Sie Ihre Betrachtung hier auf $X = [0,1]$ ein.)

10.2. *(Einheitengruppe von $\mathbb{Z}/p^\nu\mathbb{Z}$)* (4 Punkte)
Es sei p eine ungerade Primzahl und $\nu \geq 2$. Wir setzen $\lfloor \varrho \rfloor := \max\{ r \in \mathbb{Z} : r \leq \varrho \}$. Beweisen Sie die folgenden Aussagen:

(a) Es gilt $(1+p)^{p^{\nu-2}} \equiv 1 + p^{\nu-1} \bmod p^\nu$. (Hinweis: Induktion & Binomischer Lehrsatz.)
(b) $1 + p \bmod p^\nu$ hat Ordnung $p^{\nu-1}$ in $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$.
(c) Sind x und y Elemente einer endlichen abelschen Gruppe $(G, \cdot)$ mit teilerfremden Ordnungen, so ist $\operatorname{ord}(xy) = \operatorname{ord}(x)\operatorname{ord}(y)$.
(d) Hat $g \bmod p$ Ordnung $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, so hat $g^{p^{\nu-1}}(1+p) \bmod p^\nu$ Ordnung $p^\nu - p^{\nu-1}$ in $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$.

10.3. *(Primideale, Teil I)* (4 Punkte)
Ein Ideal $\mathfrak{p} \subsetneq R$ eines Ringes R heißt ***Primideal*** (oder ***prim***), falls für alle Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von R aus $\mathfrak{ab} \subseteq \mathfrak{p}$ schon $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$ folgt. Im Folgenden sei R zusätzlich als *kommutativ* vorausgesetzt. Zeigen Sie dann die folgenden Aussagen:

(a) Für jedes Ideal $\mathfrak{p} \subseteq R$ von R sind die folgenden Aussagen äquivalent:
  (1) $\mathfrak{p}$ ist prim;
  (2) $\mathfrak{p} \neq R$ und $\forall a, b \in R$: $ab \in \mathfrak{p} \Rightarrow (a \in \mathfrak{p}$ oder $b \in \mathfrak{p})$;
  (3) $R/\mathfrak{p}$ ist ein Integritätsbereich.
(b) Jedes maximale Ideal $\mathfrak{m}$ von R ist prim.
(c) Alle Primideale $\mathfrak{p} \neq \{0\}$ von $\mathbb{Z}$ sind maximal.

10.4. *(Primideale, Teil II)* (4 Punkte)
Es sei $f : R \to S$ Homomorphismus zwischen kommutativen Ringen R und S.

(a) Zeigen Sie: ist $\mathfrak{p}$ ein Primideal von S, so ist das Urbild $f^{-1}(\mathfrak{p})$ ein Primideal von R.
(b) Belegen Sie durch ein Beispiel, dass das Urbild $f^{-1}(\mathfrak{m})$ eines maximalen Ideals $\mathfrak{m}$ von S nicht maximal in R zu sein braucht.

11. Übung

11.1. *(Ringe in der Topologie, II)* (4 Punkte)
In Fortsetzung von Aufgabe 10.1 betrachten wir den Ring R der stetigen Funktionen $f : \mathbb{R} \to \mathbb{R}$. (Notiz: Im Vergleich zu Aufgabe 10.1 ist der Definitionsbereich hier nicht kompakt.) Zeigen Sie, dass es ein maximales Ideal $\mathfrak{m}$ von R gibt, welches nicht von der Form $\mathfrak{m}_x = \{ f \in R : f(x) = 0 \}$ für $x \in \mathbb{R}$ ist.
(Hinweis: Satz 6.12.)

11.2. *(Zum Chinesischen Restsatz)* (4 Punkte)
Finden Sie einen Ring R mit Idealen $\mathfrak{a}_1$, $\mathfrak{a}_2$ und $\mathfrak{a}_3$ derart, dass $\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 = R$ gilt, aber $R/\bigcap_i \mathfrak{a}_i$ *nicht* isomorph zu $\prod_i (R/\mathfrak{a}_i)$ ist.

11.3. *(Struktur von $(\mathbb{Z}/n\mathbb{Z})^\times$)* (4 Punkte)
Es sei $G := (\mathbb{Z}/540\mathbb{Z})^\times$. Wegen $540 = 2^2 3^3 5$, Korollar 6.18 und Satz 6.21 ist $(\mathbb{Z}/540\mathbb{Z})^\times \cong C_2 \times C_{18} \times C_4$. Finden Sie Elemente $a, b, c \in G$ mit $\mathrm{ord}(a) = 2$, $\mathrm{ord}(b) = 18$ und $\mathrm{ord}(c) = 4$ und $\{1_G\} = \langle a\rangle \cap \langle b, c\rangle = \langle b\rangle \cap \langle a, c\rangle = \langle c\rangle \cap \langle a, b\rangle$.

11.4. *(Radikal eines Ideals)* (4 Punkte)
Sei R ein kommutativer Ring und $\mathfrak{a}$ ein Ideal von R. Betrachten Sie ferner die Menge $\mathrm{rad}(\mathfrak{a}) := \{r \in R \ : \ \exists n \in \mathbb{N} \text{ mit } r^n \in \mathfrak{a}\}$, welche als *Radikal von* $\mathfrak{a}$ bezeichnet wird.

(a) Zeigen Sie, dass $\mathrm{rad}(\mathfrak{a})$ ein Ideal von R ist.

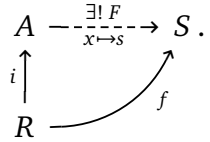
(b) Zeigen Sie die Gleichheit

$$\mathrm{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \supseteq \mathfrak{a} \\ \mathfrak{p} \text{ Primideal}}} \mathfrak{p}.$$

(Hinweis: Betrachten Sie in Teil (b) für die Teilmengeninklusion „$\supseteq$“ ein $f \in R \setminus \mathrm{rad}(\mathfrak{a})$ und zeigen Sie die Existenz eines Primideals $\mathfrak{p} \supseteq \mathfrak{a}$, welches f nicht enthält. Betrachten Sie zudem die Menge $\mathscr{A}$ aller Ideale, welche $\mathfrak{a}$ enthalten, aber keine Potenz von f enthalten, und verwenden Sie das Lemma von Zorn.)

12. Übung

12.1. *(Universelle Eigenschaft von $R[X]$)* (4 Punkte)
Es sei $i\colon R \to A$ ein Homomorphismus zwischen kommutativen Ringen und $x \in A$ sei fixiert. Ferner gelte die folgende Aussage: *für jeden Ringhomomorphismus $f\colon R \to S$ in einen kommutativen Ring S und jedes $s \in S$ gibt es genau einen Ringhomomorphismus $F\colon A \to S$ mit $F(x) = s$, der das folgende Diagramm kommutativ macht:*



Zeigen Sie, dass A isomorph zum Polynomring $R[X]$ ist.

12.2. *(Polynome und Nullstellen)* (4 Punkte)
Geben Sie ein Beispiel für einen kommutativen Ring R und ein Polynom $f \in R[X] \setminus \{0_{R[X]}\}$ an, sodass f unendlich viele verschiedene Nullstellen in R besitzt. (Hinweis: Sie können beispielsweise Polynomringe und Faktorbildung benutzen, um einen Ring R mit vielen Nullteilern zu konstruieren.)

12.3. *(Lokalisierung)* (∗4 Punkte)
Es sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$, die die beiden Eigenschaften $1_R \in S$ und $s, s' \in S \Rightarrow ss' \in S$ erfüllt, heißt *multiplikatives System*.

(a) Betrachten Sie das mengentheoretische kartesische Produkt $R \times S$ des Rings mit einem multiplikativem System und zeigen Sie, dass die via

$$(r, s) \sim (r', s') \quad :\Longleftrightarrow \quad \exists t \in S : (rs' - r's)t = 0_R$$

definierte Relation eine Äquivalenzrelation ist.

(b) Die Äquivalenzklasse $[(r,s)]_\sim$ von $(r,s) \in R \times S$ bezeichnen wir suggestiv auch mit $\frac{r}{s}$. Auf der Menge $(R \times S)/\sim$ der Äquivalenzklassen definieren wir eine Addition und eine Multiplikation via

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \quad \text{und} \quad \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Zeigen Sie, dass $(R \times S)/\sim$ mit dieser Addition und Multiplikation zu einem kommutativem Ring wird.
Bemerkung: Diesen Ring nennt man *Lokalisierung von R bei S* und schreibt auch $S^{-1}R$.

(c) Zeigen Sie die universelle Eigenschaft der Lokalisierung:
Die (kanonische) Abbildung $\tau : R \to S^{-1}R, r \mapsto \frac{r}{1}$ von einem Ring R in seine Lokalisierung bei einem multiplikativem System $S \subseteq R$ ist ein Homomorphismus mit der Eigenschaft $\tau(S) \subseteq (S^{-1}R)^\times$. Diese Abbildung ist universell in dem Sinne, dass jeder Ringhomomorphismus $\varphi : R \to R'$ mit $\varphi(S) \subseteq R'^\times$ eindeutig über $S^{-1}R$ faktorisiert. Das heißt, es existiert ein eindeutiger Ringhomomorphismus $\varphi' : S^{-1}R \to R'$ mit $\varphi = \varphi' \circ \tau$.
Weiterhin gilt: Falls φ dieselbe universelle Eigenschaft wie τ erfüllt, so ist φ' ein Isomorphismus von Ringen.
Bemerkung: Im Spezialfall $S = R \setminus \{0_R\}$ ist die Lokalisierung $S^{-1}R$ ein Körper und wird als *Quotientenkörper* bezeichnet.

(Hinweis: Das in der Vorlesung nicht behandelte Kapitel 7.3 im Skript kann Ihnen bei der Bearbeitung dieser Aufgabe behilflich sein.)

12.4. *(Lokalisierung II)* (∗4 Punkte)

Betrachten Sie das multiplikative System $S = \{2^n : n \in \mathbb{N}_0\}$ in $\mathbb{Z}$.

(a) Zeigen Sie: $S^{-1}\mathbb{Z} \cong \mathbb{Z}[\frac{1}{2}] := \{\frac{a}{2^n} \in \mathbb{Q} : a \in \mathbb{Z}, n \in \mathbb{N}_0\}$.

(b) Bestimmen Sie alle Ideale von $S^{-1}\mathbb{Z}$.

(c) Bestimmen Sie den Quotientenkörper $\mathrm{Quot}(S^{-1}\mathbb{Z})$ von $S^{-1}\mathbb{Z}$.

13. Übung

13.1. *(Erweiterter Euklidischer Algorithmus)* (4 Punkte)

(a) (Aufwärmübung:) Benutzen Sie das in den Vorlesungsnotizen in § 8.1.2 beschriebene Verfahren, um aus dem nachstehenden Divisionsschema Zahlen $x, y \in \mathbb{Z}$ mit $24x + 7y = 1$ zu gewinnen:

$$\begin{cases} 24 = 3 \cdot 7 + 3, \\ 7 = 2 \cdot 3 + 1, \\ 3 = 3 \cdot 1 + 0. \end{cases}$$

(b) Wir schreiben $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ und $\overline{a} = a + 5\mathbb{Z}$. Finden Sie Polynome $f, g \in \mathbb{F}_5[X]$ mit

$$(X^5 + X^2 + \overline{2}X - \overline{1})f + (X^2 + \overline{1})g = \overline{1}.$$

(Ihr Rechenweg ist mit anzugeben und sollte sich an § 8.1.2 orientieren.)

(c) Es sei $\mathfrak{a} = \langle X^5+X^2+\overline{2}X-\overline{1}\rangle$. Folgern Sie aus (b), dass $(X^2+\overline{1})+\mathfrak{a} \in \mathbb{F}_5[X]/\mathfrak{a}$ invertierbar ist und geben Sie das zugehörige multiplikativ inverse Element an.

13.2. *(Irreduzibilität von Polynomen mit kleinem Grad)* (4 Punkte)
Sei R ein Integritätsbereich. Ein Element $p \in R \setminus (R^\times \cup \{0_R\})$ heißt ***irreduzibel***, falls jede Zerlegung $p = ab$ mit $a, b \in R$ automatisch $a \in R^\times$ oder $b \in R^\times$ erfüllt. K sei ein beliebiger Körper und $f \in K[X]$ ein Polynom mit Grad n.

(a) Ist $n = 1$, so ist f irreduzibel. (Hinweis: Gradformel, Proposition 7.2.)

(b) Ist $n \in \{2, 3\}$, so ist f genau dann irreduzibel, wenn f keine Nullstelle in K besitzt.
(Hinweis: Wenn $f = ab$ mit Polynomen a, b gilt, welche Grade kommen dann für a und b in Frage?)

(c) Gilt $1_K + 1_K \neq 0_K$, so ist das quadratische Polynom $aX^2 + bX + c \in K[X]$ $(a, b, c \in K,\ a \neq 0_K)$ genau dann irreduzibel, wenn seine ***Diskriminante*** b^2-4ac kein Quadrat in K ist (d.h. wenn es kein $x \in K$ mit $x^2 = b^2-4ac$ gibt).

(d) $3X^2 + 4X + 3$ ist irreduzibel als Polynom über $\mathbb{Z}[\mathrm{i}\sqrt{5}]$, aber reduzibel als Polynom über $\mathbb{Q}[\mathrm{i}\sqrt{5}]$. (Hinweis: Bei $\mathbb{Q}[\mathrm{i}\sqrt{5}]$ handelt es sich sogar um einen Körper, wie man analog zu Aufgabe 9.1 sieht. Das dürfen Sie ohne Beweis benutzen.)

13.3. *(Längen von Zerlegungen in irreduzible Elemente)* (4 Punkte)
Es sei R ein Integritätsbereich und $R[X]$ der Polynomring über R in einer Variablen. $R[X^2, X^3]$ bezeichne den kleinsten Teilring von $R[X]$, der R, X^2 und X^3 enthält. Zeigen Sie:

(a) $R[X^2, X^3] = \left\{ \sum_n a_n X^n \in R[X] : a_n \in R, \text{fast alle gleich } 0_R,\ a_1 = 0_R \right\}$.

(b) Die Elemente X^2 und X^3 sind beide irreduzibel in $R[X^2, X^3]$.

13.4. *(Die ganzen Gaußschen Zahlen, II)* (4 Punkte)
Betrachten Sie den Ring $\mathbb{Z}[\mathrm{i}]$ der ganzen Gaußschen Zahlen aus Aufgabe T9.2. Ferner sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie:

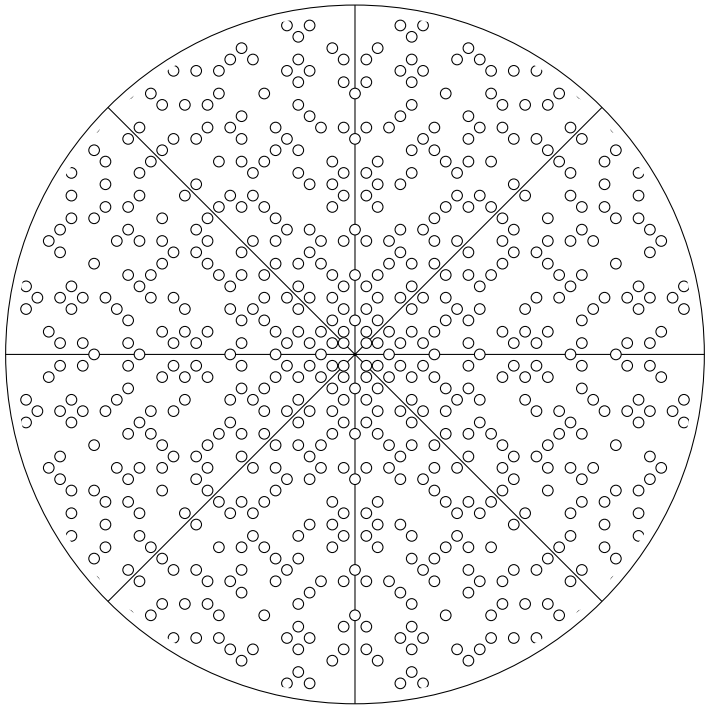
(a) Für jedes Primelement π von $\mathbb{Z}[\mathrm{i}]$ ist $N(\pi)$ entweder eine Primzahl in $\mathbb{N}$ oder das Quadrat einer solchen. (Hinweis: $N(\pi) = \pi\overline{\pi}$.)

(b) (1) Ist p Summe zweier Quadrate, d.h. $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$, so ist $p = (a + \mathrm{i}b)(a - \mathrm{i}b)$ eine Zerlegung von p in Primelemente von $\mathbb{Z}[\mathrm{i}]$ und $a + \mathrm{i}b$ ist dann und nur dann assoziiert zu $a - \mathrm{i}b$, wenn $|a| = |b| = 1$ ist.

(2) Ist p nicht Summe zweier Quadrate, so ist p ein Primelement von $\mathbb{Z}[\mathrm{i}]$.

(c) Ist $p \equiv 3 \bmod 4$, so ist p ein Primelement von $\mathbb{Z}[\mathrm{i}]$. (Hinweis: $a^2 + b^2 \equiv \boxed{?} \bmod 4$.)

(d) Bestimmen Sie alle Primelemente $a + \mathrm{i}b$ von $\mathbb{Z}[\mathrm{i}]$ mit $a, b \in \mathbb{Z}$ und $0 \leq a, b \leq 6$ und zeichnen Sie diese in der Gaußschen Zahlenebene.



(Hinweis: in dem obigen Bild ist (bei geeigneter Vergrößerung) die Lösung zu Teil (d) zu finden. Benutzen Sie dies aber allenfalls zur Selbstkontrolle Ihres Ergebnises und nicht zur Lösungsfindung.)

14. Übung

14.1. *(Ein irreduzibles Polynom über $\mathbb{F}_p$)*
Für eine Primzahl p sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Zeigen Sie, dass das Polynom $f = X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel ist.
(Hinweis: zeigen Sie, dass f invariant unter Einsetzen von $X+1$ für X ist. Betrachten Sie anschließend die hieraus hervorgehende Operation von $(\mathbb{F}_p, +) \cong (C_p, \oplus)$ auf der Menge der Primteiler von f.)

14.2. *(Faktorisieren von Polynomen)*
Zerlegen Sie die folgenden Polynome über $\mathbb{Z}[X]$ in Primfaktoren:
(a) $2X^2 + 4X + 2$,
(b) $6X^2 + 12$.

14.3. *(Irreduzibilität)*
Untersuchen Sie die folgenden Polynome auf Irreduzibilität:
(a) $X^4 + 4X^3 + 6X^2 + 4X + 10 \in \mathbb{Q}[X]$.
(b) $X^4 + 9 \in \mathbb{Q}[X]$.
(c) $X^2 + Y^2 - 1 \in \mathbb{Q}[X, Y]$. (Hinweis: $\mathbb{Q}[X, Y] \cong (\mathbb{Q}[X])[Y]$ und Eisenstein.)
(d) $X^2 + Y^2 \in \mathbb{R}[X, Y]$. (Hinweis: man faktorisiere zunächst in $\mathbb{C}[X, Y]$.)
(e) $X^4 + 4Y^4 \in \mathbb{R}[X, Y]$. (Hinweis: $X^2 + Y^2 - aXY$.)

Zeigen Sie ferner:

(f) Es gibt unendlich viele irreduzible Polynome $f \in \mathbb{Q}[X]$ mit $\deg f = 12$.

14.4. *(Faktorisierungsmethode von Kronecker)*
Es sei R ein Integritätsbereich mit unendlich vielen Elementen und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. (Sie dürfen auch gerne $R = \mathbb{Z}$ und $K = \mathbb{Q}$ annehmen, falls Ihnen das hilft.) Für jedes $a \in R$ sei $T(a) = \{ b \in R : b \mid a \}$ die Menge seiner Teiler und diese sei für alle $a \neq 0_R$ endlich.

(a) Es sei $f \in R[X]$ ein Polynom vom Grad $n > 1$ und m sei $\max\{ r \in \mathbb{N} : 2r \leq n \}$. Zeigen Sie:
  (1) Es gibt paarweise verschiedene $a_0, \ldots, a_m \in R$ derart, dass die Mengen $T_i := T(f(a_i))$ für $i = 0, \ldots, m$ endlich sind.
  (2) Zu jedem $\boldsymbol{b} = (b_0, \ldots, b_m) \in T_0 \times \cdots \times T_m =: T$ gibt es genau ein $g_{\boldsymbol{b}} \in K[X]$ mit Grad $\leq m$ und $g_{\boldsymbol{b}}(a_i) = b_i$ für $i = 0, \ldots, m$.
  (3) f ist genau dann reduzibel in $R[X]$, wenn es ein $\boldsymbol{b} \in T$ gibt derart, dass $g_{\boldsymbol{b}}$ in $R[X] \setminus R^\times \subseteq K[X]$ liegt und ein Teiler von f ist.

(b) Nun sei zusätzlich angenommen, dass für jedes $r \in R \setminus \{0_R\}$ die Menge $T(r)$ in endlich vielen „Rechenschritten“ bestimmbar ist und auch Addition und Multiplikation von Elementen in R in endlich vielen Rechenschritten durchführbar sind. Beschreiben Sie dann ein Verfahren, welches jedes Polynom aus $R[X]$ in endlich vielen Schritten in über R irreduzible Polynome zerlegt.

(c) Zerlegen Sie das folgende Polynom unter Anwendung der durch Teil (a) nahegelegten Methode in irreduzible Faktoren über $\mathbb{Z}$:

$$3X^5 + 2X^4 - 24X^3 - 26X^2 + 11X - 1.$$

(Achtung: dies ist ggf. aufwändig. Bloßes Hinschreiben einer geeigneten Faktorisierung und Prüfen, dass diese passt, ist nicht erlaubt. Der Rechenweg sollte — jedenfalls grob — ersichtlich sein.)

1. Präsenzübung

T1.1. *(Heisenberggruppe)*
Es sei K ein Körper. Betrachten Sie die Menge

$$H_3(K) := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in K^{3\times 3} : a, b, c \in K \right\}$$

mit der üblichen Matrixmultiplikation als Verknüpfung.

(a) Zeigen Sie, dass $H_3(K)$ eine nicht-abelsche Gruppe ist.

(b) Es sei nun $K = \mathbb{F}_2$. Bestimmen Sie die Ordnung der Gruppe $H_3(\mathbb{F}_2)$, die Ordnungen aller ihrer Elemente sowie alle ihre Untergruppen.

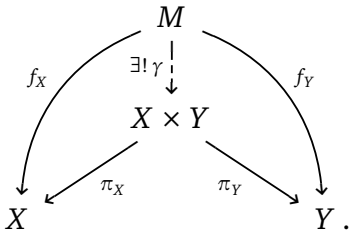
T1.2. *(Gruppentafeln)*
Es sei $G = \{g_1, \ldots, g_n\}$ eine n-elementige Menge und $\circ\colon G \times G \to G$ eine Verknüpfung derart, dass $(G, \circ)$ eine Gruppe bildet. Die zugehörige ***Gruppentafel*** ist definiert als die $n \times n$-Matrix T über G, deren (i,j)-ter Eintrag genau $g_i \circ g_j$ ist:

$$\begin{pmatrix} g_1 \circ g_1 & g_1 \circ g_2 & g_1 \circ g_3 & \cdots & g_1 \circ g_n \\ g_2 \circ g_1 & g_2 \circ g_2 & g_2 \circ g_3 & \cdots & g_2 \circ g_n \\ g_3 \circ g_1 & g_3 \circ g_2 & g_3 \circ g_3 & \cdots & g_3 \circ g_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n \circ g_1 & g_n \circ g_2 & g_n \circ g_3 & \cdots & g_n \circ g_n \end{pmatrix}.$$

(a) Zeigen Sie, dass jedes Gruppenelement $g \in G$ in jeder Zeile und in jeder Spalte der Gruppentafel T *genau einmal* vorkommt.
(b) Es seien g_1, g_2 und g_3 drei paarweise verschiedene Elemente. Bestimmen Sie alle Gruppentafeln T, die durch Ausstattung von $G = \{g_1, g_2, g_3\}$ mit einer Gruppenstruktur entstehen können. (Sie dürfen zur Vereinfachung davon ausgehen, dass nur Gruppenstrukturen auf G betrachtet werden, bezüglich derer g_1 das neutrale Element ist.)

T1.3. *(Produkte: 'abstract nonsense')*
Es seien X und Y zwei Mengen und $X \times Y = \{(x,y) : x \in X,\, y \in Y\}$ ihr kartesisches Produkt. Es sei $\pi_X\colon X \times Y \to X$ gegeben durch $\pi_X(x,y) = x$ und π_Y sei analog definiert.

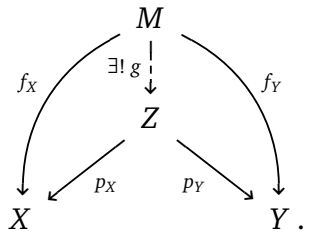
(a) Zeigen Sie, dass $X \times Y$ zusammen mit π_X und π_Y die folgende Eigenschaft erfüllt: Für je zwei Abbildungen $f_X\colon M \to X$ und $f_Y\colon M \to Y$ gibt es *genau eine* Abbildung $\gamma\colon M \to X \times Y$, die das folgende Diagramm kommutativ macht:



(Hinweis: ein Diagramm wie das obige heißt ***kommutativ***, falls je zwei Möglichkeiten von einer Stelle zu einer anderen entlang der gezeichneten Pfeile zu 'laufen' (und dabei die auf den Pfeilen notierten Abbildungen verkettend) dieselbe Abbildung vermitteln. Im vorliegenden Fall bedeutet dies $f_X \overset{!}{=} \pi_X \circ \gamma$ und $f_Y \overset{!}{=} \pi_Y \circ \gamma$.)

(b) Es sei Z eine weitere Menge zusammen mit zwei Abbildungen $p_X\colon Z \to X$ und $p_Y\colon Z \to Y$ derart, dass für jedes Tripel (M, f_X, f_Y) wie in (a) *genau eine* Abbildung $g\colon M \to Z$ existiert, welche das folgende Diagramm

kommutativ macht:



Zeigen Sie dann, dass die so für $(M, f_X, f_Y) = (X \times Y, \pi_X, \pi_Y)$ erhaltene Abbildung $g\colon X \times Y \to Z$ eine Bijektion ist.
(Hinweis: Probieren Sie, sich einen Kandidaten für eine Umkehrabbildung $Z \to X \times Y$ von g zu beschaffen. Zur Vereinfachung können Sie zusätzlich annehmen, dass π_X, π_Y, p_X sowie p_Y surjektiv sind, auch wenn diese Annahme nicht notwendig ist.)

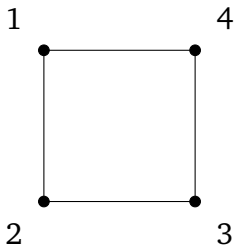
2. Präsenzübung

T2.1. *(Konjugation von Untergruppen)*
Betrachten Sie eine Gruppe $(G, \circ)$ sowie eine Untergruppe U von G.

(a) Zeigen Sie, dass für jedes $g \in G$ die Menge $U_g := g \circ U \circ g^{-1}$ ebenfalls eine Untergruppe von G ist.

(b) Nehmen sie nun an, dass U endliche Ordnung hat. Zeigen Sie, dass dann $\#U = \#U_g$ für alle $g \in G$ gilt.

T2.2. *(Symmetriegruppe des Quadrats)*
Betrachten Sie das Quadrat



(a) Bestimmen Sie alle Permutationen der 4 Ecken, die die geometrische Struktur des Quadrats erhalten.

(b) Zeigen Sie, dass sich jede Permutation aus Teil (a) als Komposition von

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad \text{und} \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} \in \mathfrak{S}_4 .$$

darstellen lässt. Zeigen Sie ferner die Gleichung $\sigma \circ \tau = \tau \circ \sigma^3$.

(c) Zeigen Sie, dass die Menge der Permutationen aus (a) eine Untergruppe der $\mathfrak{S}_4$, die sogenannte Symmetriegruppe des Quadrats, ist.

(d) Ist diese Gruppe abelsch?

Hinweis: Die Erhaltung der geometrischen Struktur bedeutet insbesondere, dass sich gegenüberliegende Ecken nach der Permutation der Ecken immer noch gegenüberliegen und die 4 Kanten mit ihren jeweiligen Eckpunkten bestehen bleiben.

T2.3. *(Untergruppen von $(\mathbb{Z},+)$)*
Beweisen Sie Proposition 1.11:
(a) Die Untergruppen von $(\mathbb{Z},+)$ sind genau die Mengen $n\mathbb{Z} = \{ nz : z \in \mathbb{Z} \}$ mit $n \in \mathbb{N}_0$.
(b) Für $m, n \in \mathbb{Z}$ gilt: $m\mathbb{Z} \supseteq n\mathbb{Z} \iff m$ teilt n. („Teilen heißt Enthalten.“)

3. Präsenzübung

T3.1. *(Fingerübungen zu Normalteilern)*
Sei G eine Gruppe. Beweisen Sie die folgenden Aussagen:
(a) Wenn G abelsch ist, so ist jede Untergruppe U von G ein Normalteiler.
(b) Wenn G endliche Ordnung hat und nur eine Untergruppe U mit Ordnung $\#U$ besitzt, so ist U ein Normalteiler.

T3.2. *(Isomorphismus zyklischer Gruppen)*
Zeigen Sie, dass die Gruppen C_n und $\mathbb{Z}/n\mathbb{Z}$ (für ein festes $n \in \mathbb{N}$) isomorph sind.

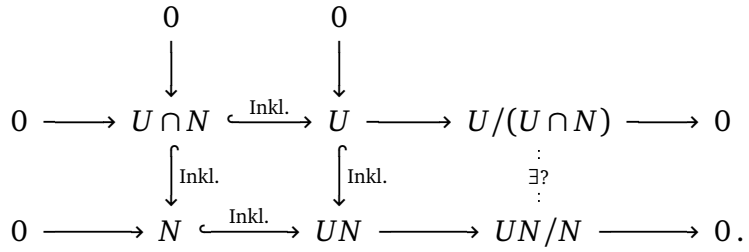
T3.3. *(Konjugation und innere Automorphismen)*
Betrachten Sie eine Gruppe $(G,\circ)$. Für ein festes $h \in G$ definieren wir die Konjugationsabbildung $i_h : G \to G, g \mapsto h \circ g \circ h^{-1}$. Zudem definieren wir die Menge aller Konjugationsabbildungen von Elementen aus G als $\mathrm{Inn}(G) := \{i_h : h \in G\}$. Zeigen Sie:
(a) Die Abbildung i_h ist ein Gruppenisomorphismus, also ein Gruppenautomorphismus von G.
(b) Die Menge $\mathrm{Inn}(G)$ ist ein Normalteiler von $\mathrm{Aut}(G)$. Man bezeichnet $\mathrm{Inn}(G)$ auch als Menge der inneren Automorphismen von G.
(c) Es gilt genau dann $i_h = \mathrm{id}_G$, wenn h mit allen $g \in G$ kommutiert.

4. Präsenzübung

T4.1. *(Beispiele zum ersten Isomorphiesatz)*
Verwenden Sie Korollar 2.7 und beweisen Sie die folgenden Isomorphismen von Gruppen:
(a) Für eine Gruppe $(G,\circ)$ gilt $G/Z(G) \cong \mathrm{Inn}(G)$, wobei $Z(G) = \{h \in G : h \circ g = g \circ h \ \ \forall g \in G\}$ das sogenannte Zentrum von G ist.
(b) Es seien G und H Gruppen sowie J ein Normalteiler von G und K ein Normalteiler von H. Dann gilt $(G \times H)/(J \times K) \cong (G/J) \times (H/K)$.
(c) Es gilt $\mathbb{C}^\times/\mathbb{S}^1 \cong \mathbb{R}_{>0}$.
(Hinweis: erinnern Sie sich in Teil (a) an Aufgabe T3.3.)

T4.2. *(Zweiter Isomorphiesatz)*
Beweisen Sie Satz 2.11: es sei G eine Gruppe, $U \leq G$ und $N \trianglelefteq G$. Dann ist auch

$UN \leq G$ und $U \cap N \trianglelefteq U$ sowie $UN/N \cong U/(U \cap N)$.
Hinweis: für die gefragte Isomorphie, betrachten Sie das folgende kommutative Diagramm mit exakten Zeilen und Spalten, wobei die gezeichneten Pfeile die „offensichtlichen“ Homomorphismen bedeuten sollen:



T4.3. *(Isomorphiesatz für Vektorräume)*

(a) Es seien K ein Körper, V ein K-Vektorraum sowie $U \leq V$ ein Untervektorraum. Zeigen Sie, dass $V/U = \{v + U : v \in V\}$ ein K-Vektorraum ist. Dieser wird als Faktorraum oder Quotientenvektorraum bezeichnet.

(b) Es seien K ein Körper, V und W jeweils K-Vektorräume sowie $\phi : V \to W, v \mapsto \phi(v)$ eine lineare Abbildung. Zeigen Sie, dass $\phi = \iota \circ \overline{\phi} \circ \pi$ gilt, wobei

- $\pi : V \to V/\ker(\phi), v \mapsto v + \ker(\phi)$ ein Epimorphismus (von Vektorräumen) ist,
- $\overline{\phi} : V/\ker(\phi) \to \phi(V), v + \ker(\phi) \mapsto \phi(v)$ ein Isomorphismus (von Vektorräumen) ist,
- $\iota : \phi(V) \to W, v \mapsto v$ ein Monomorphismus (von Vektorräumen) ist.

Insbesondere gilt also $V/\ker(\phi) \cong \phi(V) = \mathrm{im}(\phi)$.

T4.4. *(Isomorphiesatz für Vektorräume)*

(a) Es seien K ein Körper, V ein K-Vektorraum sowie $U \leq V$ ein Untervektorraum. Zeigen Sie, dass $V/U = \{v + U : v \in V\}$ ein K-Vektorraum ist. Dieser wird als Faktorraum oder Quotientenvektorraum bezeichnet.

(b) Es seien K ein Körper, V und W jeweils K-Vektorräume sowie $\phi : V \to W, v \mapsto \phi(v)$ eine lineare Abbildung. Zeigen Sie, dass $\phi = \iota \circ \overline{\phi} \circ \pi$ gilt, wobei

- $\pi : V \to V/\ker(\phi), v \mapsto v + \ker(\phi)$ ein Epimorphismus (von Vektorräumen) ist,
- $\overline{\phi} : V/\ker(\phi) \to \phi(V), v + \ker(\phi) \mapsto \phi(v)$ ein Isomorphismus (von Vektorräumen) ist,
- $\iota : \phi(V) \to W, v \mapsto v$ ein Monomorphismus (von Vektorräumen) ist.

Insbesondere gilt also $V/\ker(\phi) \cong \phi(V) = \mathrm{im}(\phi)$.

5. Präsenzübung

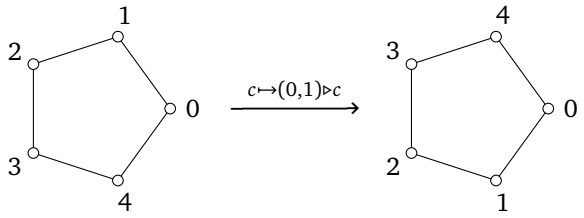
T5.1. *(Diedergruppen)*
Im Folgenden sei $n \geq 3$. Ferner bezeichne $\varphi\colon C_2 \to \mathrm{Aut}(C_n)$ den Gruppenhomomorphismus mit $\varphi(0) = \mathrm{id}_{C_n}$ und $\varphi(1) = (x \mapsto -x) \in \mathrm{Aut}(C_n)$.

(a) Es sei $D_{2n} \coloneqq C_n \rtimes_\varphi C_2$ das semidirekte Produkt von C_n mit C_2 bezüglich φ aus Teil (a) zusammen mit der Verknüpfung $\star$ (vgl. Aufgabe 4.1). Zeigen Sie, dass D_{2n} via

$$(a, b) \triangleright c \coloneqq \text{erste Koordinate von } ((a, b) \star (c, 0))$$

treu und transitiv auf C_n operiert.

(b) Beschriften Sie für $n \in \{4, 5\}$ die Seiten eines regelmäßigen n-Ecks der Reihe nach mit den Elementen $0, 1, \ldots, n-1$ von C_n und skizzieren Sie, wie die Elemente von D_{2n} darauf operieren, zum Beispiel für das Element $(0, 1) \in D_{2n}$:



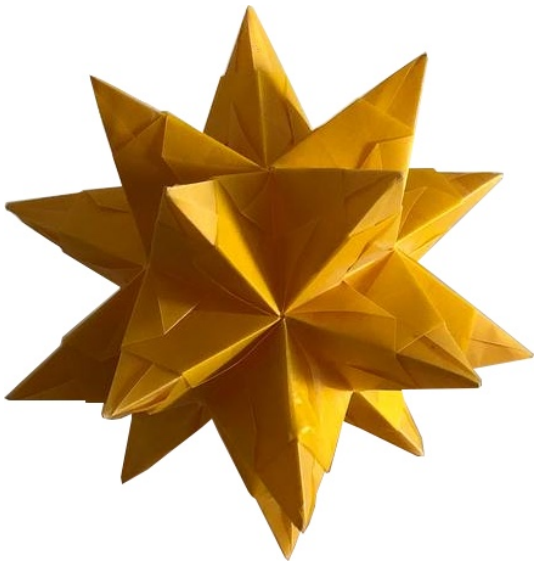
(c) Interpretieren Sie (für beliebige $n \geq 3$) die Operation von D_{2n} auf C_n geometrisch.

(d) Erinnern Sie sich an Aufgabe T1.1 und Aufgabe T2.2 und bringen Sie die Ergebnisse dieser Aufgaben mit der Gruppe $D_8 \coloneqq C_4 \rtimes_\varphi C_2$ in Zusammenhang. Hierbei dürfen Sie ebenfalls auf Aufgabe 4.1 zurückgreifen.

(e) Welche Gruppe ergibt sich für den Gruppenhomomorphismus $\varphi\colon C_2 \to \mathrm{Aut}(C_n)$ mit $\varphi(0) = \varphi(1) = \mathrm{id}_{C_n}$ (das heißt φ ist der triviale Gruppenhomomorphismus)?
Vergleichen Sie diese Gruppe mit D_{2n}.

6. Präsenzübung

T6.1. *(Operationen und Symmetrien: Bascetta-Stern, II)*
Betrachten Sie den Bascetta-Stern $\mathscr{B} \subseteq \mathbb{R}^3$ aus Aufgabe 5.4, wo Sie als Teilaufgabe (a) einen solchen Stern gebastelt hatten:



Es bezeichne G die Gruppe der Drehungen des dreidimensionalen Raumes, welche den Bascetta-Stern $\mathscr{B} \subseteq \mathbb{R}^3$ invariant lassen, wobei $\mathscr{B}$ als angemessen idealisiert anzusehen ist, sodass Faltungenauigkeiten vernachlässigt werden können. Lösen Sie nun die folgenden weiterführenden Aufgaben:

(b) Zeigen Sie, dass G treu auf $\mathscr{B}$ operiert und endlich ist.

(c) Bestimmen Sie die Ordnung von G.

T6.2. *(Gruppen der Ordnung* 12*)*

(a) Zeigen Sie, dass jede Gruppe G der Ordnung 12 einen Normalteiler $N \neq \{1_G\}, G$ besitzt.
(Hinweis: Überlegen Sie sich mittels Satz 3.3 (3), wie 2- bzw. 3-Sylowgruppen es in G geben kann. Überlegen Sie sich ferner, wie viele Sylowgruppen in G überhaupt Platz haben. Um Normalität einer Sylowgruppe zu folgern, dürfen Sie Korollar 3.4 benutzen.)

(b) Es bezeichne P_2 eine 2-Sylowgruppe von G und P_3 sei eine 3-Sylowgruppe von G. Geben Sie für jeden der folgenden drei Fälle ein Beispiel (mit Begründung!) für eine Gruppe G mit Ordnung 12 und den geforderten Eigenschaften an:

(1) $P_2 \trianglelefteq G$ und $P_3 \trianglelefteq G$, (2) $P_2 \trianglelefteq G$ und $P_3 \ntrianglelefteq G$, (3) $P_2 \ntrianglelefteq G$ und $P_3 \trianglelefteq G$.

7. Präsenzübung

T7.1. *(Nicht alle Gruppen sind ein semidirektes Produkt)*
Es seien p eine Primzahl und $n \in \mathbb{N}$. Betrachten Sie die Gruppe C_{p^n} und zeigen Sie, dass diese kein (nicht-triviales) semidirektes Produkt ist.

T7.2. *(A_n ist einfach für $n \geq 5$)*
Es bezeichne A_n die alternierende Gruppe in $\mathfrak{S}_n = \mathrm{Sym}(\{1, \ldots, n\})$. Zeigen Sie:

(a) Für $n \geq 3$ wird A_n von den 3-Zyklen erzeugt.
(Hinweis: welche Zyklen entstehen als das Produkt zweier Transpositionen?)

(b) Für $n \geq 5$ sind alle 3-Zyklen konjugiert in A_n.
(Hinweis: die fragliche Konjugiertheit in $\mathfrak{S}_n$ ist *a-priori* einfacher einzusehen. Kann man daraus nun die Konjugiertheit in A_n gewinnen? Beachten Sie, dass die Voraussetzung $n \geq 5$ einem zu jedem 3-Zyklus zwei permutierbare Zahlen zur Verfügung stellt, die nicht in selbigem 3-Zyklus vorkommen.)

(c) Satz 4.7: für $n \geq 5$ ist A_n einfach.
(Hinweis: sei $N \neq \{\mathrm{id}_{\{1,\ldots,n\}}\}$ ein Normalteiler von A_n. Betrachten Sie ein Element $\sigma \neq \mathrm{id}_{\{1,\ldots,n\}}$ von N, welches maximal viele Elemente von $\{1, \ldots, n\}$ fixiert, und zeigen Sie dann, dass σ ein 3-Zyklus sein muss. Hierbei hilft es erneut, in disjunkte Zyklen zu zerlegen. Folgern Sie anschließend $N = A_n$.)

8. Präsenzübung

T8.1. *(Isomorphietypen endlicher abelscher Gruppen mit vorgegebener Ordnung)*
Es sei G eine endliche abelsche Gruppe.

(a) Bestimmen Sie jeweils alle möglichen Isomorphietypen mit
- $|G| = 6$.
- $|G| = 12$.
- $|G| = 16$.
- $|G| = 360$.
- $|G| = p^2q^2$ für verschiedene Primzahlen p und q.
- $|G| = p^3q^3r^4$ für (paarweise) verschiedene Primzahlen p, q und r.

(b) Geben Sie eine allgemeine Formel für die Anzahl verschiedener Isomorphietypen mit Ordnung $|G|$ an.

T8.2. *(Klassifikation endlicher abelscher Gruppen via Invarianten)*

(a) Zeigen Sie:
Jede endliche abelsche Gruppe G ist isomorph zu einer Gruppe der Form

$$C_{d_1} \times \ldots \times C_{d_t}$$

mit $t \in \mathbb{N}_0$, $d_i \in \mathbb{N} \setminus \{1\}$ und $d_i \mid d_{i+1}$ für alle $1 \leq i \leq t-1$. Die d_i werden als *Elementarteiler* bezeichnet.

(b) Es sei G eine endliche abelsche Gruppe der Ordnung 48 mit Gruppenexponent 12.
Bestimmen Sie alle möglichen Isomorphietypen, die für G in Frage kommen. Falls der Isomorphietyp noch nicht eindeutig bestimmt sein sollte, geben Sie zusätzlich ein Kriterium an, wie die verschiedenen Isomorphietypen unterschieden werden können.

9. Präsenzübung

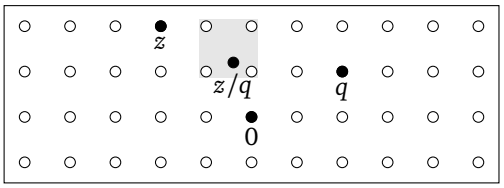
T9.1. *(Operationen mit Idealen)*
Es seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale eines Rings R. Betrachten Sie das *Komplexprodukt* $\mathfrak{a} \cdot \mathfrak{b} := \{ab : a \in \mathfrak{a},\ b \in \mathfrak{b}\}$, sowie das ***Idealprodukt*** $\mathfrak{ab} := \langle \mathfrak{a} \cdot \mathfrak{b} \rangle$ von $\mathfrak{a}$ und $\mathfrak{b}$. Zeigen Sie:

(a) $\mathfrak{a}_1 \cdot \mathfrak{a}_2$ braucht im Allgemeinen kein Ideal von R zu sein (Beispiel!).
(b) $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ und im Allgemeinen kann hierbei strikte Inklusion „$\subset$“ gelten (Beispiel!).
(c) Gilt $\mathfrak{a} + \mathfrak{b} = R$ und ist R kommutativ, so ist $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

T9.2. *(Die ganzen Gaußschen Zahlen)*
Betrachten Sie $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \in \mathbb{C} : a, b \in \mathbb{Z}\}$ zusammen mit der Funktion $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$, $a + \mathrm{i}b \mapsto (a + \mathrm{i}b)(a - \mathrm{i}b) = a^2 + b^2$ (mit $a, b \in \mathbb{Z}$). Zeigen Sie:

(a) Zu $z, q \in \mathbb{Z}[\mathrm{i}]$ mit $q \neq 0$ existieren $w, r \in \mathbb{Z}[\mathrm{i}]$ mit $z = wq + r$ derart, dass $r = 0$ oder $N(r) < N(q)$ gilt.

$\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$:



(Bemerkung: dies ist ein Analogon zur Division mit Rest in $\mathbb{Z}$ oder bei Polynomen.)

(b) $(\mathbb{Z}[\mathrm{i}])^\times = \{-1, 1, -\mathrm{i}, \mathrm{i}\}$. Ist $(\mathbb{Z}[\mathrm{i}])^\times \cong C_4$ oder $(\mathbb{Z}[\mathrm{i}])^\times \cong C_2 \times C_2$?

10. Präsenzübung

T10.1. *(Erzeugung von Idealen)*
Es seien R ein Ring und $A \subseteq R$. Betrachten Sie das von A erzeugte Ideal $\langle A \rangle$.

(a) Zeigen Sie, dass im Fall eines kommutativen Rings

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} a_i r_i \ :\ n \in \mathbb{N}_0 \text{ und } a_i \in A, r_i \in R\ \forall 1 \leq i \leq n \right\}$$

gilt.

(b) Geben Sie für den Ring $R = \mathbb{Q}^{2\times 2}$ ein Beispiel an, in dem die Gleichheit aus Teil (a) nicht gilt.

T10.2. *(Isomorphiesatz für Ringe)*
Zeigen Sie:

(a) Es seien $n \in \mathbb{N}$ und für $1 \leq i \leq n$ seien R_i Ringe und $\mathfrak{a}_i \lhd R_i$ Ideale. Dann gilt

$$\prod_{i=1}^{n} R_i \Big/ \prod_{i=1}^{n} \mathfrak{a}_i \cong \prod_{i=1}^{n} R_i/\mathfrak{a}_i.$$

(b) Seien R ein Ring und $\mathfrak{a} \lhd R$, $\mathfrak{b} \lhd R$ Ideale mit der Eigenschaft $\mathfrak{a} \subseteq \mathfrak{b}$. Dann gelten $\mathfrak{b}/\mathfrak{a} \lhd R/\mathfrak{a}$ sowie

$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong R/\mathfrak{b}.$$

11. Präsenzübung

T11.1. *(Multivariate Polynome)*
Es bezeichne I eine beliebige Indexmenge und $M = \mathbb{N}_0^{(I)}$ sei die Menge aller Abbildungen $I \to \mathbb{N}_0$, die für alle bis auf höchstens endlich viele Indizes aus I den Wert 0 annehmen, zusammen mit punktweise definierter Addition. Für einen kommutativen Ring R sei $R[M]$ die Menge aller Abbildungen $M \to R$, welche auf allen bis auf höchstens endlich vielen Elementen von M den Wert 0_R annehmen, zusammen mit punktweise definierter Addition und der wie folgt zu definierenden Multiplikation:

$$(f\colon M \to R) \cdot (g\colon M \to R) := \left(M \to R,\ c \mapsto \sum_{\substack{a,b \in M \\ a+b=c}} f(a)g(b)\right).$$

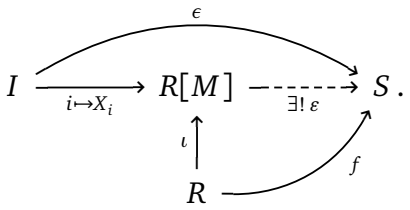
Für $i \in I$ bezeichne $X_i\colon M \to R$ die Abbildung mit $X_i(i) = 1_R$ und $X_i(j) = 0_R$ für alle $j \in I \setminus \{i\}$. Zeigen Sie die folgenden Aussagen:

(a) Das oben definierte Produkt $f \cdot g$ zweier Elemente $f, g \in R[M]$ ist tatsächlich ein Element von $R[M]$ und $R[M]$ bildet zusammen mit den hier definierten inneren Verknüpfungen einen kommutativen Ring. (Hinweis: alle Ringaxiome zu verifizieren wäre etwas lästig. Besprechen Sie nur eine repräsentative Auswahl nach eigenem Ermessen.)

(b) $\iota\colon R \to R[M],\ r \mapsto \begin{cases} M \to R, \\ \quad a \mapsto \begin{cases} r & \text{falls } a = (i \mapsto 0), \\ 0_R & \text{sonst,} \end{cases} \end{cases}$
ist ein Ringmonomorphismus.

(c) Jedes $f \in R[M]$ lässt sich als $f = \sum_{a \in M} \iota(f(a)) \prod_{i \in I} X_i^{a(i)}$ schreiben.
(Die auftretenden Produkte haben stets höchstens endlich viele von $1_{R[M]} = X_i^0$ verschiedene Faktoren und die auftretende Summe nur höchstens endlich viele von $0_{R[M]}$ verschiedene Summanden und können somit betrachtet werden, ohne über Konvergenz sprechen zu müssen.)

(d) Ist $f\colon R \to S$ ein Homomorphismus in einen beliebigen kommutativen Ring S und $\epsilon\colon I \to S$ eine beliebige Abbildung, so gibt es genau einen Ringhomomorphismus $\varepsilon\colon R[M] \to S$, welcher das folgende Diagramm kommutativ macht:



Bemerkung: man schreibt auch $R[\boldsymbol{X}]$ statt $R[M]$ mit $\boldsymbol{X} = \{X_i : i \in I\}$ und nennt $R[\boldsymbol{X}]$ den ***Polynomring*** über R in den ***Variablen*** (oder ***Unbestimmten/Veränderlichen***) X_i $(i \in I)$. Eigentlich sind die hier diskutierten Objekte sehr konkret: etwa für $I = \{1,2,3,4\}$ und $R = \mathbb{Z}$ ist ein typisches Element von $R[\boldsymbol{X}]$ gleich $10X_1^0 + X_1^{20} + 60X_1^9X_2X_4^7$. Das Bild dieses Elements unter f aus Teil (d) wäre dann $f(10)\epsilon(1)^0 + \epsilon(1)^{20} + f(60)\epsilon(1)^9\epsilon(2)\epsilon(4)^7$.

T11.2. *(Multivariate Polynome)*
Es bezeichne I eine beliebige Indexmenge und $M = \mathbb{N}_0^{(I)}$ sei die Menge aller Abbildungen $I \to \mathbb{N}_0$, die für alle bis auf höchstens endlich viele Indizes aus I den Wert 0 annehmen, zusammen mit punktweise definierter Addition. Für einen kommutativen Ring R sei $R[M]$ die Menge aller Abbildungen $M \to R$, welche auf allen bis auf höchstens endlich vielen Elementen von M den Wert 0_R annehmen, zusammen mit punktweise definierter Addition und der wie folgt zu definierenden Multiplikation:

$$(f\colon M \to R) \cdot (g\colon M \to R) := \left(M \to R,\ c \mapsto \sum_{\substack{a,b \in M \\ a+b=c}} \sum f(a)g(b)\right).$$

Für $i \in I$ bezeichne $X_i\colon M \to R$ die Abbildung mit $X_i(i) = 1_R$ und $X_i(j) = 0_R$ für alle $j \in I \setminus \{i\}$. Zeigen Sie die folgenden Aussagen:

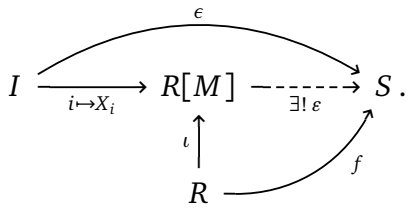
(a) Das oben definierte Produkt $f \cdot g$ zweier Elemente $f, g \in R[M]$ ist tatsächlich ein Element von $R[M]$ und $R[M]$ bildet zusammen mit den hier definierten inneren Verknüpfungen einen kommutativen Ring. (Hinweis: alle Ringaxiome zu verifizieren wäre etwas lästig. Besprechen Sie nur eine repräsentative Auswahl nach eigenem Ermessen.)

(b) $\iota\colon R \to R[M],\ r \mapsto \begin{cases} M \to R, \\ \quad a \mapsto \begin{cases} r & \text{falls } a = (i \mapsto 0), \\ 0_R & \text{sonst,} \end{cases} \end{cases}$
ist ein Ringmonomorphismus.

(c) Jedes $f \in R[M]$ lässt sich als $f = \sum_{a \in M} \iota(f(a)) \prod_{i \in I} X_i^{a(i)}$ schreiben.
(Die auftretenden Produkte haben stets höchstens endlich viele von

$1_{R[M]} = X_i^0$ verschiedene Faktoren und die auftretende Summe nur höchstens endlich viele von $0_{R[M]}$ verschiedene Summanden und können somit betrachtet werden, ohne über Konvergenz sprechen zu müssen.)

(d) Ist $f: R \to S$ ein Homomorphismus in einen beliebigen kommutativen Ring S und $\epsilon: I \to S$ eine beliebige Abbildung, so gibt es genau einen Ringhomomorphismus $\varepsilon: R[M] \to S$, welcher das folgende Diagramm kommutativ macht:



Bemerkung: man schreibt auch $R[\boldsymbol{X}]$ statt $R[M]$ mit $\boldsymbol{X} = \{X_i : i \in I\}$ und nennt $R[\boldsymbol{X}]$ den ***Polynomring*** über R in den ***Variablen*** (oder ***Unbestimmten/Veränderlichen***) X_i $(i \in I)$. Eigentlich sind die hier diskutierten Objekte sehr konkret: etwa für $I = \{1,2,3,4\}$ und $R = \mathbb{Z}$ ist ein typisches Element von $R[\boldsymbol{X}]$ gleich $10X_1^0 + X_1^{20} + 60X_1^9X_2X_4^7$. Das Bild dieses Elements unter f aus Teil (d) wäre dann $f(10)\epsilon(1)^0 + \epsilon(1)^{20} + f(60)\epsilon(1)^9\epsilon(2)\epsilon(4)^7$.

12. Präsenzübung

T12.1. *(Nicht-prime irreduzible Elemente)*
Betrachten Sie den Ring $R := \mathbb{Z}[\mathrm{i}\sqrt{5}] = \{a + \mathrm{i}\sqrt{5}b \in \mathbb{C} : a, b \in \mathbb{Z}\}$. (Die Ringaxiome nachzurechnen ist hier nicht gefordert.) Zeigen Sie dann, dass es sich bei

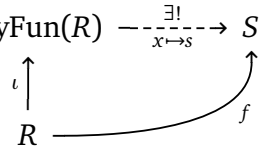
$$2 \cdot 3 = (1 + \mathrm{i}\sqrt{5}) \cdot (1 - \mathrm{i}\sqrt{5}),$$

um zwei Zerlegungen von $6 \in R$ in Produkte irreduzibler Elemente handelt, aber die darin vorkommenden Elemente keine Primelemente in R sind.
(Hinweis: betrachten Sie die Funktion $N: R \to \mathbb{Z}$ aus Aufgabe 9.4 ; wegen $N(xy) = N(x)N(y)$ für alle $x, y \in R$ lässt sich damit Teilbarkeit in R auf Teilbarkeit in $\mathbb{Z}$ zurückführen.)

T12.2. *(Polynome vs. Polynomfunktionen)*
Sei R ein kommutativer Ring. Es bezeichne $\mathrm{PolyFun}(R) \subseteq \mathrm{Abb}(R,R)$ die Menge der Funktionen $R \to R$, welche durch Polynome gegeben sind (also $\epsilon_\bullet(R[X])$ in der Notation von § 7.2). Man hat die kanonische Einbettung $\iota: R \to \mathrm{PolyFun}(R)$, welche jedem $r \in R$ die konstante Abbildung $R \to R$, $a \mapsto r$, zuordnet. Wir sagen, $x \in \mathrm{PolyFun}(R)$ sei ***von variablem Typ***, falls die folgende Eigenschaft erfüllt ist (vgl. Satz 7.4):

> Für jeden kommutativen Ring S, Ringhomomorphismus $f: R \to S$ und jedes $s \in S$ gibt es genau einen Ringhomomorphismus

PolyFun$(R) \to S$, welcher x auf s abbildet und das folgende Diagramm kommutativ macht:



(a) Geben Sie ein Beispiel für einen Ring R und ein Element $x \in \text{PolyFun}(R)$ von variablem Typ an.
(b) Geben Sie ein Beispiel für einen Ring R an, sodass es kein Element $x \in \text{PolyFun}(R)$ von variablem Typ gibt.

13. Präsenzübung

T13.1. *(Nicht-Existenz des ggT)*
Betrachten Sie den Ring $R := \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \in \mathbb{C} : a, b \in \mathbb{Z}\}$.
Zeigen Sie für die beiden Elemente $\alpha = 2$ und $\beta = 1 + \sqrt{-3}$ von R, dass $\text{ggT}(\alpha^2, \alpha\beta)$ nicht existiert.
(Hinweis: Erinnern Sie sich an Aufgabe T12.1.)

T13.2. *(Ein Körper mit genau 4 Elementen)*
Es sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ und $f = X^2 + X + 1_{\mathbb{F}_2} \in \mathbb{F}_2[X]$. Ferner sei $K = \mathbb{F}_2[X]/\langle f \rangle$.
(a) Zeigen Sie, dass f irreduzibel ist und folgern Sie, dass K ein Körper ist.
(b) Bestimmen Sie alle Elemente von K und stellen Sie die zugehörigen Additions- und Multiplikationstafeln auf (vgl. Tutoriumsblatt 1).
(c) Ist $K^\times$ zyklisch? Falls ja, bestimmen Sie *alle* Erzeuger von $K^\times$.

T13.3. *(Satz über rationale Nullstellen)*
(a) Es sei $f = c_n X^n + \ldots + c_1 X + c_0 X^0 \in \mathbb{Z}[X]$ ein Polynom vom Grad $n \geq 1$ mit rationaler Nullstelle $\frac{a}{q} \in \mathbb{Q}$, a und q teilerfremd. Zeigen Sie $a \mid c_0$ und $q \mid c_n$.
(b) Benutzen Sie Teil (a), um einzusehen, dass $\sqrt{2}$ (eine Nullstelle von $X^2 - 2$) nicht rational ist.
(c) Bestimmen Sie alle Nullstellen in $\mathbb{Q}$ des Polynoms $3X^4 - 5X^3 + X^2 - 5X - 2$.

14. Präsenzübung

T14.1. *(Faktorisieren von Polynomen)*
Zerlegen Sie die folgenden Polynome über $\mathbb{Z}[X]$ in Primfaktoren:
(a) $X^8 - 1$,
(b) $8X^3 + 16X + 24$.

T14.2. *(Irreduzibilität)*
Untersuchen Sie die folgenden Polynome auf Irreduzibilität:
(a) $X^6 + 3X^2 + 15X^2 + 3X + 6 \in \mathbb{Q}[X]$.
(b) $X^3 + 5 \in \mathbb{Q}[X]$.
(c) $X^2 + 4XY + 4Y^2 \in \mathbb{Q}[X, Y]$.

(d) $X^5 + 1 \in \mathbb{Z}[X]$.
(e) $X^4 + X^3 + 2X^2 + X + 1 \in \mathbb{Z}[X]$.

T14.3. *(Kreisteilungspolynome)*
Es sei p eine Primzahl. Betrachten Sie das Polynom $f_p(X) = X^p - 1 \in \mathbb{Z}[X]$.
(a) Zeigen Sie, dass das Polynom $f_p(X)$ in $\mathbb{Z}[X]$ reduzibel ist.
(b) Zerlegen Sie $f_p(X)$ über $\mathbb{Z}[X]$ in irreduzible Faktoren. Die Irreduzibilität der Faktoren ist zu begründen.
(c) Es sei nun $\zeta \in \mathbb{C} \setminus \{1\}$ eine beliebige Nullstelle von $f_p(X)$.
Wie sehen alle p komplexen Nullstellen von $f_p(X)$ aus?
Zeigen Sie, dass alle Nullstellen von $f_p(X)$ eine Untergruppe von $\mathbb{C}^\times$ bilden und bestimmen Sie den Isomorphietyp dieser Gruppe.
(d) Zeigen Sie die Identität

$$\prod_{i=1}^{p-1} \left(1 - \zeta^i\right) = p.$$

Literaturverzeichnis

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Ann. Math. (2)*, 160(2): 781–793, 2004.

[2] P. Aluffi. *Algebra: Chapter 0*. Providence, RI: AMS, 2009.

[3] M. Atiyah. Mathematics in the 20th century. *Bull. Lond. Math. Soc.*, 34(1):1–15, 2002.

[4] P. Borwein and T. Erdélyi. *Polynomials and polynomial inequalities*. New York, NY: Springer-Verlag, 1995.

[5] S. Bosch. *Algebraic geometry and commutative algebra*. London: Springer, 2. Auflage, 2022.

[6] S. Bosch. *Algebra*. Berlin: Springer, 10. Auflage, 2023.

[7] J. Brüdern. *Einführung in die analytische Zahlentheorie*. Berlin: Springer, 1995.

[8] J. Buchmann. *Einführung in die Kryptographie*. Berlin: Springer, 6. Auflage, 2016.

[9] P.-J. Cahen and J.-L. Chabert. What you should know about integer-valued polynomials. *Am. Math. Mon.*, 123(4):311–337, 2016.

[10] J. J. Callagy. The central angle of the regular 17-gon. *Math. Gaz.*, 67:290–292, 1983.

[11] C. Cocks. A note on 'non-secret encryption'. 1973.

[12] H. Cohen. *A course in computational algebraic number theory*. Berlin: Springer, 1993.

[13] H. Cohen. *Number theory. Volume I: Tools and Diophantine equations*. New York, NY: Springer, 2007.

[14] K. Conrad. Expository papers. Online verfügbar, 2019.

[15] M. Dehn. Über den Rauminhalt. *Math. Ann.*, 55(3):465–478, 1901.

[16] S. Devadoss, Z. Epstein, and D. Smirnov. Visualizing scissors congruence. In *32nd international symposium on computational geometry, SoCG'16, Boston, MA, USA, June 14–17, 2016. Proceedings*, volume 49(4). Wadern: Schloss Dagstuhl – Leibniz Zentrum für Informatik, 2018. Id/No 66; Siehe auch `https://dsmirnov.me/scissors-congruence/`.

[17] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry*. Berlin: Springer, 1995.

[18] G. Fischer and B. Springborn. *Lineare Algebra. Eine Einführung für Studienanfänger*. Berlin: Springer, 19. Auflage, 2020.

[19] C. F. Gauß. *Untersuchungen über höhere Arithmetik. (*Disquisitiones arithmeticae.*)*. Berlin: Springer, 1889. Herausgegeben von H. Maser.
[20] Th. Grundhöfer. Einführung in die Algebra. Vorlesungsskriptum. LaTeX-Satz von Markus Sauer und Andreas Beck, 2018.
[21] R. Gupta and M. R. Murty. A remark on Artin's conjecture. *Invent. Math.*, 78: 127–130, 1984.
[22] R. Hartshorne. *Geometry: Euclid and beyond*. Berlin: Springer, 2000.
[23] A. Hatcher. *Algebraic topology*. Cambridge: Cambridge University Press, 2002.
[24] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Q. J. Math., Oxf. II. Ser.*, 37:27–38, 1986.
[25] D. Hilbert. *Gesammelte Abhandlungen. Bd. 3. Analysis · Grundlagen der Mathematik · Physik · Verschiedenes · Lebensgeschichte*. 1935.
[26] O. Hölder. Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. *Math. Ann.*, 43: 301–412, 1893.
[27] Ch. Hooley. On Artin's conjecture. *J. reine angew. Math.*, 225:209–220, 1967.
[28] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. New York, NY: Springer, 2. Auflage, 1990.
[29] H. Iwaniec and E. Kowalski. *Analytic number theory*. Providence, RI: American Mathematical Society (AMS), 2004.
[30] K. Jänich. *Funktionentheorie. Eine Einführung*. Berlin: Springer, 6. Auflage, 2004.
[31] K. Jänich. *Vektoranalysis*. Berlin: Springer, 5. Auflage, 2005.
[32] Y. Jiang and Y. Deng. Strong pseudoprimes to the first eight prime bases. *Math. Comput.*, 83:2915–2924, 2014.
[33] Chr. Karpfinger and K. Meyberg. *Algebra. Gruppen, Ringe, Körper*. Berlin: Springer, 6. Auflage, 2024.
[34] E. Landau. Sur quelques problèmes relatifs à la distribution des nombres premiers. *Bull. Soc. Math. Fr.*, 28:25–38, 1900.
[35] E. Landau. Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate. *Arch. der Math. u. Phys. (3)*, 13:305–312, 1908.
[36] E. Landau. *Grundlagen der Analysis*. Darmstadt: Wissenschaftliche Buchgesellschaft XIII, 2. Auflage, 1970.
[37] S. Lang. *Algebra*. New York, NY: Springer, 3. Auflage, 2002.
[38] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*. Cambridge: Cambridge University Press, 2007.
[39] M. R. Murty and P. Rath. *Transcendental numbers*. New York, NY: Springer, 2014.
[40] N. Oswald and J. Steuding. *Elementare Zahlentheorie. Ein sanfter Einstieg in die höhere Mathematik*. Heidelberg: Springer Spektrum, 2015.
[41] H. Poincaré. Analysis situs. *J. Éc. Politech*, 2(1):1–123, 1895.
[42] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff jun. The pseudoprimes to $25 \cdot 10^9$. *Math. Comput.*, 35:1003–1026, 1980.

[43] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12:128–138, 1980.
[44] J.-P. Sydler. Conditions nécessaires et suffisantes pour l'équivalence des polyèdres de l'espace euclidien à trois dimensions. *Comment. Math. Helv.*, 40:43–80, 1965.
[45] M. Technau. Algebra. Vorlesungsskriptum, 2021.
[46] M. Technau. Einführung in die komplexe Analysis. Vorlesungsskriptum, 2021.
[47] H. Wielandt. Ein Beweis für die Existenz der Sylowgruppen. *Arch. Math.*, 10: 401–402, 1959.
[48] J. Wolfahrt. *Einführung in die Zahlentheorie und Algebra*. Braunschweig: Vieweg, 2. Auflage, 2011.

Index